Redefining the Right to Be Let Alone: Privacy Rights and the Constitutionality of Technical Surveillance Measures in Germany and the United States

By Nicole Jacoby*

Introduction

The fight against international terrorism has led many countries, including Germany and the United States, to implement new criminal statutes that grant law enforcement officials additional powers to observe and investigate criminal suspects. Notably, the U.S.A. P.A.T.R.I.O.T. Act of 2001 and Germany's Second Anti-Terrorism Package of 2002 both sought to remove bureaucratic red tape, to increase collection of personal data at the border, and to improve the exchange of information between security agencies.[1] These laws have given rise to new privacy concerns in both countries, especially in light of the development of new investigative technologies and increasingly intrusive government surveillance methods.[2]

U.S. and German courts alike long have struggled to find the proper balance between protecting the privacy rights of criminal suspects and granting law enforcement officials the adequate technical tools to fight crime.[3] The highest courts in each country have produced different paradigms for determining where the public sphere ends and the private sphere begins in cases involving technical surveillance. In the United States, the right to privacy is a negative right. Individuals have the right to be free from illegal government searches and seizures, but the government has no constitutional duty to preserve or cultivate an individual's private sphere. Against this backdrop, the U.S. Supreme Court has inquired simply whether a criminal suspect's reasonable expectation of privacy has been violated in cases involving state use of technical surveillance measures. In contrast, privacy is a positive right in Germany.

---

* Nicole Jacoby, Attorney, Alston & Bird; L.L.M., Westfälische Wilhelms-Universität Münster (Fulbright Scholar 2005-2006). The author would like to thank Prof. Bodo Pieroth of the University of Münster, as well as Dr. Jutta Kemper and Dr. Angelika Schlunck of the German Federal Ministry of Justice, for their helpful comments. Many thanks also to the German Fulbright Commission and the Robert Bosch Foundation for their financial support of the research that led to this article.

[1] *See* Shawn Boyne, "The Future of Liberal Democracies in a Time of Terror: A Comparison of the Impact On Civil Liberties in the Federal Republic of Germany and the United States," 11 Tulsa J. Comp. & Int'l L. 111, 119, 126 (2003) (discussing measures implemented in the United States in 2001 and in Germany in 2002 to improve information-gathering by intelligence agencies).

[2] *See* Boyne, *supra* note 1, at 128.

Accordingly, Germany's *Bundesverfassungsgericht* [Federal Constitutional Court] has constructed an affirmative obligation on the part of the state to create the conditions that foster and uphold the private sphere. In analyzing state use of technical surveillance methods, the Federal Constitutional Court has examined the effect of such surveillance on a suspect's human dignity and whether a surveillance technique inhibits the free development of personality.

Despite these differences in approach, the countries' highest courts more often than not have reached similar conclusions. Part I of this Article traces modern U.S. privacy jurisprudence as it has evolved under the Fourth Amendment in light of new developments in surveillance technologies. It describes the shift from a privacy paradigm based on principles of trespass to one that instead focuses on reasonable expectations of privacy. Part II evaluates the roots of Germany's human dignity principle in the privacy context and evaluates four very recent privacy decisions involving the use of sophisticated surveillance techniques in government investigations. Part III compares the U.S. and German approaches.

Despite their contrasting judicial philosophies, German and U.S. courts both have recognized the home as the most highly protected realm in their respective societies. In both countries, the state may use technical surveillance measures in a private home only in the most limited of circumstances. Notwithstanding this similarity, the article concludes that German jurisprudence is better prepared to protect the privacy rights of criminal defendants in the 21st century. By linking privacy to human dignity, the German Federal Constitutional Court has assured that privacy lines are not redrawn simply because investigative technologies get more sophisticated or law enforcement priorities shift.

[3] *See* Boyne, *supra* note 1, at 147-152.

I. The United States

A. The Constitutional Framework

i. Background

The United States Constitution makes no explicit mention of the right to privacy. Nonetheless, U.S. courts over the years have recognized a constitutional right to privacy. This protection has not been all encompassing. Rather, it has targeted specific circumstances, which have been expanded over time to include privacy in marriage, reproduction, birth control, family relationships, child rearing and education.[4]

The most direct expression of the right to privacy can be found in the U.S Constitution's Fourth Amendment.[5] The Fourth Amendment states:

> 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.[6]

The purpose of the amendment was to protect people from arbitrary government intrusion into their liberty, privacy, and possessory interests. The Fourth Amendment encompasses two main ideas. First, a government search or seizure must be "reasonable." Second, before embarking on a search or seizure, government actors should obtain warrants whenever possible, and warrants should be based on the principle of "probable cause." Because the Fourth Amendment applies only to "searches" and "seizures," an investigative method that falls within neither category need not be reasonable and may be employed without a warrant and without probable case, regardless of the circumstances surrounding its use. Therefore, in determining whether the Fourth Amendment has been violated, courts traditionally have looked first to whether a search or seizure actually has taken place. Only after concluding that

[4] *See* Gebhard Rehm, "Just Judicial Activism? Privacy and Informational Self-Determination in U.S. and German Constitutional Law," 32 U. West. L.A. L. Rev. 275, 303 (2001).
[5] *See* James Q. Whitman, "The Two Western Cultures of Privacy: Dignity Versus Liberty," 113 Yale L.J. 1151, 1212 (2004) (noting that "privacy" begins with the Fourth Amendment).
[6] U.S. Const., Fourth Amendment.

a search or seizure has occurred will courts consider whether the search or seizure was reasonable and/or required a warrant.

A search that is conducted with consent is not unconstitutional under the Fourth Amendment.[7] Similarly, an unconstitutional search has not taken place where police investigators make observations in a public space, such as a street,[8] a bar,[9] or a sports stadium.[10] Only in particularly intimate areas within a public space, such as a locked bathroom stall in an otherwise public building, are the police required to obtain a search warrant.[11] The consequence of an illegal search is that the evidence obtained cannot be used against the criminal defendant who was the subject of the search in a court proceeding.[12]

ii. Exceptions for Emergencies and Exigent Circumstances

U.S. courts have recognized important limits and exceptions to the Fourth Amendment when the police are conducting searches in emergency situations or under exigent circumstances. Under exigent or emergency circumstances that require immediate aid law enforcement officials may search a private home or property or person without a search warrant.[13] In the aftermath of the warrantless search a court will consider whether a reasonable police officer under the same circumstances would have determined that emergency circumstances were present.[14]

---

[7] *Schneckloth v. Bustamonte*, 412 U.S. 218, 219 (1973) (citing Davis v. United States, 328 U.S. 582, 593-594, 66 S. Ct. 1256, 90 L. Ed. 2d 1453 (1946)); *Zap v. United States*, 328 U.S. 624, 6307 (1946), rev'd, 330 U.S. 800 (1947).

[8] *Rodriguez v. United States*, 878 F. Supp. 20, 24 (S.D.N.Y. 1995); *People v. Warren*, 199 Cal. Rptr. 864, 867 (Ct. App. 1984); *People v. Carlson*, 677 P.2d 310, 316 (Colo. 1984).

[9] *Id. See also Gordon v. State*, 640 S.W.2d 743, 753 (Tex. Ct. App. 1982); *Pellatz v. State*, 711 P.2d 1138, 1141 (Wyo. 1986).

[10] *Weber v. City of Cedarburg*, 384 N.W.2d 333, 339 (Wis. 1986).

[11] *People v. Kalchik,* 407 N.W.2d 627, 631 (Mich. Ct. App. 1987) (camera installed by police in ceiling of public restroom in mall videotaped individuals engaging in homosexual activities); *People v. Dezek*, 308 N.W.2d 652, 654 (Mich. Ct. App. 1981) (police installed needle-point video camera lens in ceiling above toilet stalls).

[12] *Mapp v.* Ohio, 367 U.S. 643, (1961) (applying rule to state courts); *Weeks v. United States*, 232 U.S. 383, 391-94 (1914) (applying rule to federal courts).

[13] *See* Matthew Bender, *Criminal Constitutional Law* § 3.02 (2004).

[14] *See Hopkins v. City of Sierra Vista, Ariz.*, 931 F.2d 524 (9th Cir. 1991); *United States v. Lindsey*, 877 F.2d 777, 781-82 (9th Cir. 1988); *United States v. Socey*, 846 F.2d 1439, 1446 (D.C. Cir. 1988); *United States v. Rivera*, 825 F.2d 152, 156 (7th Cir.), cert. denied, 484 U.S. 979 (1987).

A search conducted without a warrant can be justified where a person's life is endangered, a risk of serious bodily harm exists,[15] or private property[16] must be protected. Similarly, investigators may conduct an immediate search of an area (including rooms in a residential dwelling) when they arrive at the scene of a murder[17] or burglary[18] to ensure that no additional victims exist and to determine whether the suspect remains in the area. Additionally, investigators may conduct a search without a warrant where a substantial risk exists that evidence will be lost, removed or destroyed before a search warrant can be obtained.[19] However, investigators must believe with reasonable certainty that the evidence in question is located on the property they are searching and that an imminent threat exists that it will be destroyed, removed or lost.[20]

Police officers must obtain a search warrant as soon as the exigent or emergency circumstances that justified the warrantless search have passed.[21] Prosecutors have the burden to prove in the aftermath that police investigators genuinely faced exigent circumstances or an emergency situation.[22] However, even exigent circumstances will not justify a warrantless search in cases where the search involved only a minor offense.[23]

Finally, investigators may search a private residence without a warrant under the "hot pursuit" doctrine.[24] Under this doctrine, police officers may search an area without a warrant when they are in "hot pursuit" of a suspect they want to arrest. A pursuit qualifies as "hot" when the suspect immediately or directly fled from the crime of a scene or attempted arrest.[25]

---

[15] *Mincey v. Arizona,* 437 U.S. 385, 392 (1978), quoting *Wayne v. United States*, 318 F.2d 205, 212 (D.C. Cir. 1963) (opinion of Burger, J.).
[16] *Reardon v. Wroan,* 811 F.2d 1025, 1029-30 (7th Cir. 1987); *State v. Myers,* 601 P.2d 239, 244 (Alaska 1979); *People v. Duncan*, 720 P.2d 2, 5 (Cal. 1986).
[17] *Wayne v. United States,* 318 F.2d 205, 212 (D.C. Cir. 1963) (opinion of Burger, J.).
[18] *Reardon v. Wroan,* 811 F.2d 1025, 1030 (7th Cir. 1987*)*; *United States v. Dart*, 747 F.2d 263, 267 (4th Cir. 1984); *People v. Duncan*, 720 P.2d 2, 5 (Cal. 1986); *People v. Bradley*, 183 Cal. Rptr. 434, 437 (Ct. App. 1982); *State v. Metz*, 422 N.W.2d 754, 757 (Minn. Ct. App. 1988).
[19] *United States v. Sangineto-Miranda,* 859 F.2d 1501, 1511 (6th Cir. 1988); *United States v. Clement*, 854 F.2d 1116, 1119 (8th Cir. 1988); *United States v. Socey*, 846 F.2d 1439, 1444 (D.C. Cir. 1988*)*; *United States v. Napue,* 834 F.2d 1311, 1326 (7th Cir. 1987*)*; *United States v. Rivera*, 825 F.2d 152, 156 (7th Cir.), cert. denied, 484 U.S. 979 (1987); *United States v. Moore*, 790 F.2d 13, 15 (1st Cir. 1985).
[20] *United States v. Wilson,* 865 F.2d 215, 216 (10th Cir. 1989); *United States v. Sangineto-Miranda,* 859 F.2d 1501, 1511 (6th Cir. 1988); *United States v. Clement*, 854 F.2d 1116, 1119 (8th Cir. 1988); *United States v. Socey,* 846 F.2d 1439, 1444 n.5, 1445 (D.C. Cir. 1988); *United States v. Aquino*, 836 F.2d 1268, 1272 (10th Cir. 1988).
[21] 437 U.S. at 393; *United States v. Forker*, 928 F.2d 365, 368 (11th Cir. 1991); *United States v. Grisset,* 925 F.2d 776, 778 (4th Cir.), cert. denied, 500 U.S. 945 (1991); *People v. Krueger*, 567 N.E.2d 717 (Ill. App. Ct. 1991), cert. denied, 112 S. Ct. 1293 (1992).
[22] *Welsh v. Wisconsin,* 466 U.S. 740, 750 (1984).
[23] *See* Bender, *supra* note 13, at § 3.02.
[24] *U.S. v. Santana*, 427 U.S. 38, 42 (1976); *Warden v. Hayden*, 387 U.S. 294, 298 (1967). *See also Minnesota v. Olson*, 495 U.S. 91, 100 (1990).
[25] 466 U.S. 740 (1984).

B. The Fourth Amendment and the Use of Technical Surveillance Measures

i. The Trespass Doctrine

For much of the 20th century, the legal concept of privacy was closely linked to the protection of property interests.[26] Under this logic, a search occurred when government actors trespassed on private property. As a result, under the jurisprudence prior to the 1960s, warrants were necessary only in cases in which the courts found that the government had interfered with the possessory interests of individuals.

The 1928 case, *Olmstead v. U.S.*, provides an example of how this analysis was applied to police use of wiretaps to intercept private telephone conversations.[27] In ruling that no search (and therefore no constitutional violation) had occurred, the Court emphasized that neither the "defendant's person," nor "his papers or his tangible material effects" had been searched, nor had "an actual physical invasion of his house" taken place.[28] Rather, the phones were tapped "without trespass upon any property of the defendants"[29] and the law enforcement officials intercepting the telephone calls "were not in the house of either party to the conversation."[30] Accordingly, the Court concluded that the tapped wires were not part of the defendant's home or office "any more than […] the highways along which they [were] stretched."[31] Therefore, the wiretapping did not amount to a search or seizure within the meaning of the Fourth Amendment.[32]

The Court came to the same conclusion in a 1942 case addressing the use of a detectaphone, or listening device, by federal agents to eavesdrop on conversations taking place in the defendant's office.[33] In *Goldman v. U.S.*, the Court rejected arguments that

[26] *See* Ric Simmons, "From Katz to Kyllo: A Blueprint for Adapting the Fourth Amendment to Twenty-First Century Technologies," 53 Hastings L.J. 1303, 1307 (2002).
[27] *Olmstead v. U.S.,* 277 U.S. 438 (1928).
[28] *Id.* at 466.
[29] *Id.* at 457.
[30] *Id.*
[31] *Id.* at 465.
[32] *Id.* at 466.
[33] *Goldman v. U.S.,* 316 U.S. 129 (1942).

attempted to distinguish between the taping of a live conversation occurring within the confines of four walls and a telephone conversation that involved the transmission of voices over wires outside of a building.[34] The Court concluded that "no reasonable or logical distinction" could be drawn between a listening device and a wiretap, and that the use of the detectaphone by Government agents was not a violation of the Fourth Amendment.[35]

The Court sharpened its analysis in 1961, distinguishing between a listening device placed on an outside adjoining wall, such as the detectaphone in *Goldman*, and a microphone that actually penetrated a wall considered to be the defendants' property.[36] In *Silverman v. U.S.*, the Court found that the use of the so-called "spike mike" constituted an illegal trespass because, unlike the detectaphone in *Olmstead*, it physically intruded into the defendants' premises.[37] The Court noted that "the officers overheard the petitioners' conversations only by usurping part of the petitioners' house or office […], a usurpation that was effected without their knowledge and without their consent."[38] Accordingly, the Court held that the defendants' Fourth Amendment rights had been violated.[39]

ii. The Birth of Reasonable Expectations: *U.S. v. Katz*

In the landmark 1967 case, *United States v. Katz*,[40] the Supreme Court overturned its prior reasoning, marking a major shift in Fourth Amendment jurisprudence. In *Katz*, the Court outright rejected the property-based trespass doctrine and moved toward a more qualitative framework that evaluated an individual's reasonable expectation of privacy.[41]

In *Katz*, agents from the Federal Bureau of Investigation (FBI) had attached an electronic listening and recording device to the outside of a public phone booth from which

[34] *Id.* at 135.
[35] *Id.*
[36] 365 U.S. 505, 510-511.
[37] *Id.*
[38] *Id.* at 511.
[39] *Id.* at 511-512.
[40] *Katz v. U.S.*, 389 U.S. 347 (1967).
[41] *Id.* at 353.

the defendant placed phone calls.[42] The Ninth Circuit Court of Appeals had rejected arguments that the collection of the recordings violated the Fourth Amendment.[43] Citing *Olmstead* and *Goldman*, the Ninth Circuit noted that "no physical entrance into an area occupied by the [defendant]" had occurred.[44] The Supreme Court reversed, declaring that "the Fourth Amendment protects people, not places."[45] In explaining its ruling, the Court noted that a person who enters a phone booth and shuts the door behind him assumes his conversation will not be broadcast to the world.[46] The fact that the caller could be seen through the glass of the booth was not relevant to the Fourth Amendment inquiry, when "what [the caller] sought to exclude... was not the intruding eye – [but] the uninvited ear."[47] Accordingly, the Court ruled that an illegal search had taken place, emphasizing that "what a person knowingly exposes to the public, even in his own 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."[48]

In his concurring opinion, Justice Harlan formulated a highly influential two-part test for determining whether an invasion of privacy violated the Fourth Amendment.[49] First, a person must exhibit an actual or subjective expectation of privacy, and, second, the expectation must be one that society recognizes as "reasonable." [50] This test was subsequently adopted by a majority of the Court and provided the foundation for Fourth Amendment jurisprudence for the remainder of the Twentieth Century.

In the same year as *Katz* the Supreme Court decided a second case, which demonstrated the Court's increasing concerns about the invasiveness of new technical investigatory methods. In *Berger v. New York*, the Court struck down several provisions of a

[42] *Id.* at 348.
[43] *Katz v. U.S.*, 369 F.2d 130 (9th Cir. 1966).
[44] 389 U.S. at 348-49.
[45] *Id.* at 351.
[46] *Id.* at 352.
[47] *Id.*
[48] *Id.* at 351.
[49] *Id.* at 361.
[50] *Id.* at 361.

New York statute as unconstitutional because it allowed wiretapping without adequate legal safeguards.[51] First, the statute authorized eavesdropping without requiring a foundation for the presumption that any particular offense had been or was being committed.[52] Second, the statute did not require that police investigators provide a "precise and discriminate" description of the conversations to be wiretapped.[53] Third, the statute did not require that police end the acoustic surveillance as soon as they obtained the information sought by their investigation.[54] Fourth, the Court viewed as unconstitutional the fact that investigators could wiretap a suspect's phone for a period of two months without a fixed termination date and could obtain an extension without a showing of probable cause.[55] Finally, the law did not require that the suspect be notified of the surveillance even when no exigent circumstances were present.[56]

Although *Berger* was decided a few months prior to *Katz*, the *Berger* decision made plain that the Supreme Court had reservations regarding the development of new investigative technologies. The Court noted that the law had not kept pace with advances in scientific knowledge[57] and recognized that wiretapping by its very nature represented a broad invasion of privacy.[58] The legislature agreed. In response to the Court's decisions in *Katz* and *Berger*, Congress passed a law to ensure that wiretapping could be used by the state only in limited circumstances.

The Wiretap Statute of 1968 limited the crimes and circumstances under which the state could wiretap conversations and established strict compensation measures for private persons who were illegally wiretapped by other private citizens.[59] The requirements of the Wiretap Statute were stricter than those set forth by the Supreme Court in *Berger*.[60] The law

[51] 388 U.S. 41.
[52] *Id.* at 56.
[53] *Id.*
[54] *Id.* at 59.
[55] *Id.* at 59.
[56] *Id.* at 60.
[57] "The law, though jealous of individual privacy, has not kept pace with these advances in scientific knowledge." *Id.* at 49.
[58] "By its very nature eavesdropping involves an intrusion on privacy that is broad in scope." *Id.* at 56.
[59] Title III of the Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 197, 211 (1968) (codified as amended at 18 U.S.C. §§ 2510-2522 (1994)).
[60] *See* Robert A. Pikowsky, "An Overview of the Law of Electronic Surveillance Post September 11, 2001," 94 Law Libr. J. 601, 604 (2002).

prohibited the willful eavesdropping of wire, electronic or oral communications.[61] Only certain officials, such as the Attorney General, could request a search warrant from a judge in order to wiretap telephone conversations and only in cases where specific serious crimes were the focus of the investigation.[62] A judge could only permit the wiretap where there was probable cause that the suspect committed, or imminently would commit, one of the crimes listed in the statute, and that specific conversations about the crime would be revealed during the acoustic surveillance.[63] In addition, other traditional investigatory measures had to have been unsuccessful, less likely to be successful or too dangerous. The statute foresaw an exception in emergency situations.[64] Where an immediate risk of life or severe bodily injury was present or where conspiratorial activities threatening the national security interest were being investigated, prosecutors could begin the acoustic surveillance without a search warrant so long as one was obtained within 48 hours of the start of the surveillance.[65] In addition, the Wiretap Statute reaffirmed the right of the Executive Branch to use appropriate measures in situations where the national security of the United States was at risk.[66]

The Wiretap Statute has been updated numerous times over the years to accommodate new developments in communications technology. In 1986 cell phones and other electronic communications, such as email, were given the same protections as landline telephone calls under the Electronic Communications Privacy Act (ECPA).[67] The Communications Assistance for Law Enforcement Act of 1994 added cordless phones to the list of prohibited communications, which the ECPA had overlooked. [68]

iii. Privacy Protection and National Security after *Katz*

[61] § 802, 82 Stat. at 213-14 (current version at 18 U.S.C. § 2511 (2000)).
[62] § 802, 82 Stat. at 216-17 (current version at 18 U.S.C. § 2516(1) (2000)).
[63] *See* Wayne R. Lafave, Jerold H. Israel, & Nancy J. King, *Criminal Procedure* 333 (2d ed. 1999).
[64] *See* Lafave, Israel, et. al, *supra* note 63, at 333.
[65] 18 U.S.C. § 2518(7).
[66] Nothing in the statute should be seen as limiting "the constitutional power of the President to take such measures as he deems necessary to protect the United States against the overthrow of the Government by force or other unlawful means, or against any other clear and present danger to the structure or existence of the Government." *Id.* at 2511(3).
[67] *See* Pikowsky, *supra* note 60, at 605.
[68] *See* Pikowsky, *supra* note 60, at 605.

In *Katz*, the Supreme Court emphasized that its decision did not address situations in which the national security of the United States was at risk.[69] This was the focus of the 1972 *Keith* case, in which the Court had to determine whether the use of wiretaps without a search warrant was constitutional in situations involving national security. In the *Keith* case three members of a domestic extremist group were accused of conspiring to plant explosives at the headquarters of the Central Intelligence Agency (CIA). Prosecutors had wiretapped the suspects without a search warrant.

Prosecutors argued that they had the right to wiretap conversations in two types of situations involving national security: in cases involving domestic subversion and foreign intelligence operations.[70] They argued that this right was a reasonable extension of executive power, which allowed the president to take appropriate steps to ensure the national security of the United States.[71]

In a unanimous decision the Supreme Court ruled that a search warrant was constitutionally required in cases involving domestic subversion.[72] The circumstances at hand were not sufficient to justify an exception to Fourth Amendment requirements.[73] The Court emphasized that the use of wiretaps was particularly sensitive where domestic subversion was involved because the gathering of intelligence was by nature "necessarily broad and continuing" and the temptation to use such a surveillance to oversee political dissent would be difficult to resist.[74]

The *Keith* decision left open the question of whether a search warrant was constitutionally required in cases where the Executive Branch asked prosecutors to wiretap so-called "foreign powers" within the United States.[75] In order to fill this gap, the U.S.

---

[69] 389 U.S. at 359.
[70] *U.S. v. U.S. District Court*, 407 U.S. 297 (1972).
[71] *Id.* at 318-319. The President of the United States has the constitutional duty to "preserve, protect and defend the Constitution of the United States." U.S. Const. art. II, 1, cl. 7.
[72] *Id.* at 320.
[73] *Id.*
[74] *Id.*
[75] *Id.* at 321-322.

Congress passed the Foreign Intelligence Surveillance Act (FISA) in 1978.[76] The statute established a special court with exclusive jurisdiction over cases in which the state wanted to wiretap foreign powers within the United States in order to investigate foreign intelligence operations. Under the statute the term "foreign powers" refers not only to foreign states, but also to international terrorists and members of foreign political organizations.[77] In order to wiretap foreign powers within the United States, prosecutors had to demonstrate that the primary goal of the surveillance was the collection of intelligence and that there was probable cause that the suspect was a foreign power or agent of a foreign power.[78] Investigators had to fulfill specific conditions to ensure that U.S. persons[79] were not impacted too severely by the surveillance.[80] In emergency situations investigators were permitted to begin the surveillance without a search warrant, however, they had to obtain a warrant within 72 hours.[81] The Executive Branch could also, under limited circumstances, wiretap conversations between foreign powers.[82] However, this exception applied only where foreign powers or their agents were the focus of the surveillance and no substantial likelihood existed that a U.S. person would be the subject of surveillance.[83]

After the September 11, 2001 terrorist attacks in New York, Congress amended FISA by passing the U.S.A. P.A.T.R.I.O.T. Act (Patriot Act).[84] The Patriot Act broadened the range of tools federal investigators could use to surveil foreign powers to include "roving" wiretaps and the surveillance of email.[85] The statute was also more permissible regarding the use of pen registers and trap-and-trace devices, which allow investigators to see which numbers have

[76] Foreign Intelligence Surveillance Act of 1978, Pub. L. No. 95-511, 92 Stat. 1783 (codified as amended at 50 U.S.C. 1801-1811, 1821-1829, 1841-1846 (1994 & Supp. II 1996 & Supp. III 1997)).
[77] *See* 50 U.S.C. 1801 (a)-(c).
[78] *See* 50 U.S.C. 1805 (a) (3).
[79] A "United States person" is defined as "a citizen of the United States [or] an alien lawfully admitted for permanent residence." *See* 50 U.S.C. 1801 (i).
[80] *See* 50 U.S.C. 1801 (h) (1-4) (requiring "minimization" procedures in FISA).
[81] *See* 50 U.S.C. 1805 (f) (1-2).
[82] *See* 50 U.S.C. 1802 (a).
[83] *See* 50 U.S.C. 1802 (a).
[84] Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA PATRIOT Act), Pub. L. No. 107-56, 115 Stat. 272 (2001).
[85] USA PATRIOT Act 206.

been dialed or received on a specific phone.[86] In addition, the statute made less strict the requirement that foreign intelligence gathering must be the "primary" goal of the surveillance. Under the Patriot Act the gathering of foreign intelligence must only be a "significant" goal of the surveillance.[87]

C. Beyond Wiretaps: *Katz* and the Evolution of New Surveillance Measures

Katz marked a new direction for the Court. Having decoupled the link between Fourth Amendment privacy and common law notions of trespass, the Court created a novel lens through which to view expectations of privacy. However, *Katz* left open the question of precisely what privacy expectations were "reasonable" in an age of modern criminal surveillance. This was an issue the Court repeatedly confronted in the latter part of the twentieth century in cases involving pen registers, aerial surveillance and mapping tools, radio transmitters, and sense-enhancing technology.

i. Pen Registers (1979)

In one of its most important decisions after *Katz*, the Supreme Court had to decide in *Smith v. Maryland* whether police use of pen registers without a search warrant was constitutionally permissible under the Fourth Amendment.[88] A pen register is a technical device that allows investigators to monitor the numbers dialed from a specific phone.[89] In *Smith*, a pen register was put in place after a victim of a burglary received harassing calls from the man suspected of committing the burglary. [90] The suspect argued that the use of the pen register violated his Fourth Amendment rights.[91]

[86] USA PATRIOT Act 216.
[87] USA PATRIOT Act 218.
[88] 442 U.S. 735 (1979).
[89] *Id.* at 736 n.1.
[90] *Id.* at 737.
[91] *Id.*

The Supreme Court rejected this argument.[92] Essential to the Court's finding was the fact that only the phone numbers dialed, not the contents of his conversations, were monitored.[93] Applying *Katz*, the Court analyzed whether the suspect in the case had a reasonable expectation of privacy that the numbers dialed on his home phone would not become public.[94] The Court found that pen registers were readily distinguishable from the wiretap in *Katz* because they could not reveal the content of conversations.[95] The Court expressed doubt that a reasonable person would expect that phone numbers dialed from his home phone would remain private because the telephone company issued a monthly bill listing all numbers dialed from a particular phone.[96] In addition, it was impossible for a person to dial a phone number without the telephone company knowing about it.[97]

Moreover, the Supreme Court found it inconsequential that that the telephone calls in question were made from the suspect's home.[98] The location from which the suspect placed the phone calls might be relevant in a case where investigators monitored the contents of a phone conversation, but not in the present case in which only the numbers dialed were seized.[99] Accordingly, the Court ruled that there was no reasonable expectation of privacy in the numbers dialed from one's home phone.[100]

ii. Radio Transmitters (1983-1984)

In *U.S. v Knots*, the Supreme Court addressed the issue of whether the use of a battery-operated radio transmitter, or beeper, to trace the movements of a criminal defendant constituted an unlawful search under the Fourth Amendment.[101] In *Knots*, police officers

[92] *Id.* at 740-41.
[93] *Id.* at 741.
[94] *Id.* at 740.
[95] *Id.* at 741.
[96] *Id.*
[97] *Id.* at 743.
[98] *Id.*
[99] *Id.*
[100] *Id.*
[101] 460 U.S. 276 (1983).

planted a beeper on a container of chloroform that was subsequently sold to the defendant.[102] The chemical company that retailed the chloroform had granted permission for the beeper's placement. [103] With the aid of the device, which emits periodic signals that can be picked up by a radio receiver, the police were able to monitor the movements of the defendant in his car after he placed the can of chloroform inside.[104] Police followed the defendant home, after which the beeper was no longer used.[105]

In finding that the use of the radio transmitter did not constitute a search under the Fourth Amendment, the Supreme Court noted that "a person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[106] Also dispositive was the police's limited use of the signals from the beeper.[107] Although the beeper enabled officers' to find the defendant's home when their own visual observations failed them because they lost sight of defendant's car on the highway, the Court found that the use of visual surveillance and a radio transmitter in this context were qualitatively the same.[108] The Court explained that "[n]othing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case."[109]

In *U.S. v. Karo*, the issue of radio transmitters in police work was once again brought before the Supreme Court.[110] Here, the Court addressed the question of whether police use of a beeper to monitor defendants' movements constituted a search under the Fourth Amendment when it revealed information not obtainable through visual surveillance.[111] Like police officers in *Knotts*, officials in *Karo* used a beeper on a chemical can to follow the

[102] *Id.* at 278.
[103] *Id.*
[104] *Id.*
[105] *Id.* at 278-279.
[106] *Id.* at 281.
[107] *Id.* at 284.
[108] *Id.* at 282.
[109] *Id.*
[110] 468 U.S. 705 (1984).
[111] *Id.* at 707.

defendant home.[112] However, in *Karo*, the officers also used the beeper's signals to trace the container's location within the defendant's residence, as well as a co-conspirator's residence, and eventually a commercial storage facility.[113] At no time had the officers been able to rely on visual surveillance to track the container as it moved between these locations.[114]

The Court rejected arguments that the mere transfer of a can containing a beeper to the defendant implicated any privacy interests.[115] Rather, the Court found troublesome the use of the beeper in a private residence, "a location not open to visual surveillance."[116] The Court explained that "private residences are places in which the individual normally expects privacy free of governmental intrusion not authorized by a warrant."[117] In finding that the use of the beeper in a private abode constituted a search, the Court concluded that "indiscriminate monitoring of property that has been withdrawn from public view would present far too serious a threat to privacy interest in the home to escape entirely some sort of Fourth Amendment oversight."[118]

iii. Aerial Surveillance (1986-1989)

In a pair of companion cases in 1986, the Supreme Court for the first time addressed the issue of whether aerial observations from high altitudes constituted a search within the meaning of the Fourth Amendment. In both cases, one involving a fenced-in backyard and the other an industrial complex, the court found that no search had taken place. In *California v. Ciraolo*, police officers trained in marijuana identification flew a private airplane over the defendant's house at an altitude of 1,000 feet and identified marijuana plants growing in the yard.[119] The cannabis could be seen with the naked eye and police officers photographed the

[112] *Id.* at 708.
[113] *Id.*
[114] *Id.*
[115] *Id.* at 712.
[116] *Id.* at 714.
[117] *Id.*
[118] *Id.* at 716.
[119] 476 U.S. 207, 209 (1986).

plants with a standard 35mm camera.[120] Applying *Katz*, the Court analyzed whether (1) the defendant had manifested a subjective expectation of privacy in the object of the challenged search, and (2) society was willing to recognize that expectation as reasonable.[121]

The Court found that the defendant did not have a reasonable privacy expectation in his backyard, despite the fact that he had taken measures to restrict the area from public view by surrounding it with a ten-foot fence.[122] The Court reasoned that that this barrier might have created some sphere of privacy from "normal sidewalk traffic," but it did not necessarily entitle the defendant to "a subjective expectation of privacy from *all* observations of his backyard."[123] Moreover, because any member of the flying public could have seen everything that the officers observed from their plane, no reasonable expectation of privacy existed.[124] The Court explained that the "Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares."[125] Noting that private and commercial flight had become "routine," the Court concluded that the defendant's expectation that the Fourth Amendment protect him from naked-eye observations from an altitude of 1,000 feet was unreasonable.[126]

In the companion case, *Dow Chemical v. U.S.*, the Court addressed the issue of whether the use of a precision aerial mapping camera from an airplane flying in public air space constituted a search under the Fourth Amendment.[127] As part of a government investigation, the Environmental Protection Agency (EPA) had taken aerial photographs of a 2,000-acre industrial complex from altitudes of 12,000, 3,000, and 1,200 feet.[128] In finding that no illegal search had taken place, the Court emphasized the fact that the complex was "*not* an area immediately adjacent to a private home, where privacy expectations are most

[120] *Id.* at 209.
[121] *Id.* at 211.
[122] *Id.*
[123] *Id.* at 212.
[124] *Id.* at 213-214.
[125] *Id.* at 213.
[126] *Id.* at 215.
[127] 476 U.S. 227 (1986).
[128] *Id.* at 229.

heightened."[129] The Court found that "the intimate activities associated with family privacy and the home and its curtilage simply do not reach the outdoor areas or spaces between structures and buildings of a manufacturing plant."[130]

The Court also considered the fact that the aerial mapping camera provided the EPA with "more detailed information than naked-eye views."[131] However, because the details observed remained limited to an outline of the facility's buildings and equipment, this factor did not prove troubling to the Court.[132] The Court reasoned that "the mere fact that human vision is enhanced somewhat, at least to the degree here, does not give rise to constitutional problems."[133] The Court conceded, however that "that surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public, such as satellite technology, might be constitutionally proscribed absent a warrant."[134]

Three years later, the Court again addressed the issue of aerial surveillance in *Florida v. Riley*.[135] In a case reminiscent of *Ciraolo*, the Court evaluated whether a police officer making naked eye observations of a greenhouse located within the curtilage of a mobile home from a helicopter at an altitude of 400-feet violated the Fourth Amendment by failing to secure a warrant.[136] A plurality found that no warrant was required even though the occupant had a subjective expectation of privacy.[137] Citing *Ciraolo*, the plurality noted that "private and commercial flight [by helicopter] in the public airways is routine" and that the occupant "could not reasonably have expected that his greenhouse was protected from public or official observation from a helicopter had it been flying within the navigable airspace for fixed-wing

[129] *Id.* at 237 n. 4.
[130] *Id.* at 236.
[131] *Id.* at 238.
[132] *Id.*
[133] *Id.*
[134] *Id.*
[135] 488 U.S. 445 (1989).
[136] *Id.* at 447-448.
[137] *Id.* at 449.

aircraft."[138] In addition, because the surveillance revealed no intimate details, the plurality found that no Fourth Amendment violation had occurred.[139]

iv. Sense-Enhancers (2001)

In *Kyllo v. U.S.,* the Court addressed the issue of whether the warrantless use of sense-enhancing technologies violated the Fourth Amendment.[140] Specifically, the case presented the question of whether the use of a thermal-imaging device aimed at a private residence from a public street to detect relative amounts of heat within the home constituted a search.[141] The Court held that it did.[142]

In *Kyllo*, police officers used a thermal imager to investigate whether the defendant was cultivating marijuana in his home. Thermal-imaging devices detect the infrared radiation that virtually all objects emit, but which are not visible to the naked eye.[143] Because indoor marijuana cannot generally be grown without the assistance of high-intensity lamps, investigators used thermal-imaging technology to determine whether the amount of heat emanating from the defendant's residence was consistent with the use of these lamps.[144] In its analysis, the Court emphasized the fact that police officers conducted "more than a naked-eye surveillance of a home."[145] The Court noted that because investigators used the sense-technology to obtain "information regarding the interior of the home that could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,'" the act constituted a search.[146] The Court distinguished *Kyllo* from *Dow Chemical*, noting that the use of aerial photography in *Dow Chemical* did not constitute a search in part

[138] *Id.* at 450-451.
[139] *Id.* at 452.
[140] 533 U.S. 27 (2001).
[141] *Id.* at 29.
[142] *Id.* at 35, 40.
[143] *Id.* at 29.
[144] *Id.*
[145] *Id.* at 33.
[146] *Id.* at 34 (citing *Silverman*, 365 U.S. at 512).

because the target of surveillance was an industrial complex, not a private residence.[147] The fact that the technology was "not in general use" was also a factor in the Court's analysis.[148]

D. Summary

The Supreme Court after *Katz* has focused on three primary elements in order to answer the question of whether a state actor has exceeded the limits of the Fourth Amendment in cases involving new investigative technologies. First, what is the target of the surveillance? It is plain that a person's living quarters receive greater protection than a commercial property. Second, what type of information is revealed in the surveillance? Where technical surveillance reveals intimate or private details, it is more likely that someone's Fourth amendment privacy has been invaded. Third, what is the nature of the technical means used? Investigative technologies that are broadly used and well known lead to a lower expectation of privacy than those that are less well known or not generally available to the public.

[147] *Id.* at 33.
[148] *Id.* at 34.

II. Germany

A. The Basic Law

i. The Applicable Basic Rights

Like the U.S. Constitution, Germany's *Grundgesetz* [Basic Law or Constitution] does not create a general right to privacy.[149] Rather, privacy interests are protected primarily through four constitutional provisions: the inviolability of human dignity under Article 1 of the Basic Law,[150] the right to personality under Article 2(1),[151] the privacy of post and telecommunications under Article 10,[152] and the guarantee of the home's inviolability under Article 13.[153]

Articles 1 and 2(1) have been at the center of Germany's privacy cases for the past three decades. Article 1 of the Basic Law declares: "Human dignity shall be inviolable. To respect and protect it shall be the duty of all state authority."[154] Under Article 1, the state has an affirmative obligation to create the conditions that foster and uphold human dignity.[155] A person shall not be made into a "mere object" of the state. [156] The protection of human dignity is the most important of all the Basic Rights,[157] and Article 1 of the Basic Law cannot be amended or removed.[158] The drafters of Germany's Basic Law, responding to the horrors of National Socialism, hoped that the placement of human dignity at the center of Germany's constitutional order would act to prevent the replication of torture, humiliation, and other

---

[149] Michael Sachs, *Grundgesetz Kommentar*, 3. Aufl., München 2003, Art. 10 Rn. 6; Walter Schmitt Glaeser, "Schutz der Privatsphäre," in *Handbuch des Staatsrechts*, Band VI (Hrsg. Josef Isensee und Paul Kirchhof) 2. Aufl., Heidelberg 2001, Rn. 2.
[150] *Grundgesetz* [Basic Law] art. 1, para. 1-2.
[151] *Grundgesetz* [Basic Law] art. 2, para. 1-2.
[152] "Privacy of letters, posts, and telecommunications shall be inviolable. Restrictions may only be ordered pursuant to a statute. Where a restriction serves to protect the free democratic basic order or the existence or security of the Federation, the statute may stipulate that the person affected shall not be informed of such restriction and that recourse to the courts shall be replaced by a review of the case by bodies and auxiliary bodies appointed by Parliament." *Grundgesetz* [Constitution] art. 10, para. 1-2.
[153] "The home is inviolable. Searches may be ordered only by a judge or, in the event of danger in delay, by other organs as provided by law and may be carried out only in the form prescribed by law. Otherwise, this inviolability may be encroached upon or restricted only to avert a common danger or a mortal danger to individuals, or, pursuant to a law, to prevent imminent danger to public security and order, especially to alleviate the housing shortage, to combat the danger of epidemics or to protect endangered juveniles." *Grundgesetz* [Basic Law] art. 13, para. 1-3.
[154] *Grundgesetz* [Basic Law] art. 1, para. 1.
[155] James J. Killean, *Der Große Lauschangriff: Germany Brings Home the War on Organized Crime*, 23 Hastings Int'l & Comp. L. Rev 173, 186 (2000); Horst Dreier, *Grundgesetz Kommentar*, 2. Aufl., 2004, Art. 1 I Rn. 136ff; Hermann v. Mangoldt & Friedrich Klein, *Kommentar zum Grundgesetz*, 5. Aufl., München 20005, Art. 1 I Rn. 40ff.
[156] Mangoldt/Klein, Art. 1 I Rn. 17; Sachs, Art. 1 Rn. 13ff.
[157] Dreier, Art. 1 I Rn. 40ff; Mangoldt/Klein, Art. 1 I Rn. 10.

atrocities that had plagued Germany in the past.[159] Since its creation, the human dignity clause has been invoked in a wide range of contexts, including cases involving life imprisonment,[160] abortion,[161] and free expression.[162]

Article 1 is closely linked to Article 2's personality clause. Articles 2(1) states that "every person shall have the right to free development of his personality insofar as he does not violate the rights of others or offend against the constitutional order or the moral law."[163] Paragraph 2 continues: "Every person shall have the right to life and physical integrity. Freedom of the person shall be inviolable. These rights may be interfered with only pursuant to a law."[164] Thus, the right to personality, unlike the human dignity clause, is not absolute, and it does not impose upon the state an affirmative obligation to create the conditions necessary for its realization.[165] The Federal Constitutional Court has held that the personality clause should be invoked only when intrusive state action is at stake.[166]

Article 2(1) has been interpreted as guaranteeing a general freedom of action and, in conjunction with Article 1, as a general right to personality.[167] The first part of Article 2(1) protects the right to act or refrain from acting as one pleases.[168] The latter part ensures a general existential space in which an individual can freely develop his or her personality, without consideration of societal expectations.[169] The right to personality also includes a right to „informational self-determination," which gives an individual the right to control when and under what circumstances his personal data is made public or shared.[170]

---

[158] Dreier, Art. 1 I Rn. 43; Mangoldt/Klein, Art. 1 I Rn. 1, 14.
[159] *See* Ernst Benda, "Fifty Years of Basic Law, The New Departure for Germany," 53 SMU L. Rev. 443, 445 (2000); Dreier, Art. 1 I Rn. 22, 39; Mangoldt/Klein, Art. 1 I Rn. 1. *See also* David P. Currie, *The Constitution of the Federal Republic of Germany* 11 (1994).
[160] *See Life Imprisonment Case*, 45 BverfGE 187 (1977).
[161] *See Abortion I Case,*39 BverfGE I (1975); *Abortion II Case* (1993), 8 BverfGE 203 (1993).
[162] *See Mephisto Case*, 30 BverfGE 173 (1971).
[163] *Grundgesetz* [Basic Law] art. 2, para. 1.
[164] *Grundgesetz* [Basic Law] art. 2, para. 2.
[165] *See* Killean, *supra* note 155, at 189.
[166] *Id.*
[167] Dreier, Art. 2 I Rn. 23; Mangoldt/Klein, Art. 2 I Rn. 8ff.
[168] Dreier, Art. 2 I Rn. 23ff; Sachs, Art. 2 I Rn. 43ff.
[169] Dreier, Art. 2 I Rn. 70; Mangoldt/Klein, Art. 2 I Rn. 85.
[170] Dreier, Art. 2 I Rn. 78; Mangoldt/Klein, Art. 2 I Rn. 114ff; Currie, 320.

Article 2(1) generally has been interpreted in light of Article 1.[171] The prevalent view among German constitutional scholars is that an individual must be given broad freedom to develop his personality in order to protect his dignity.[172] The sometimes controversial "sphere theory" divides different aspects of life into categories requiring different levels of constitutional privacy protection.[173] The core sphere of privacy requires absolute protection and may not be invaded because it is closely linked to human dignity, which is inviolable under Article 1.[174] The intimate sphere, which pertains to private activities that have little social relevance, receives strong, but not absolute, protection.[175] The more intense the social relevance is the less likely the activity is to receive absolute privacy protection. [176] A state invasion of the intimate sphere of privacy may occur when it is in the preponderant interest of the common good and strict principles of proportionality are followed.[177] The third level is the social sphere. Here invasions of privacy are permitted under requirements listed in Art. 2(1)(2).[178]

Article 10 shields the confidentiality of certain communications. Specifically, it protects the privacy of postal and telecommunications. Protected postal communications include the contents of letters or other written correspondence.[179] In addition, Article 10 gives an individual control over how postal communications are stored, utilized or distributed.[180] Protected telecommunications include traditional phone calls, as well as all other wired and wireless communications, such as email or text messages.[181] Although the once state-owned German Telecom and German Postal Service have been privatized, these entities continue to be bound to Article 10.[182]

---

[171] Glaeser, Rn. 23; Mangoldt/Klein, Art. 2 I Rn. 57; Sachs, Art. 2 I Rn. 103.
[172] Glaeser, Rn. 23; Sachs, Art. 2 I Rn. 106.
[173] Glaeser, Rn. 34; Sachs, Art. 2 I Rn. 104.
[174] Glaeser, Rn. 35; Mangoldt/Klein, Art. 2 I Rn. 88; Bernd Wölfl, "Sphärentheorie und Vorbehalt des Gesetzes," in NVwZ 2002 Heft 01 (50).
[175] Glaeser, Rn. 36; Sachs, Art. 2 I Rn. 104.
[176] Glaeser, Rn. 37; Wölfl, S. 51.
[177] Glaeser, Rn. 37ff; Mangoldt/Klein, Art. 2 I Rn. 88; Sachs, Art. 2 I Rn. 103ff; Wölfl, S. 50.
[178] Glaeser, Rn. 37; Bodo Pieroth & Bernhard Schlink, *Grundrechte. Staatsrecht II*, 21. Aufl., Heidelberg 2005, Rn. 382.
[179] Pieroth/Schlink, Rn. 765; Mangoldt/Klein, Art. 10 Rn. 27.
[180] Dreier, Art. 10 Rn. 16. *Vgl.* Mangoldt/Klein, Art. 10 Rn. 86ff.
[181] Dreier, Art. 10 Rn. 19ff; Pieroth/Schlink, Rn. 773.
[182] Dreier Art. 10 Rn. 22ff, 83ff; Pieroth/Schlink, Rn. 762f, 768, 772, 774.

Article 13 protects the privacy of the home. This Basic Right aims to provide a fundamental living space in which an individual has the right to be let alone.[183] It preserves the right of a resident to determine who can access his home, as well as when and under what circumstances.[184] Accordingly, the inviolability of the home does not apply when the resident consents to a search or other invasion of his privacy at home.[185]

The concept of "home" or living quarters has been construed broadly to be understood as any domain of privacy, so that workspaces such as offices and curtilages such as yards or gardens are included. [186] However, Germany's Federal Constitutional Court has given workspaces such as offices a more limited level of privacy protection because of the strong social ties associated with such environments. [187]

Under Article 13(2), a home may only be searched if a search warrant is obtained. [188] Technical means may be used to surveil a home under Article 13(4) and (5) to avert acute dangers to public safety, but a search warrant must be obtained in the aftermath of the surveillance if it was not possible to obtain such an order in advance.[189] At a minimum, however, the surveillance measures must be ordered by other authorities designated by law.[190]

ii. State Curtailment of Basic Rights

According to Germany's Basic Law the state may encroach on certain Basic Rights under some circumstances. Whether a Basic Right can be limited or an encroachment of a Basic Right can be justified depends in large part on whether a reservation or caveat for that right has been expressed in the Basic Law. Additionally, a Basic Right may be limited by another Basic Right, with whose principles it collides. There are three types of Basic Rights:

[183] Dreier, Art. 13 Rn. 12; Pieroth/Schlink, Rn. 872.
[184] Dreier, Art. 13 Rn. 12; Mangoldt/Klein, Art. 13 I Rn. 2.
[185] Glaeser, Rn. 54; Sachs, Art. 13 Rn. 23.
[186] Dreier Art 13 Rn. 12; Pieroth/Schlink, Rn. 872.
[187] Glaeser, Rn. 50; Mangoldt/Klein, Art. 13 I Rn. 26, 62.
[188] Glaeser, Rn. 59; Mangoldt/Klein, Art. 13 I Rn. 71, 75.
[189] Mangoldt/Klein, Art. 13 I Rn. 134; Sachs, Art. 13 Rn 46.
[190] Mangoldt/Klein, Art. 13 I Rn. 133; Pieroth/Schlink, Rn. 884.

those with simple reservations, those with qualified reservations and those without reservations.

A simple reservation states that a Basic Right may be encroached only by statute.[191] Article 10(2)(1), which states that restrictions to the privacy of postal and telecommunications "may be ordered only pursuant to a law," is an example of such a reservation. It is to be distinguished from the second sentence in Article 10(2), which is viewed by German constitutional scholars as an exception rather than a reservation. That sentence allows the state to undertake exceptional measures to protect the Constitution and the state. [192]

A qualified reservation requires not only a statute to limit a Basic Right, but mandates that the law be based on specific circumstances, serve a specific purpose, or use specific means.[193] Article 13 includes several qualified reservations.[194] Article 13(2), for example, permits searches as long as search warrant is obtained from a judge. Article 13(3) permits the use of technical measures to surveil suspects where specific facts can support that a suspect has committed a particularly severe crime. The use of technical measures is, however, limited so that they are only permitted with judicial order and where other investigative means would be particularly difficult or pointless. Article 13(4) and (5) permit acoustic surveillance for the purpose of preventing immediate danger. Article 13 is also qualified by Article 17a(2), which states that the inviolability of the home can be revoked by law in order to defend the country, including to protect the civilian population. [195]

If a Basic Right is not limited by an express or qualified reservation, then it may only be limited by colliding Basic Rights of third parties.[196] A conflict between two constitutional rights or principles will generally be resolved by weighing the rights against one another with the hope that a "practical concordance" will be reached.[197] Article 1, which declares human dignity inviolable, is an example of a Basic Right that has no reservation. Unlike other Basic

[191] Dreier Vorb. Rn. 136; Pieroth/Schlink, Rn. 253; Sachs, Vor Art. 1 Rn. 115.
[192] Dreier, Art. 10 Rn. 56ff; Mangoldt/Klein, Art. 10 Rn. 64.
[193] Dreier Vorb. Rn. 136; Pieroth/Schlink, Rn. 255; Sachs, Rn. Vor Art. 1 Rn. 116.
[194] Dreier, Art. 13 Rn. 29ff; Sachs, Art. 13 Rn. 25ff.
[195] Dreier, Art. 13 Rn. 48; Mangoldt/Klein, Art. 17a Rn. 36ff; Sachs, Art. 17a Rn. 26.

Rights, however, the inviolability of human dignity cannot be compromised or weighed against another Basic Right.[198] In addition, Article 1 is further strengthened because Article 79(3) prohibits its alteration or abolition.[199]

Similarly, Article 2(1) is an exception in this context. Article 2 is generally seen as a Basic Right that includes a simple reservation because it requires that the right to personality be preserved only in so far as it does not disturb the constitutional order.[200] Notably, however, encroachments on the right to personality that impact the core sphere of privacy are only permissible where constitutional rights collide.[201]

iii. Justifying State Encroachments on Basic Rights

Reservations permit the legislature to encroach on Basic Rights where necessary. However, legislators are subject to their own constitutional limitations in exercising this right. These so-called *Schranken-Schranken* [or "limits on limits," the restrictions that govern to what extent Basic Rights may be restricted] arise from Articles 19 and 20 of the Basic Law.

Article 19 lists several conditions that must be met when legislators limit Basic Rights. Under Article 19(1)(1), a statute that restricts a Basic Right must be a general and abstract rule.[202] Article 19(1) also requires that the legislature name the Basic Right in the law that limits it.[203] This *Zitiergebot* ["citation requirement"] aims to warn and inform the legislature and the public at large that a Basic Right is being impacted.[204] Finally, a Basic Right may in no case be limited so that its essential content or character is defeated.[205] This is known as the *Wesenhaltsgarantie* ["guarantee of the essential"].

---

[196] Dreier Vorb. Rn. 139ff, 158; Sachs, Vor Art. 1 Rn. 120.
[197] Pieroth/Schlink, Rn. 321; Sachs, Vor Art. 1 Rn. 124.
[198] Dreier, Art. 1 Rn. 44, 132ff; Mangoldt/Klein, Art. 1 I Rn. 61, Sachs Art. Rn. 6, 10ff.
[199] Dreier, Art. 1 Rn. 43; Sachs , Art. 79 para. 3 Rn. 30ff.
[200] Pieroth/Schlink, Rn. 383; Sachs, Art. 2 Rn. 90.
[201] Glaeser, Rn. 37; Wölfl, S. 50.
[202] Pieroth/Schlink, Rn. 307; Sachs, Art. 19 Rn. 20ff.
[203] Pieroth/Schlink, Rn. 310; Sachs, Art. 19 Rn. 25ff.
[204] Pieroth/Schlink, Rn. 310; Sachs, Art. 19 Rn. 26.
[205] Mangoldt/Klein, Art. 19 Rn. 139; Sachs, Art. 19 Rn. 9.

A law that restricts a Basic Right must follow the rule of law principles found in Article 20. Accordingly, such a law must be proportional, specific and not retroactive. The principle of proportionality requires that the statute limiting the Basic Right must have a legitimate goal for whose accomplishment it is suited and necessary.[206] A measure is considered necessary when no other means by which the state could reasonably reach the same result that would be less burdensome for the citizen.[207] Under the specificity requirement a citizen must be able to recognize what consequences his behavior could or will have. [208] The state response to certain behaviors must be predictable to avoid arbitrariness. [209] The prohibition on retroactivity prohibits state action where a legal norm or process has been so transformed that a past deed now has a different consequence than it once had.[210]

B. Privacy Rights and the Development of New Technologies

Throughout the second half of the 20th century the Federal Constitutional Court repeatedly had to address to what extent the state could invade the privacy of individual citizens and under what circumstances government encroachment on privacy could be justified. In several cases, the Court's decisions were in direct response to new developments in technology that raised new questions regarding privacy. As a result, case law developed in Germany that linked privacy protection to the inviolability of human dignity and the right to freely develop one's personality.

i. The Microcensus Case (1969)

In 1969 the Federal Constitutional Court had to address the question of whether the federal government could collect personal information for a national census. Its decision in the case was the first to link privacy rights, the right to personality, and the inviolability of

[206] Dreier, Vorb. Rn. 145ff; Sachs, Art. 20 Rn. 149ff.
[207] Dreier, Vorb. Rn. 148; Pieroth/Schlink, Rn. 285ff.
[208] Pieroth/Schlink, Rn. 312; Sachs, Art. 20 Rn. 126.
[209] Pieroth/Schlink, Rn. 312; Sachs, Art. 20 Rn. 126.
[210] Pieroth/Schlink, Rn. 295a; Sachs, Art. 20 Rn.133.

human dignity in relation to the use of new technologies. At that time the German federal government was permitted by law to collect general personal data as part of a national census. However, a 1960 amendment to the law required German citizens to provide additional information about their vacations, including the length, destination, and means of transportation used. [211] In the Microcensus Case a group of Bavarian citizens filed a suit after they were fined DM100 (approx. $50) because they refused to provide this information to federal data collectors. The claimants alleged that the questionnaire violated their privacy rights under Article 1. [212]

The Federal Ministry of the Interior countered that the survey was constitutional because it did not exceed the legitimate purpose of the census, nor would the questionnaire results be used for any other purpose than statistical compilations. [213] In addition, the ministry argued that the right to freely develop one's personality was not injured where the state interest outweighed the individual's interest in not having his privacy disturbed. [214] In this case, the ministry argued, the questions regarding vacation and relaxation were of particular interest to the state, while the invasion of privacy in the individual's intimate sphere was minimal. [215] According, the ministry argued the surveys were constitutional. [216]

The Federal Constitutional Court ruled that the federal survey did not violate human dignity and was not unconstitutional.[217] However, the Court recognized that human dignity would be offended if the individual were transformed into a "mere object" of the state. [218] It would be unconstitutional for the state to assert the right to catalogue and register every aspect of an individual's private life, even if that data was used only in the context of anonymous statistics. [219] The Court noted that in order for the individual to freely develop his personality, he must be given an inner space in which he is in full possession of himself, to which he can

[211] BVerfGE 27, 1 (3).
[212] *Id.*
[213] *Id.* at 4.
[214] *Id.*
[215] *Id.*
[216] *Id.*
[217] *Id.* at 6.
[218] *Id.*

withdraw, and to which the outer world has no access so that he can be let alone to enjoy his right to solitude. [220]

Nonetheless, the Court emphasized that not every statistical collection of personal data violated human dignity. [221] As a member of society, an individual citizen had to accept the necessity of collecting statistics under certain circumstances, such as in a census that assisted government in policy planning.[222] Determinative was whether the data collected by the state by its very nature had a secret character. [223] Where the statistical collection only measured general behavior of an individual that was related to the outside world, personality rights were not violated at the core of private being, so long as this data was maintained anonymously.[224]

The Court ruled that the case at hand did not deal with information that had by its nature a secret character. [225] Although the census questionnaire did impact an area of private life, it neither forced the respondent to reveal aspects of his intimate sphere, nor did it provide the state with information that was not otherwise available in the public domain. [226] Information about vacation destinations, the length of vacation, accommodations and transportation could be obtained through (though admittedly more difficult) other means. [227] In addition the anonymity of the information had been guaranteed, and there was no danger that the data would be misused for unforeseen purposes. [228] As a result, the Bavarian citizens' constitutional rights were not violated. [229]

ii. The Lebach Case (1973)

In 1973 the Federal Constitutional Court had to decide whether the personality rights of a convicted criminal should supersede the general interest of the public good. The suspect

---

[219] *Id.*
[220] *Id.*
[221] *Id.* at 7.
[222] *Id.*
[223] *Id.*
[224] *Id.*
[225] *Id.* at 8.
[226] *Id.*
[227] *Id.*
[228] *Id.* at 9.
[229] *Id.*

had been involved in the notorious "soldier murders of Lebach," whereby four German soldiers were killed during a burglary of an ammunition dump in 1969.[230] The two primary perpetrators were friends with the complainant and the relationship had a homosexual component.[231] During the planning of the attack, the complainant repeatedly had expressed reluctance in carrying out the deed, and he did not take part in the attack. [232] The two primary perpetrators were convicted in 1970 and received life sentences, whereas the claimant received a sentence of six years for aiding and abetting the crime.[233]

In 1972 the state-owned German television channel ZDF planned to broadcast a television drama about the Lebach murders. In an introduction to the drama, broadcasters planned to display the names and pictures of those involved in the crime. Additionally, ZDF planned to air a docu-drama in which actors would reconstruct the crime. The claimant wanted to prevent the airing of the docu-drama insofar as he (or his name) would be represented in it. [234]

The Federal Constitutional Court had to decide which of two constitutional values would take priority: the freedom of the media under Article 5 of the Basic Law or the personality rights of the convicted criminal under Article 2. The Court ruled that the complainant's constitutional rights deserved priority because the right to freely develop one's personality and protect one's dignity guarantees every individual an autonomous space in which to develop and protect his individualism.[235] The Court noted that everyone should determine independently and for themselves whether and to what extent his life and image can be publicized.[236] The Court noted, however, that not the entire area of private life fell under the protection of personality rights.[237] Where, as a member of society at large, an individual enters into communications with others or impacts them through his presence or

[230] BVerfGE 35, 202 (204).
[231] *Id.*
[232] *Id.* at 205.
[233] *Id.*
[234] *Id.*
[235] *Id.*at 220.
[236] *Id.*
[237] *Id.*

behavior and therefore impacts the private sphere of others, he limits the privacy of his own life.[238] Where such social interactions are present, the state may take certain measures to protect the public good. [239]

The Court emphasized that in most cases freedom of information would receive constitutional priority over the personality rights of a convicted criminal.[240] However, the Court found that the encroachment on the convicted criminal's personality rights should not go any further than required to satisfy what was necessary to serve the public interest, and moreover, the disadvantages for the convicted criminal should be weighed against the severity of the crime committed.[241] Using these criteria, the Court found that the planned ZDF broadcast violated the complainant's personality rights because of the way in which it named, pictured and represented him.[242]

The Court noted that the broadcast represented the complainant, who was recognizable through the facts of the story even though his name and face were not shown, in a negative and unsympathetic manner.[243] Additionally, the complainant was represented as a primary perpetrator when in actuality he aided and abetted the crime.[244] Moreover, the documentary put more emphasis on the homosexual element of the relationships between the perpetrators than the results of the trial warranted.[245] The Court also found it relevant that as a general rule television had a much stronger impact on privacy than a written or verbal report in a newspaper or radio show.[246] Finally, it was important that the ZDF broadcast did not add anything important or new to the plaintiff's story.[247]

Applying these criteria, the Court found that the ZDF report could prevent the resocialization of the plaintiff in violation of his rights under Articles 1 and 2(1) of the Basic Law. The inviolability of human dignity required that an ex-convict receive the opportunity

---

[238] *Id.*
[239] *Id.*
[240] *Id.* at 231.
[241] *Id.* at 232.
[242] *Id.* at 226.
[243] *Id.*
[244] *Id* .at 240.
[245] *Id.*at 242.
[246] *Id.* at 226.

to re-enter society once he has served his prison term and paid his dues to society.[248] The convicted criminal's resocialization was put at risk where a television broadcast was to reenact the crimes of a perpetrator near or after the time of his release from prison.[249] Moreover, ZDF's stated goal of informing the public about the effectiveness of the prosecution and the security measures taken by the German military since the attacks could be reached without identifying the complainant in the manner planned.[250]

iii. The Census Act Case (1983)

Ten years later the Federal Constitutional Court had to evaluate the constitutionality of another government census. In the Census Act Case of 1983 the Court recognized for the first time a right to informational self-determination that flowed from the general right to personality and human dignity under Articles 1 and 2(1) of the Basic Law.[251] The decision is a milestone in German privacy and data protection law.

The case addressed the constitutionality of the federal census required under a 1983 law.[252] The goal of the census was to collect information for regional planning and compare that data to the data in community registers.[253] The goal of the census was not a mere head count. Rather, it sought to collect data related to job titles, employers and residences.[254] In addition, the Federal Census Act permitted the sharing of federal data with local and state agencies.

The Federal Constitutional Court distinguished its analysis of the Federal Census Act of 1983 from the law in the *Microcensus Case* in 1979 because of the fundamental technical

---

[247] *Id.* at 234.
[248] *Id.* at 235.
[249] *Id.* at 238.
[250] *Id.* at 243.
[251] BVerfGE 65, 1.
[252] VoZählG 1983 § 9 para. 2-3.
[253] BVerfGE 65, 1 (7). Everybody living in Germany permanently or for a period of time exceeding three months has to be registered with the police. This information is stored in community registers.
[254] *Id.* at 4.

changes that had taken place in data collection and processing in 14 years.[255] Targeted information could be obtained with less effort, and smaller invasions of privacy could lead to more specific results.[256] State agencies in charge of statistical analyses had created comprehensive databases.[257] At the community level, community registries had turned into comprehensive resident databases, from which any state agency could draw upon.[258] In addition, the Court expressed concern over the fact that recipients of the census data had access to other databases, which combined with the census information, could lead to the formation of a complete and detailed picture of the lives of individual residents – a so-called "personality profile" that could include even the protected intimate sphere.[259] Individual citizens ran the risk that they could become transparent "persons of glass."[260]

In its decision the Federal Constitutional Court declared that the general personality right under Article 2(1) in connection with Article 1(1) protected individuals against the collection, storage, use, and dissemination of personal data.[261] These constitutional provisions protected the fundamental right of the individual to control the use of personal information,[262] and only the overwhelming public interest could limit this right of informational self-determination.[263] In reaching its decision, the Court emphasized that a person who could not oversee what information about himself was available in certain social spheres could be limited in his freedom to plan or make life decisions.[264]

The Court held that the legislature had a duty to comply with principles of proportionality in passing laws affecting personal data collection,[265] and that organizational and procedural measure to prevent encroachment on personality rights had to be put in

[255] *Id.* at 17.
[256] *Id.* at 18.
[257] *Id* at 17.
[258] *Id.*
[259] *Id.*
[260] *Id.*
[261] *Id.*at 1.
[262] *Id.*
[263] *Id.*at 44.
[264] *Id.* at 43.
[265] *Id.*at 44.

place.[266] The Court, however, distinguished between two types of data collection: data that was individualized, non-anonymous and had to be processed and data that was intended for statistical purposes only.[267] The latter type of data collection did not need to be linked to a specific purpose,[268] but had to be subject to certain limitations within the information system.[269]

Because the principles of specificity and proportionality were upheld in the data collection resulting from the 1983 Federal Census Act, the Federal Constitutional Court ruled that the statute did not violate human dignity. The census did not lead to an unconstitutional cataloguing or registration of human personality.[270] However, the anticipated data-sharing rules by which state and local agencies could compare information violated the personality right because they were unsuited to the statute's goal, and their breadth was incomprehensible to the ordinary citizen.[271] It was not foreseeable for persons affected that that their statistical information would be passed on to state agencies and other public authorities.[272] Accordingly, the Court held that data could only be passed on for research purposes[273] because a researcher generally was not interested in the person as an individual but rather as a carrier of specific traits.[274] Moreover, a researcher would not be able to combine such data with information from other government databases.[275]

C. Recent German Case Law

In the past ten years, German privacy law evolved rapidly as new investigative measures and technologies became increasingly popular with police and federal investigators. The Federal Census Case has proven to be particularly influential and has served as the

[266] *Id.*
[267] *Id.*at 45.
[268] *Id.*
[269] *Id.*at 48.
[270] *Id.* at 52.
[271] *Id.* at 64.
[272] *Id.* at 65.
[273] VoZählG 1983 § 9 para. 4 VZG 1983.
[274] BVerfGE 65, 1 (69).

foundation of German privacy law in several constitutional cases in the past decade. Most recently, the Federal Constitutional Court has had to determine whether wiretapping, acoustic surveillance of the home, and use of GPS surveillance were constitutional under the Basic Law.

i. Strategic Telegram Surveillance (1999)

In 1999 the Federal Constitutional Court had to decide for the first time whether the state, specifically the *Bundesnachrichtendienst* ["BND" or federal intelligence agency], could surveil international telephone and telefax communications without establishing probable cause. This so-called "strategic telegram surveillance" was made possible through a 1994 federal crime prevention statute. The law empowered the BND to surveil all non-wired international telecommunications.

The 1994 law amended a pre-existing statute that had allowed the BND to undertake similar telecommunications surveillance for strategic intelligence-gathering purposes to recognize and prevent armed attacks on the Federal Republic of Germany.[276] Following an earlier decision of the Federal Constitutional Court, the BND had only been allowed to surveil telecommunications to prevent foreign threats, not to prevent threats to domestic security.[277] The BND would surveil batches of phone conversations and use search terms to obtain information that could lead to a general understanding of the situation in a particular country or region.[278] When specific terms or area codes cropped up, the BND would collect the data associated with these. However, the agency was not allowed to make note of individual phone numbers or callers and the information had to remain anonymous. In addition, the

[275] *Id.*
[276] BVerfGE 100, 313, at para. 3.
[277] BVerfGE 67, 157 (2004).
[278] BVerfGE 100, 313, at para. 9.

BND had to follow a so-called "no disadvantage" rule which mandated that collected data could not be used to the disadvantage of an individual (e.g., in a criminal proceeding).[279]

The 1994 amendment broadened the power of the BND to surveil non-wired international telecommunications without probable cause to investigate serious crimes, [280] such as arms and drug trade, counterfeiting, money laundering, and terrorism,[281] if they could be connected to a risk of attack on Germany.[282] Additionally, the legislature abandoned the "no disadvantage" rule that had previously protected individuals from the misuse of their private information.[283] The amended law also permitted the BND to use any data collected in the surveillance to prevent or prosecute any of the above-described crimes and to share the information with a number of government agencies, including the customs office, government prosecutors, and police authorities, insofar as it was necessary for them to fulfill their duties.[284]

The complainants in the constitutional case were several individuals who used means of international communications for professional reasons. One complainant was a university professor researching narcotics law who frequently placed telephone calls and sent and received faxes to and from abroad.[285] Additionally, several journalists and one newspaper publisher who regularly phoned or faxed abroad as part of their reporting duties filed complaints.[286]

The complainants claimed that the law itself, as well as the surveillance of their communications, violated their Basic Rights under Article 10 and Article 1 in conjunction with Article 2(1).[287] The complainants found particularly troublesome the fact that the collection of their data was taking place without any showing of probable cause[288] and that the mere use of a search term could trigger surveillance.[289]

---

[279] *Id.* at para. 4.
[280] *Id.* at para. 6, 8.
[281] *Id.* at para. 6.
[282] *Id.* at para. 8.
[283] *Id.* at para. 10.
[284] *Id.*
[285] *Id.* at para. 50, 150.
[286] *Id.* at para. 65, 76, 77, 151.
[287] *Id.* at para. 50, 72, 79.
[288] *Id.* at para. 55.
[289] *Id.*

The Federal Constitutional Court in large part approved the 1994 law, but held a few provisions of the statute unconstitutional.[290] The Court emphasized that the surveillance of international telecommunications indeed was a large encroachment on the right of secrecy of telecommunications under Article 10 of the Basic Law. However, the Court noted that limitations on this right were permissible to protect highly valued public interests if the purposes of the encroachment were precisely defined and the dissemination of the data collected was limited.[291] But the 1994 law did not meet these criteria fully. The Court found that the BND could continue its surveillance without probable cause, but the dissemination of collected data had to be limited, the notification of the individual affected improved, and the parliamentary oversight improved.[292]

In its decision, the Court relied explicitly on its *Census Act* decision of 1993 and applied the reasoning of that case to the special guarantees of the Basic Law's Article 10.[293] The Court stated that the free communication that Article 10 guaranteed would suffer if individuals feared that the state could use the circumstances or contents of a communication abroad against the participant in a different context.[294] Accordingly, the Court found that the protection of Article 10 extended not just to the communications themselves, but to the data processing measures to which the communications were subject.[295] Because the dissemination of the strategically collected data leads to an increase in the number of people who know and can make use of the communications collected, the Court mandated that better safeguards in regard to dissemination be put in place.[296] Agencies should not have access to the full database of "strategically" obtained information,[297] and the data that is passed on should be labeled as such. [298]

[290] *Id.* at para. 84.
[291] *Id.* at para. 165.
[292] *Id.* at para. 261.
[293] *Id.* at para. 164.
[294] *Id.* at para.163.
[295] *Id.*
[296] *Id.* at para. 190.
[297] *Id.* at para. 262.
[298] *Id.* at para. 284.

The Court held that individuals who have been surveilled must be informed in the aftermath of the surveillance.[299] This was the only way to ensure that such individuals could defend their interests and turn to the courts if necessary.[300] The destruction of strategically collected data should only be allowed after the individual affected by the data has consented.[301] If the individual did not consent to destruction, then his or her data should be handed over to the individual.[302] The Court found that the current rule requiring no notification where data was destroyed within three months was insufficient[303] because the mere running of time could not ensure that the collected data was not misused during that period.[304] An exception to the notification requirement was permissible only in very limited circumstances, e.g., if notification would endanger an ongoing investigation.[305] Finally, the Court held that the parliamentary oversight needed to be strengthened. The legislature had to be able to oversee the entire data collection and evaluation process. The Court noted that the individual's ability to take legal action could not depend solely only on the fact that he was notified of the surveillance.[306]

[299] *Id.* at para. 287.
[300] *Id.* at para. 72.
[301] *Id.*
[302] *Id.*
[303] *Id.* at para. 290.
[304] *Id.* at para. 292.
[305] *Id.* at para. 288.
[306] *Id.* at para. 298.

ii. The "Large Eavesdropping Attack" Case (2004)

In 1998, the German parliament revised Article 13 of the Basic Law to permit the use of electronic surveillance to monitor private homes. The legislation was part of a larger attempt to fight organized crime, whose rapid growth in the 1990s due to an influx of sophisticated crime groups from the former Soviet Bloc countries had alarmed German politicians.[307] The law was controversial from the outset, with supporters describing it as a necessary tool in the fight against organized crime and detractors calling it an attack on civil liberties.[308] The debate was complicated by the fact that amendments to the Basic Law require a 2/3 majority in both chambers of parliament, the *Bundestag* and the *Bundesrat*.[309] Nonetheless, after seven years of controversy and thorny debate, the *Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität* [Law to Fight Illegal Drug Trafficking and Other Manifestations of Organized Crime] became law by the narrowest of margins. The so-called "Großer Lauschangriff" ["large eavesdropping attack"] passed in the *Bundestag* by four votes and by one vote in the *Bundesrat*.[310]

The new law permitted police authorities to listen and record private speech on private premises under certain conditions without the knowledge of the targeted person.[311] Well-founded evidence facts had to indicate that the target had committed one or more of a series of enumerated high crimes, such as murder, treason, or money laundering.[312] Moreover, alternate means of establishing the facts or determining the perpetrator's whereabouts had to be disproportionately more difficult or offer no prospects of success.[313] Acoustic surveillance could take place at the accused's home or on another person's premises

[307] *See* Killean, *supra* note 155, at 173; Jutta Stender-Vorwachs, "The Decision of the Federal Constitutional Court of March 3, 2004 Concerning Acoustic Surveillance of Housing Space," 5 German L.J. 1337, 1340 (2004).
[308] *See* Killean, *supra* note 155, at 173-174; Stender-Vorwachs, *supra* note 307, at 1341.
[309] *See* Killean, *supra* note 155, at 199; Stender-Vorwachs, *supra* note 307, at 1341.
[310] *See* Killean, *supra* note 155, at 199-200.
[311] § 100(c)(1)(3) StPo.
[312] § 100(c)(1)(3)(a-f) StPo.

if applying the measure on the accused's premises alone would not enable investigators to establish the perpetrator's whereabouts or other sought-after facts sufficiently and if other means of establishing the facts or determining the accused's whereabouts would be disproportionately more difficult or offered no prospects of success.[314] Finally, the measures could be implemented even if they unavoidably involved third persons.[315]

On March 3, 2004, the Federal Constitutional Court declared significant portions of the law unconstitutional.[316] Specifically, the Court found that certain provisions of the surveillance laws infringed upon the guarantees of human dignity and the inviolability of the home under Articles 1 and 13 of the Basic Law. In its ruling, the Court emphasized the interrelationship between human dignity, the right to personality, and the inviolability of the home, noting that all citizens were entitled to a sphere of intimacy in which to conduct private conversations without fear of government intrusion.[317] The Court described the home as "last refuge" for the development of one's personality and preservation of one's dignity — the place where one's innermost perceptions, thoughts, and opinions emerge.[318] The Court noted that persons may be able to forego writing letters or making telephone calls to preserve their privacy, but asserted that the right to retreat into one's home was absolute.[319] Because acoustic surveillance of the home implicated privacy rights so fundamentally, the Court framed the question not as whether evidence gathered through such means should be admissible in court, but whether such an investigative measure should be permitted at all.[320]

In its inquiry, the Court found that particularly intimate types of communications should be constitutionally safeguarded in all but exceptional cases. The Court created a protected category of communications that included conversations between close family

---

[313] § 100(c)(1)(3) StPo.
[314] § 100(c)(2) StPo.
[315] § 100(c)(3) StPo.
[316] BVerfG, 1 BvR 2378/98 (2004).
[317] *Id.* at para. 119-120.
[318] *Id.* at para. 120.
[319] *Id.* at para. 54.

members or other persons of trust, such as members of the clergy, physicians, and criminal defense attorneys.[321] Under the Court's decision, government officials may monitor these conversations only if concrete evidence exists at the time an eavesdropping warrant is issued that at least one of the persons speaking is or was involved in a criminal offense.[322] Moreover, the government must show that the crime was particularly serious[323] and that there is strong reason to believe that the content of conversation will not be of the protected type described above.[324] Finally, acoustic surveillance of a private residence may take place only if and so long as the person being monitored is on the premises.[325]

Thus, government surveillance of private conversations is permissible so long it is unlikely to touch on the absolutely protected private sphere. But conversations about the commission of past, present, or future crimes are not protected.[326] If government surveillance unexpectedly touches upon absolutely protected personal information, it must be halted immediately.[327] Any recordings made must be destroyed, and data collected cannot be used in criminal prosecutions.[328]

---

[320] *Id.* at para. 61.
[321] *Id.* at para.148.
[322] *Id.* at para. 126-127.
[323] *Id.* at para. 126.
[324] *Id.* at para. 132.
[325] *Id* at para. 127.
[326] *Id.* at para. 137.
[327] *Id.* at para. 152.
[328] *Id.* at para. 186.

iii. The Global Positioning System Case (2005)

The Constitutional Court gave the German legislature until June 2005 to amend the law to comply with the court's "Large Eavesdropping Attack" decision.[329] But before the legislature had a chance to respond, a second case involving the 1992 law against organized crime[330] came before the Court. This time, the Constitutional Court considered the question of whether government investigators could use global positioning system (GPS) technology in investigations and whether such measures conflicted with Articles 1 and 2 of the Basic Law.

In addition to permitting the acoustic surveillance of homes, the 1992 law had expanded the types of investigative measures law enforcement officials could undertake. One provision of the new law,[331] which was integrated into the Code of Criminal Procedure as § 100c StPO, permitted the taking of photographs and visual recordings without the knowledge of the person that was the subject of the surveillance.[332] In addition, the provision permitted, under certain conditions, the use of "other special technical measures" for the purposes of surveillance to establish the facts of a case or to determine the whereabouts of a perpetrator.[333] Such measures were permissible where the investigation concerned a criminal offense of considerable importance, and other means of establishing the facts or determining the perpetrator's whereabouts were considerably less promising or more difficult.[334]

An amendment to the law that came into effect on November 1, 2000 further expanded the investigative powers of the police by allowing for long-term surveillance of suspects.[335] Under § 163f StPO, in investigations concerning a criminal offense of considerable importance, the surveillance of suspects was allowed take longer than twenty-four hours and could take place on more than two days so long as other means of establishing the facts or

[329] *Id.* at para. 352.
[330] *Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität*, of 15 July 1992 (BGBI. 1992, p. 1302).
[331] § 100c StPO.
[332] § 100c StPO (1)1a.
[333] § 100c StPO (1)1b.
[334] § 100c StPO (1)1b.

determining the perpetrator's whereabouts would be considerably less promising or would be more difficult.[336] Such surveillance had to be approved by a criminal prosecutor.[337] For surveillance periods of longer than one month, an order had to be obtained from a judge.[338]

In the *Verfassungsbeschwerde* [constitutional complaint] that led to the Court's April 12, 2005 decision, the claimant, Bernhard Falk, argued that the use of GPS by police investigators violated his rights under Articles 1(1) and 2(1) of the Basic Law.[339] Falk, a member of the left extremist group *Antimperialistische Zelle* [Antimperialist Cell] who has since converted to Islam and now uses the surname Uzun, had been investigated for his use of explosives against German political parties in furtherance of his political cause as early as 1985. In 1999, he was convicted on four counts of attempted murder and was convicted to thirteen years in prison.[340] Criminal proceedings took place before the *Oberlandsgericht* (OLG – Highest Regional Criminal Court) in Düsseldorf, and the court depended heavily on surveillance evidence collected by police investigators in convicting Falk.[341]

In addition to traditional observation methods that included video, telephone, and mail surveillance, police investigators placed a GPS receiver on the claimant's car. Through a system of satellite signals and computers, GPS technology can be used to determine the latitude and longitude of a receiver on Earth. Using this technology, police investigators were able to pinpoint the location of the claimant's vehicle within a 50-meter radius for a period of approximately 10 weeks. The claimant alleged that the use of GPS surveillance violated his fundamental right to privacy and exceeded the legal boundaries set by § 100c StPO 1(1b). In addition, Falk claimed that the use of GPS, coupled with the other observation methods, cumulatively constituted an unconstitutional invasion of his privacy.

---

[335] *See* § 163f StPO.
[336] § 163f StPO (1)1-2.
[337] § 163f StPO (3).
[338] § 163f StPO.(4).
[339] BVerfG, 2 BvR 581/01 (2005), at para. 27-29.
[340] *Id.* at para. 14.
[341] *Id.* at para. 15.

In its April 12, 2005 opinion, the Federal Constitutional Court agreed that the use of GPS technology in police investigations of crimes of considerable importance was not unconstitutional.[342] Although the Court noted that GPS surveillance did constitute an attack on the suspect's personality rights, the extent and intensity of the invasion was not at a level that violated human dignity or the untouchable core sphere of privacy.[343] The Court emphasized the usefulness of GPS technology was limited to revealing a person's location and the length of time spent in a given location, and that GPS did not function effectively in closed rooms or on streets in dense neighborhoods.[344]

In rendering its decision, however, the Court asserted that the rapid development of information technologies demanded that legislators be alert to the creation of new investigative measures that could infringe upon the constitutional right to informational self-determination.[345] Accordingly, the Court required lawmakers to be prepared to step in with corrective legislation as necessary to limit the scope of § 100c StPO should the term "other special technical measures" evolve to include technologies that overreach constitutional privacy bounds.[346]

Notably, the Court found that a *Rundumüberwachung*, or total surveillance (i.e., multiple simultaneous observations), leading to the construction of a personality profile of a suspect, would be constitutionally impermissible.[347] Nonetheless, the Court did not find that the comprehensive surveillance of Falk rose to the level of a *Rundumüberwachung* even though police periodically read the suspect's mail, tapped the suspect's phone lines, and observed his home via video.[348] The Court noted that the additional surveillance measures, which were used primarily on the weekends, merely supplemented the GPS surveillance.[349]

---

[342] *Id.* at para. 56.
[343] *Id.*
[344] *Id.* at para. 53.
[345] *Id.* at para. 51.
[346] *Id.*
[347] *Id.* at para. 60.
[348] *Id.* at para. 16.
[349] *Id.* at para. 67.

Moreover, the Court noted that the use of what it considered to be particularly sensitive acoustic surveillance had been very limited. [350]

As a preventative measure, the Court mandated that prosecutors be the primary decision makers regarding all investigative matters in a case and that prosecutors be informed of all investigative tools in use.[351] The Court noted that a full documentation of all completed or possible investigative measures must be recorded in the suspect's file.[352] Moreover, in order to prevent parallel surveillances of the same suspect, prosecutors from different *Länder* [federal states] should coordinate their investigative efforts through the *Verfahrenregister* [prosecutorial procedure register].[353] Similar coordination should occur between prosecutors and federal intelligence agencies.[354] The Court stated that legislators should be vigilant in regard to whether such coordination is taking place and, if not, create regulations that would prevent uncoordinated investigative measures.[355]

iv. Preventative Telecommunications Surveillance (2005)

In 2005 the Federal Constitutional Court also had to decide whether a law in the state of Lower Saxony that permitted "preventative" telephone surveillance was constitutional. The law, which went into effect in 2004, allowed state investigators to surveil the telecommunications of persons in cases where well-founded facts could support the assumption that the individual being wiretapped had committed a serious crime and that there appeared to be no other means to prosecute or prevent the crime.[356] The law covered both the content and connection data of the communication and encompassed telephone calls, faces, text messages on mobile phones, and emails.[357] Companions and contact persons could also

[350] *Id.*
[351] *Id.* at para. 62.
[352] *Id.*
[353] *Id.*
[354] *Id.* at para. 63.
[355] *Id.* at para. 64.
[356] § 33a I Nr. 2 des Niedersächsischen Gesetzes über die öffentliche Sicherheit und Ordnung (Nds. SOG).
[357] § 33a Nds. SOG para. 2.

be surveilled.[358] The law limited surveillances to three months, with a possibility for a three-month extension.[359] The target of the surveillance had to be informed of the surveillance retroactively, although some exceptions were permitted.[360]

The Federal Constitutional Court upheld the constitutional complaint on several grounds and voided portions of the law. First, the Court found that the legislature of Lower Saxony had overstepped its bounds in trying to regulate telecommunications for purposes of crime prevention.[361] Because this was an area in which the federal government had concurrent jurisdiction and the federal government had made use of its competency, state legislators did not have the competency to pass the law.[362] Moreover, legislators had not followed the requirements of Article 19's *Zitiergebot* which requires that lawmakers name the Basic Right in a law that limits it.[363]

Substantively, the Court found that the law also did not comply with the *Bestimmtheitsgebot* [definitiveness requirement],[364] which requires that a law is clearly stated so that an individual affected by the law can adjust his behavior according to its consequences.[365] The Court noted that an individual should generally be aware under what conditions and circumstances he may be the subject of a surveillance.[366]

Additionally, the law was not precise enough in distinguishing between potentially harmless and criminal behavior.[367] The statute permitted the surveillance of an individual where the facts supported that the individual was about to commit a serious crime. [368] But the law failed to list any criteria that the police could use to distinguish harmless behavior from criminal preparation.[369] An assumption, even one based on facts, was not sufficient.[370]

---

[358] § 33a Nds. SOG para. Nr. 3.
[359] § 33a Nds. SOG para. 3.
[360] § 30 Grundsätze der Datenerhebung.
[361] BVerfG, 1 BvR 2378/98 (2004), at para. 91.
[362] *Id.* at para. 97.
[363] *Id.* at para. 84.
[364] *Id.* at para. 14.
[365] *Id.* at para. 17.
[366] *Id.*
[367] *Id.* at para. 27.
[368] *Id.* at para. 24.
[369] *Id.* at para. 27.
[370] *Id.* at para. 24.

The Court also found that the constitutional principle of proportionality was not followed in the Lower Saxony statute. The Court emphasized that the state cannot set limits on protected freedoms unless the means by which it does so are proportional to the goals of the law.[371] The Court noted that the limitations on the freedom of communications set forth in the statute were severe.[372] The collection of the data proscribed would reveal communication behavior, as well as the social contacts and personal habits of a targeted individual.[373] Such an extreme encroachment on privacy could be justified only where the public interest was of overwhelming importance. [374] But the law made no mention of such an interest. In addition, the law had the potential of impacting the privacy rights not only of the prospective perpetrator, but of anyone with whom the perpetrator communicated.[375] The encroachment was further intensified by the possibility that government agencies could use the data for other or more general crime-fighting purposes.[376] The Court found that this his possibility alone qualified as its own encroachment.[377]

The Court also found that the statute violated Article 10. As a general matter, the state should not have the possibility to inform itself of the contents of verbal or written communications.[378] Article 10 protected not just the contents of communications, but when, how, and how frequently and between what persons communications take place.[379] The free communication protected by Article 10 would suffer if the state evaluated such matters.[380] Applying its reasoning in the "large eavesdropping attack" case, the Court found that the core sphere of private life deserved strong protection in regard to telephone wiretaps.[381] The Court held that Article 10 protects the free development of personality by providing a private

[371] *Id.* at para. 36.
[372] *Id.* at para. 37.
[373] *Id.* at para. 38.
[374] *Id.* at para. 36.
[375] *Id.* at para. 40.
[376] *Id.* at para. 43.
[377] *Id.*
[378] *Id.* at para. 81.
[379] *Id.*
[380] *Id.*
[381] *Id.* at para. 61.

exchange of communications that also preserves human dignity.[382] Although the Court noted that this protection was not as strong as that of the home,[383] it held that a well-founded basis that a suspected perpetrator was about commit a serious crime was necessary to justify the privacy invasion permitted by the Lower Saxony law.[384] Additionally, the surveillance of a telephone conversation had to be stopped where highly private topics are broached.[385] The results of such measures could not be evaluated and had to be deleted if accidentally seized.[386] Such precautions were not in place with the Lower Saxony law.

D. Summary

Like the U.S. Supreme Court, Germany's highest court has ruled that the home deserves the highest privacy protection in all but the most extreme cases. The type of information obtained in state investigations has also proved important. The Federal Constitutional Court has found the processing and dissemination of information through new technology particularly dangerous because it could lead to the construction of a "personality profile." Unlike that of the U.S. Supreme Court, the analysis of the Federal Constitutional Court has not focused very heavily on the nature of technology used, though it has recognized that developments in investigative techniques have given rise to new privacy concerns.

[382] *Id.* at para. 62.
[383] *Id.*
[384] *Id.* at para. 61.
[385] *Id.* at para. 64.
[386] *Id.*

III. Comparing Germany and the United States: Human Dignity as the Final Safeguard of Individual Privacy

In a post-*Katz* world, three overriding factors appear essential to the American question of whether a state actor has overstepped Fourth Amendment boundaries. First and foremost, what is the target of government surveillance? Private residences plainly receive more protection than commercial property. Second, what type of information does the surveillance reveal? If the surveillance discloses intimate or otherwise personal details, then it likely has interfered with an expectation of privacy that society is willing to recognize. Third, what is the nature of the surveillance technology used? Technologies that are widely known and broadly used give rise to lower expectations of privacy than those that are unknown or inaccessible to the public at large.

Similarly, Germany's Federal Constitutional Court has held that private residences shall receive the highest privacy protection under all but exceptional circumstances. The Constitutional Court has also considered what type of information is revealed in police surveillance. Conversations between family members, or with doctors and attorneys have been deemed particularly intimate and plainly receive greater protection than other types of communications. The Court has been less troubled about whether use of the technology is widely accepted, though it has certainly expressed concern over the increasing invasiveness of new investigative measures. Finally, the Court has viewed as particularly problematic the technological processing and distribution of data by government agencies because of the risk that such actions could lead to the construction of a "personality profile."

A. The Sanctity of the Home

In U.S. jurisprudence the home receives the highest privacy protection. Historically, the Fourth Amendment was enacted precisely to prevent state intrusions in the home under almost all circumstances. The importance placed on the sanctity of the home by U.S. courts has not diminished despite the evolution of new investigative technologies.

The preservation of the sanctity of the home was essential to the U.S. Supreme Court's holding in *Kyllo*. There, the Court noted that "any physical invasion of the structure of the *home*, by even a fraction of an inch, is too much"[387] and emphasized that "the Fourth Amendment draws a firm line at the entrance to the *house*."[388] Similarly, the key difference between the Court's holdings in *Knots* and *Karo* was that in the latter case, the police beeper was used to trace movements within the defendant's home.[389] The Court stated that "private residences are places in which the individual normally expects privacy… and that expectation is plainly one that society is prepared to recognize as justifiable."[390] Conversely, the fact that the target of surveillance in *Dow Chemical* was commercial property and "*not* an area immediately adjacent to a private home" was dispositive to the Court's finding that no Fourth Amendment violation had taken place in that case.[391]

Like the United States, German jurisprudence has placed strong emphasis on the absolute impenetrability of the home. In fact, the inviolability of the home is a basic right articulated in the country's Basic Law. This goes further than the protection offered by U.S. Constitution's Fourth Amendment, which merely protects against unlawful searches and seizures. In the "Large Eavesdropping Attack" Case, Germany's Constitutional Court made plain that the home was an area that warranted almost absolute protection, describing it as the

[387] 533 U.S. at 37 (emphasis added.)
[388] 533 U.S. at 40 (emphasis added.)
[389] 468 U.S. at 714.
[390] *Id.*
[391] 476 U.S. at 237 n. 4.

"last refuge" for the development of one's personality and preservation of one's dignity.[392] The Court also noted that the ability to retreat into one's home was not a right an individual could readily give up.[393]

A comparison between the decisions in the GPS and Preventative Telecommunications Surveillance Cases make plain the importance the Federal Constitutional Court has placed on privacy in the home. In the GPS Case the Court emphasized the limits of GPS technology, noting that its utility in closed rooms or narrow alleyways was virtually non-existent.[394] Therefore, GPS technology could not be used to invade the home. Similarly, the Federal Constitutional Court noted in the Preventative Telecommunications Surveillance Case that communications did not deserve as much privacy protection as behaviors in the privacy of one's home.[395] The court has pointed out that the inviolability of the home is closely linked to the preservation of human dignity, which should guarantee "absolute protection" for behaviors in the home in so far as it represents an individual's manifestation of his or her personality.[396]

B. Intimacy of Details and Relationships

The U.S. Supreme Court has insisted that the intimacy of the details revealed cannot on its own determine whether society would be willing to recognize an expectation of privacy as reasonable.[397] In *Kyllo*, the Court emphasized that "the Fourth Amendment's protection of the home has never been tied to measurement of the quality or quantity of information obtained."[398] The problem with such an approach, the Court explained, was that it would require "a jurisprudence specifying which home activities are 'intimate' and which are not."[399] Specifically, "no police officer would be able to know *in advance* whether his

[392] 1 BvR 2378/98 (2004), at para. 20.
[393] *Id.* at para. 54.
[394] 2 BvR 581/01 (2005), at para. 53.
[395] 1 BvR 2378/98 (2004), at para. 62.
[396] *Id.*
[397] 533 U.S. at 38-39.
[398] 533 U.S. at 37.
[399] 533 U.S. at 38-39.

through-the-wall surveillance pick[ed] up 'intimate' details — and thus would be unable to know in advance whether [his action was] constitutional."[400] In order to avoid such complications, the Court has concluded that where a private residence is involved, "all details are intimate details."[401]

Where, however, the area outside of a home is the subject of government surveillance, the U.S. Supreme Court has focused on the level of intimacy associated with the space surveyed. In *Riley*, the Court found that no Fourth Amendment violation occurred because "no intimate details connected with the use of the home or curtilage were observed."[402] In *Dow Chemical*, the fact that the details observed remained limited to an outline of the facility's buildings and equipment was important.[403] But where the home's curtilage is the target of surveillance, the Court has said it will inquire "whether the area in question harbors those intimate activities associated with domestic life and the privacies of the home."[404]

The intimacy of details revealed as a result of government action has been at the heart of Germany's privacy cases, including those involving criminal defendants. The judicially recognized sphere theory, which associates different areas of life with different levels of privacy, provides that the innermost sphere – the intimate sphere – is inviolable.[405] In contrast, a violation of the next sphere – the private sphere – is permissible in the overwhelming interest of public good so long as strict principles of proportionality are adhered to.[406] The Court has found that the outer sphere – the social sphere – may be invaded, so long as such an invasion is sanctioned by law.[407]

As far back as the *Lebach* case the Federal Constitutional Court recognized that certain areas of private life should be protected from state invasion.[408] In *Lebach*, the Federal

[400] *Id.*
[401] 533 U.S. at 37 (emphasis added).
[402] 488 U.S. at 452.
[403] 476 U.S. at 238.
[404] *U.S. v. Dunn*, 480 U.S. 294, 301 n. 4 (1987).
[405] Mangoldt/Klein, Art. 2 I Rn. 88; Glaeser, Rn. 35.
[406] Mangoldt/Klein, Art. 2 I Rn. 88; Sachs, Art. 2 I Rn. 103ff; Glaeser, Rn. 37ff.
[407] Pieroth/Schlink, Rn. 382; Glaeser, Rn. 37.
[408] BVerfGE 80, 367 (373).

Constitutional Court held that a television report that revealed a convicted criminal's name and face did not touch the most intimate sphere of private life, but violated the criminal's general personality rights.[409] Nonetheless, the court ruled that the reporting of these details could not be justified by the public's right to freedom of information.[410]

As early as the Microcensus Case, the Federal Constitutional Court reasoned that general information about an individual's recreational trips did not involve "the most intimate realm" and therefore the Basic Law did not protect such details.[411] In contrast, the Court found in the Federal Census Act Case that the possibility that government authorities could construct a "complete personality profile" that detailed an individual's cumulative activities violated the right to informational self-determination.[412]

In a later criminal case involving acoustic surveillance, the Federal Constitutional Court noted that particularly intimate types of communications warranted almost absolute privacy protection.[413] Accordingly, the German court created a protected category of communications that included conversations between close family members or other persons of trust, such as members of the clergy, physicians, and criminal defense attorneys.[414] The Court held that the government could monitor such types of communications only if concrete evidence existed at the time an eavesdropping warrant was issued that at least one of the persons speaking is or was involved in a criminal offense.[415] In the Preventative Telecommunications Surveillance Case, the Federal Constitutional Court reiterated this analysis. The Court found that in order for the core sphere of privacy to remain protected telephone surveillance had to be limited.[416] The Court explained that telephone conversations did not warrant as much privacy protection as activities inside the home.[417] However, the

[409] BVerfGE 35, 202 (226).
[410] *Id.*
[411] BVerfGE 27, 1 (8).
[412] BVerfGE 65, 1 (17).
[413] BVerfG, 1 BvR 2378/98 (2004), at para. 148.
[414] *Id.*
[415] *Id.* at para. 37.
[416] BVerfGE 100, 313, at para. 61.
[417] *Id.* at para. 62.

Court held that where very private or intimate matters were discussed on the telephone, government surveillance must cease.[418]

The Federal Constitutional Court distinguished the cases involving acoustic surveillance in the home and preventative telecommunications surveillance from the use of GPS technology because there was little likelihood that GPS could reveal intimate details of a subject's life. The Court emphasized the usefulness of GPS technology was limited to revealing a person's location and the length of time spent in a given location, and that GPS did not function effectively in closed rooms or on streets in dense neighborhoods.[419] Accordingly, the Court found that although GPS surveillance did constitute an attack on the suspect's personality rights, the extent and intensity of the invasion was not at a level that violated human dignity or the untouchable core sphere of privacy.[420]

How the courts have defined which details are "intimate" and which are not has been different in Germany and the United States. Should the numbers dialed from a phone, for example, be protected in the same manner as the contents of the phone conversation? The U.S. Supreme Court has determined that no one can reasonably expect that the numbers dialed from one's telephone are protected as private because this information is readily available to the phone company.[421] In contrast, the Federal Constitutional Court has found that the knowledge of when, how often and between whom telephone conversations take place deserves some privacy protection.[422]

[418] *Id.* at para. 64.
[419] *Id.* at para. 56.
[420] *Id.* at para. 56.
[421] 442 U.S. at 742.
[422] 1 BvR 2378/98 (2004), at para. 81.

C. Technology

The U.S. Supreme Court also has considered the nature of the investigative technology itself in order to determine whether an individual's reasonable expectation of privacy has been violated. Two factors have been particularly relevant. First, how sophisticated is the surveillance equipment being used? In cases where the equipment reveals details analogous to those government officers could make through naked observations, the technique was less likely to require a warrant.

As far back as the *Smith* case the Supreme Court expressed no reservations regarding police use of pen registers because they did not reveal any information that was not otherwise available to the phone companies.[423] Similarly, the Court did not object to the use of a 35mm camera from an altitude of 1,000 feet in *Ciraol*o[424] and expressed only limited concerns regarding the use of a precision aerial mapping camera from as high as 12,000 feet in *Dow Chemical*.[425] Additionally, the Court distinguished *Karo* from *Knotts* because the police officers in *Knotts* used a beeper to ascertain information they theoretically could have obtained by making visual observations.[426] In contrast, state officials in *Karo* gained information from the radio transmitter not otherwise available to them.[427]

Second, the Court has evaluated the ubiquitousness of the investigative equipment used. In regard to the use of 35mm camera, planes, and helicopters, the Court has assumed a certain "general knowledge" on the part of the general public. Because private and commercial flight has, for example, become "routine," no expectation of privacy can be assumed in regard to police use of such items.[428] However, in regard to more sophisticated equipment, the Court has raised serious concerns. In *Kyllo*, the Court emphasized that

[423] 442 U.S. at 743.
[424] 476 U.S. at 207, 209.
[425] *Id.* at 238.
[426] 460 U.S. at 282-284.
[427] 468 U.S. at 708, 714.
[428] 476 U.S. at 215.

"where… the technology in question is not in general public use" and reveals information that could not otherwise be obtained without "physical 'intrusion into a constitutionally protected area,'" its use is likely to constitute a search within the meaning of the Fourth Amendment.[429] In *Kyllo* as well as *Dow Chemical*, the Court has indicated that the use of satellite technology without a warrant would be unconstitutional.[430]

Germany's Federal Constitutional Court also has looked at the type of technology used, but it has focused less on the ubiquitousness of the surveillance measure than on its effect. Primarily, the Constitutional Court has considered whether (1) the surveillance measure violates human dignity, and (2) whether a *Rundumüberwachung* has occurred that could lead to the dangerous and unconstitutional construction of a complete "personality profile." Although the characteristics of a *Rundumüberwachung* remain loosely defined, the Constitutional Court indicated that such an analysis is qualitative, rather than quantitative.

The Federal Constitutional Court recognized early on that new advances in technology would lead to deeper invasions of privacy. In the *Lebach* case the Court recognized that a television report that revealed private information by its very nature was more invasive than a written or verbal news report would be.[431] Similarly, in the Federal Census Act case, the Court would rethink its Microcensus Case reasoning, on the grounds that data processing and distribution techniques had changed significantly in fourteen years.[432] The Court noted that the disclosure of limited information could lead much more easily to the construction of an unconstitutional personality profile in 1983 than in 1969.[433]

In the newer German cases addressing privacy rights the Federal Constitutional Court also recognized that private data could be much more quickly and readily utilized for illegitimate purposes than before. This reality led the Court to require stricter data

[429] 533 U.S. at 34 (citing *Silverman*, 365 U.S. 505, 512).
[430] *See* 476 U.S. at 238; 533 U.S. at 35.
[431] BVerfGE 35, 202 (226).
[432] BVerfGE 65, 1 (17).
[433] *Id.*

distribution measures in the Strategic Telegram Surveillance Case[434] and to forbid government agencies from having full access to each other's databases.[435] In the Preventative Telecommunications Surveillance Case the Court emphasized constitutional privacy rights had become particularly at risk due to the sheer quantity of data that could be obtained as a result of modern telecommunications.[436] In that case, the Court found that the possibility that collected data could be used for purposes other than those for which they could be collected represented a violated of Article 10 of the Basic Law.

The Court also found that a particularly severe constitutional invasion of privacy occurrs where a *Rundumüberwachung* or total surveillance takes place that would lead to the construction of a personality profile, as would have been the case in the Federal Census Act case. In the GPS case the Court ruled that no total surveillance had taken place despite the fact that investigators had read a suspect's mail, tapped his phones, and videotaped the outside of his home.[437] The Court found significant the fact that the acoustic surveillance was limited and that GPS was used only as a supplement to the other surveillance methods.[438] Nonetheless the Court emphasized in cases of heavy surveillance, government agencies should coordinate their efforts with one another to ensure that no unconstitutional total surveillance takes place.[439]

D. National Security and Preventative Measures

Where national security and the prevention of imminent danger are at stake, the U.S. Supreme Court and Germany's Federal Constitutional Court have expressed similar views in regard to state use of surveillance technologies. The U.S. Supreme Court never directly has had to address the question of under what circumstances government use of technical means might be constitutionally permissible if used to prevent imminent danger, though the Court

[434] BVerfGE 100, 313, at para. 190.
[435] *Id.* at para. 262.
[436] BVerfG, 1 BvR 2378/98 (2004), at para. 82.
[437] BVerfG, 2 BvR 581/01 (2005), at para. 6.
[438] *Id.* at para. 67.

has set limits in regard to technical surveillance for the protection of national security. The Federal Constitutional Court has permitted state use of technical surveillance measures under limited circumstances to prevent imminent danger and protect national security.

According to the Federal Constitutional Court, the use of technical surveillance measures to prevent imminent danger can be justified only where a concrete danger is present that a specific crime of significant importance is about to be committed. In the Preventative Telecommunications Surveillance Case of 2005, the Court explained that a law that permitted preventative telephone wiretapping only could be viewed as reasonable if it had the goal of protecting an overriding public interest.[440] Additionally, a law permitting such surveillance would have to define in precise terms which crimes it intended to prevent and what types of behaviors indicated that such a crime was imminently going to be committed.[441]

In the "Large Eavesdropping Attack" Case of 2004, the German Court made it plain that only the protection of life and limb could justify that a suspect was not informed in the immediate aftermath that he had been the subject of an acoustic surveillance in his home. Any subject of acoustic surveillance would have to be informed immediately that he had been the target of an acoustic surveillance at home as soon as the danger to life and limb had passed and as soon as the investigation no longer could be compromised.[442]

Unlike the German Federal Constitutional Court, the U.S. Supreme Court has yet to decide a case in which it must determine how far the state may go in using technical surveillance measures to prevent imminent danger. It is likely that the Court would apply similar principles as it has in other cases involving emergency situations and exigent circumstances. According to those cases, one could make the argument that the use of technical surveillance measures without a search warrant could be justified where life is

[439] BVerfG, 2 BvR 581/01 (2005), at para. 62.
[440] BVerfG, 1 BvR 2378/98 (2004), at para. 36.
[441] *Id.* at para. 28.
[442] *Id.* at para. 300.

endangered or where the risk of serious bodily harm is present.[443] As soon as the exigent circumstances or emergency situation that justified the warrantless use of surveillance measures has passed, an investigator likely would have to apply for a search warrant to undertake any additional surveillance.[444]

In cases where the state has used technical surveillance measures for preventative purposes, where no danger to life or limb is present, lower U.S. courts have found other means of justifying the surveillance. The use of metal detectors at airports, for example, has been justified by the argument that airline passengers implicitly consent to be searched when they buy a plane ticket.[445] Video surveillance in public buildings has been rationalized because no reasonable expectation of privacy exists in a public space.[446] Accordingly, those scenarios have proved mostly unproblematic.

Where national security is at risk, U.S. and German jurisprudence has evolved differently despite the fact that courts in both countries have seen similar dangers in such surveillances. The U.S. Supreme Court has recognized that state surveillance of political groups with unpopular political opinions could be abused by the government and thereby endanger freedom of speech under the First Amendment.[447] Similarly, the Federal Constitutional Court has explained that freedom of telecommunication under Article 10 of the Basic Law would suffer if the population had to fear that the state could use the contents of phone calls and other telecommunications to their disadvantage.[448]

The highest courts in Germany and the United States have resolved this problem differently, however. The U.S. Supreme Court has distinguished between intelligence-gathering activities that affect domestic persons and groups and those that only affect foreign powers of foreign persons and groups. Surveillance of the first category of persons requires a

[443] *See* Bender, *supra* note 13, at § 3.02.
[444] *See* Bender, *supra* note 13, at § 3.02.
[445] *See* Bender, *supra* note 13, at § 3.10.
[446] *See* Bender, *supra* note 13, at § 2.03.
[447] *See* Bender, *supra* note 13, at § 2.03.
[448] BVerfGE 100, 313, at para. 163.

search warrant.[449] Whether a search warrant is constitutionally required for the second group remains an open question. In contrast, the Federal Constitutional Court has held that Article 10 of the Basic Law, which guarantees freedom of communications, is implicated when a conversation is recorded and evaluated on German soil – regardless of the nationality or location of the person communicating.[450] The German Court has left open the question of whether such a territorial link is required or whether Article 10 also protects foreign communications taking place on foreign soil.[451]

In both countries legislators have attempted to limit by statute the negative consequences the surveillance of overseas phone calls or communications with "foreign powers" can have on the rights of their citizens. In the United States prosecutors must meet certain conditions to ensure that U.S. persons are not affected too strongly during surveillances of foreign powers.[452] Similarly, German legislators have put safeguards in the new G-10 security law [453] to ensure that the surveillance of overseas telecommunications is limited in such a way as to avoid the surveillance of telephone lines used predominantly by German citizens [454]

What is required by each country's constitution is different. In the Strategic Telegram Surveillance Case, the Federal Constitutional Court required that the distribution of collected data remain limited, that notification of surveilled suspects be improved, and that parliamentary oversight be strengthened.[455] The U.S. Congress has addressed similar concerns in the Wiretap Statute and FISA with similar legal results. But the U.S. Supreme Court has not mandated these legislatively imposed safeguards as constitutionally required.

[449] 407 U.S. at 320.
[450] BVerfGE 100, 313 (363).
[451] *Id.* at 364.
[452] *See* 50 U.S.C. 1805(a)(4); (b)(1)(F); (b)(2) (1994) (requiring "minimization" procedures in FISA).
[453] Gesetz zur Neuregelung von Beschränkungen des Brief-, Post- und Fernmeldegeheimnisses vom 26.6.2001 (BGBl. I S. 1254).
[454] Dreier, Art. 10 Rn. 43.
[455] BVerfGE 100, 313, at para. 261.

E. Prospects for the Future: When "Reasonable Expectations" Cease to Be Reasonable

At first glance, it appears that different legal approaches to privacy law in Germany and the U.S. have yielded final results that do not differ substantially. Despite dissimilar emphases on the technological nature of the government investigative measures used and the types of information revealed, both countries' regimes ultimately recognize the home as the most protected of private spheres. In both countries, government investigators must meet the highest constitutional standards to penetrate a private residence.

The approach taken by Germany's Federal Constitutional Court, however, may be better equipped to address future privacy concerns arising from continued developments in investigative technologies because of a key difference that exists between the U.S. and German privacy regimes. Simply stated, while U.S. law protects merely the *expectation* of privacy, German jurisprudence protects privacy itself. In Germany, privacy is a positive right. By linking privacy to human dignity, Germany's Federal Constitutional Court has constructed an affirmative obligation on the part of the state to create the conditions that foster and uphold the private sphere. In contrast, the right to privacy in the United States is a negative right. Individuals have the right to be free from illegal government searches and seizures, but the government has no constitutional duty to preserve or cultivate an individual's private sphere.

Because Germany's jurisprudence puts such a high premium on privacy itself, it should come as no surprise that the Federal Constitutional Court has placed more weight on the type of information revealed in a government investigation and less emphasis on the nature of investigative measures used. The sophistication or ubiquitousness of an investigative measure is simply not relevant if the end result of an investigation is that the constitutionally protected private sphere has been pierced. In this sense, the German regime is quite absolutist.

In contrast, the types of observation measures used in government investigations is highly relevant in U.S privacy law because it goes to the heart of the question of whether an individual had a reasonable expectation of privacy that society is willing to recognize. Technologies that are widely known and broadly used give rise to lower expectations of privacy than those that are unknown or inaccessible to the public at large. The U.S. approach is problematic because expectations are by their nature malleable. As technologies become increasingly "routine," individuals cannot reasonably expect that the government will not use such technologies against them. Accordingly, privacy rights are diminished. The existing case law bears this out. Prior to the invention of airplanes and helicopters, for example, a fenced-in backyard would have been considered private because no individual could have reasonably anticipated that someone could see over the edge of a tall barrier.

Under German law, however, the development of new investigative technologies does not and would not require a shift in privacy standards. Because German law protects the principle of privacy itself and provides for an affirmative right to informational self-determination, certain spheres of privacy remain absolutely impenetrable, regardless of the investigative measure used. Therefore, any government invasion of privacy that offends human dignity is prohibited in all but the most extraordinary of circumstances. Moreover, because individuals have the right to control the distribution of information about themselves, it is irrelevant whether it is data processing software, acoustic surveillance equipment, or global position technology leads to a breach of privacy. The issue remains whether the personal information revealed or the profile constructed violates an individual's human dignity.

IV. Conclusion

As government surveillance methods become increasingly sophisticated, the United States will have to consider a more comprehensive approach to privacy law. A rule based strictly on the reasonable expectation of privacy is ill equipped to protect individuals against increasingly invasive police investigative methods made possible through advances in technology. In contrast, Germany's Federal Constitutional Court has established a privacy regime capable of standing the test of time. By linking privacy to human dignity, the Federal Constitutional Court has assured that privacy lines are not redrawn simply because investigative technologies get more sophisticated or law enforcement priorities shift.