DEVELOPMENTS

Germany's Federal Constitutional Court and the Regulation of GPS surveillance

By Jacqueline E. Ross[*]

A. Introduction

In its recent decision of April 12, 2005, Germany's Federal Constitutional Court (FCC) addressed concerns that advances in the technologies of surveillance will erode fundamental rights.[1] Though it rejected the petitioner's call to limit use of the Global Positioning System ("GPS") to track the movements of suspects, the Court did warn that surveillance technologies working in tandem posed privacy risks that were greater than the sum of each one working alone. The Court required investigators from different agencies and states to coordinate their activities and disclose all ongoing surveillance when seeking judicial approval of additional methods and technologies. It likewise cautioned the *Bundestag* (German Federal Parliament) to monitor advances in surveillance technology and to develop new statutory safeguards that would protect personal data by limiting the use of more powerful innovations. Yet the Court's opinion left many questions unanswered. It did not explain how legislators or investigative agencies could avoid unnecessarily and intrusively multiplying the use of surveillance, given the overlapping jurisdiction of intelligence agencies with state and federal police. And insofar as the German *Strafprozessordnung* (Criminal Procedure Code – StPO) regulates only those modes of surveillance that produce criminal prosecutions, statutory suppression remedies have no clear impact on the investigative use of surveillance for purely preventive or intelligence-gathering purposes. My essay will explore the implications and limitations of the Court's opinion with an eye on analogous American law (introduced to gain a comparative perspective.)

B. Procedural Background

The petitioner was a member of the so-called "Anti-imperialist Cell," an outgrowth of the erstwhile "Red Army Faction," who appealed his attempted murder

[*] Associate Professor, University of Illinois College of Law.

[1] 2 BvR 581/01; the decision is available in German at: www.bverfg.de/entscheidungen/rs20050412_2bvr058101.html. See also Jacoby 6 GLJ 1085 (2005).

convictions for carrying out a series of terrorist bombings. His petition challenged the state's use of GPS technology to monitor his movements. Several government agencies, including the *Bundeskriminalamt* (Federal Police Agency) and the *Verfassungsschutz* (Agency for the Protection of the Constitution) in two German *Länder*, investigated the petitioner and his co-defendant for past and ongoing terrorist offenses. During the course of these investigations, the *Bundeskriminalamt* and the *Verfassungsschutz* conducted visual surveillance, intercepted telephone and radio communications, and installed a GPS tracking device in the co-conspirator's vehicle (after the petitioner and his accomplice had detected and disabled a more primitive electronic beeper.) The GPS tracking device was significantly more powerful than the electronic beeper, which operates only in real time. The device recorded a vehicle's location, movements, and speed along with the corresponding dates and times and stored the information for subsequent downloading. In this way, it permitted the investigators to construct a complete picture of the car's past and present movements. By contrast, the beeper provides only contemporaneous information and requires investigators to know the general location of the vehicle in order to intercept the electronic signal.

On appeal from his convictions for terrorist offenses, the petitioner claimed that Section 100(c)(1)(b) of the StPO did not validly authorize the use of the GPS device. The provision did permit investigators to use "technological means" to conduct visual surveillance of persons suspected of serious crimes. But the petitioner claimed that the code's reference to technology was insufficiently specific to authorize the use of powerful GPS tracking devices, which allowed investigators to create a seamless timeline of a person's comings and goings. He also contended that powerful GPS surveillance devices required greater procedural safeguards than more primitive tracking technology. If Section 100(c)(1)(b) were read to authorize GPS devices, it would infringe his constitutional "rights of personality"[2] —his autonomy (and "*für-sich-sein-wollen*")—as well as the privacy rights protected not only by the *Grundgesetz* (German Basic Law) but also by Article 8, § 1 of the European Convention on Human Rights. Instead, Section 100(c)(1)(b) should be interpreted to protect these rights by imposing greater procedural demands on more powerful surveillance technologies.

C. Informational Self-determination, Privacy, and the Technologies of Surveillance: The Differing German and American Perspectives

The FCC affirmed the *Oberlandesgericht* (Regional Appellate Court) and the *Bundesgerichtshof* (Federal Court of Justice) in rejecting the petitioner's arguments.

[2] Articles 1 and 2 of the Grundgesetz.

In upholding the use of GPS technology, the Supreme Court rejected the lower courts' view that the global positioning system was the functional equivalent of electronic beepers, which Section 100(c)(1)(b) authorized. An electronic beeper requires some contemporaneous knowledge of the vehicle's approximate whereabouts. A GPS tracking devices does not; it records a target's movements without gaps. On the other hand, the Court noted, a GPS device qualifies as a "technological means" of surveillance under the statute. Like electronic beepers, it provides information about the target's location. The Court thus rejected two of the petitioner's claims: first, that the investigative use of a GPS device required authorization from a statute specific to that technology; and second, that the criteria by which Section100(c)(1)(b) regulates the use of surveillance were too lenient when applied to GPS technology. Electronic tracking is considerably less intrusive than electronic listening, the Court reasoned, and facilitating the use of the former might obviate the need for the latter. And as it is, the statute restricts tracking technology to the investigation of serious offenses, when these would otherwise be harder to solve or their perpetrators more difficult to locate.

One consideration complicated the Court's assessment of whether the state had properly used GPS tracking technology in this case. The investigation at issue had taken place four years before the *Bundestag* had revised the Code of Criminal Procedure, specifically Section 163f, to require advance judicial approval for long-term surveillance of suspects. The state had neither sought nor been statutorily required to seek judicial authorization to monitor the petitioner long-term. But if the statutory change were constitutionally mandated, then the lack of judicial oversight would have violated the petitioner's constitutional privacy rights regardless of what the Code of Criminal Procedure required at the time. The Court, however, did not interpret the judicial approval requirement as a dictate of constitutional law. In revising Section 163f, the Bundestag had simply used its discretion to enhance procedural protections for privacy. The code's new requirements therefore had no retroactive implications.

The most significant issue that the Court confronted, however, concerned the cumulative impact of combining multiple modes of surveillance, such as wiretaps and GPS technology. In the petitioner's case, the federal investigators not only used GPS technology but also conducted visual surveillance and monitored his telephone and his mail. These together permit a fairly detailed reconstruction of a target's daily activities. Invoking the "law of personality"[3] that protects individual autonomy and "informational self-determination" as aspects of privacy and

[3] Article 2 (1) of the Grundgesetz (German Constitution); and English version is available at: www.bundestag.de/htdocs_e/info/gg.pdf.

dignity[4], the petitioner had argued that the cumulation of different modes of surveillance exposed too much personal information to the government, shining a light, as it were, on his innermost thoughts and permitting the police to construct a comprehensive personality profile. A separate statutory provision was therefore necessary to regulate and limit the coordinated use of different surveillance techniques. Such a law should require a judge to consider the cumulative impact of these technologies on the petitioner's privacy and to decide in advance whether the joint use of surveillance tactics was warranted. Absent such protections, the petitioner had claimed, the evidence obtained through the Global Positioning System could not have been used to convict him without infringing his right to a fair trial.

The Court rejected this argument in part because the effective overlap of different surveillance techniques had been quite small. Investigators had come to rely primarily on the GPS technology because the petitioner had proven remarkably successful in evading vehicles that tailed him and in disabling other surveillance technologies such as electronic beepers. Only on weekends had the investigators supplemented the Global Positioning System with visual surveillance. The police conducted minimal wiretapping. The petitioner, who suspected that his phone lines were being monitored, had spoken very little by telephone.

More importantly, however, the FCC found that Code of Criminal Procedure already limits cumulation of surveillance techniques by requiring judges to take account of the marginal extent to which each new mode of surveillance contributes to an ongoing investigation. Every statute authorizing some form of surveillance incorporates a "principle of subsidiarity," which permits covert powers to be utilized only when other investigative means are inadequate. Courts interpret this limitation with an eye on the intrusiveness of the surveillance. The police may use tracking technologies upon a determination that the offense would be more difficult to investigate or the suspect harder to locate without the use of such devices. By contrast, the use of wiretaps or long-term undercover agents requires a judicial finding that the investigation would otherwise be hopeless or *significantly* more difficult ("*aussichtslos oder wesentlich erschwert*.")[5] The principle of subsidiarity suggests that less intrusive modes of surveillance have to be exhausted or at least considered before more invasive alternatives may be authorized. The more modes of surveillance the state deploys, the less each additional covert technique contributes at the margin and the more difficult it becomes to justify its use. In this way, the system for regulating covert surveillance powers pursues proportionality between investigative means and evidentiary payoffs. It avoids the nightmare

[4] BVerfGE 65, 1.
[5] *See* St PO Sections 100a, 110a. For an English version see: www.iuscomp.org/gla/statutes/StPO.html.

scenario of "total surveillance" that the FCC recognizes as constitutionally prohibited.

Nonetheless, the FCC acknowledges that these safeguards depend on effective coordination between investigative agencies. The prosecutor in charge of a criminal investigation must know about all ongoing forms of surveillance in order to assess the need for additional modes of surveillance and to brief the judge who must approve requests for approval. The decision directs prosecutors to use a national register of criminal investigations in order to avoid duplication of their efforts by prosecutors in other states. And intelligence agencies, including *Länder* and federal *Verfassungsschutz* offices, must have access to prosecutors' records or case files, so that intelligence agencies can coordinate their surveillance activities with those of the police. The Court therefore admonishes legislatures—presumably both on the level of the *Länder* and on the federal level—to consider enacting guidelines to regulate inter-agency cooperation.

Germany's approach to the regulation of covert surveillance thus differs remarkably from its American counterpart. The United States Supreme Court has held that "a person traveling in an automobile on public thoroughfares has no reasonable expectation of privacy in his movements from one place to another."[6] These reduced protections for privacy follow from the circumstance that surveillance is conducted in public areas and from the mobility and extensive regulation of automobiles.[7] (Some federal district court and state appellate courts, however, have required a court order for the installation of GPS devices, citing their greater intrusiveness.)[8] By contrast, German suspects enjoy privacy rights in public as well as private areas. The degree of constitutional protection turns on how "personal" the information is that investigators seek. Whether observation takes place in public or private is a secondary concern. The German approach follows from the FCC's recognition of a right of "informational self-determination," that is, a right of all persons to control their personal data and to limit the government's collection, storage, and transmission of personal information about them. (This right, a hybrid of dignitary and privacy interests, emerged from the federal Supreme Court's decision in the famous *Volkszählung* (Microcensus) case of 1984.[9]

---

[6] *United States v. Knotts*, 460 U.S. 276, 284-85 (1983).

[7] *See e.g. United States v. Moran*, 349 F.Supp.2d 425, 467-68 (N.D.N.Y. 2005)(upholding that the warrantless installation of a GPS device).

[8] *See e.g. People v. Lacey*, 787 N.Y.S.2d 680 (N.Y.Co.Ct., 2004); *People v. Gant*, 2005 WL 1767655, June 27, 2005 (N.Y.Co.Ct. 2005); *State v. Campbell*, 759 P.2d 1040 (Oregon, 1988); *State v. Jackson*, 76 P.3d 217 (Washington, 2003); *see also United States v. Berry*, 300 F.Supp.2d 366, 368 (D.Md. 2004)(contrasting memory feature of GPS with more limited, real-time information revealed by electronic beeper, and calling for court order, in *dicta*.)

[9] BVerfGE 65, 1.

James Whitman has described Germany's approach to privacy as embodying a concern with dignity and with affording people control over the way they present themselves to the world.[10] He has contrasted it with an American concern with physical privacy in the home and decisional privacy, including a right to autonomy from government interference with personal decisions (concerning abortion and contraception, for example.)[11]

On the German approach to privacy, therefore, people do not forfeit legal protection by "knowingly exposing" themselves or their activities to public view. As Whitman points out, naked sunbathers in German parks may even suppress the publication of nude photographs of themselves taken in public.[12] Under German law, of course, people enjoy less protection for privacy in public areas than in their home or workplace. Filming a suspect in public is permissible, while filming him in his home is not. But appearing in public only diminishes privacy protections; it does not cancel them altogether. Thus it makes sense that German law requires advance judicial authorization of long-term visual surveillance even when conducted entirely in public areas.[13] In addressing the permissibility of GPS surveillance, the FCC reaffirms the larger principle that the degree of privacy protection depends crucially on the nature of the information, which this technology discloses. When combined with other surveillance techniques in ways that yield too comprehensive a record of a person's doings and habits, even the use of a tracking device may violate suspects constitutional right to "informational self-determination."

There is another way in which the FCC's GPS decision presents a striking contrast with American privacy regulation. As the U.S. Supreme Court's decision in *Kyllo*[14] made clear, the advent and spread of new surveillance technologies may diminish privacy protections. American constitutional doctrine ties constitutional safeguards to subjective expectations of privacy. These diminish as intrusive surveillance technologies come into general use. Germany's FCC takes the opposite approach. In the GPS opinion, it calls on legislators to keep pace with advances in the technologies of surveillance and, if necessary, to enact new statutory regulation to counteract emerging conflicts with privacy. The decision does not suggest the technological threats that the court has in mind. Nor does it tell legislators how to implement protections for privacy. It assigns these questions to the democratic process (though subject, ultimately, to judicial review.) This means that a FCC

---

[10] James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty,* 113 Yale L. J. 1151 (2004).
[11] *Id.*
[12] *Id.*
[13] St PO 163f.
[14] Kyllo v. United States, 533 U.S. 27 (2001).

decision to extend constitutional privacy protections does not pre-empt legislative action as the American *Miranda* decision has been accused of having done for the regulation of police interrogation. German constitutional protection for privacy leaves legislators a considerable field of action in crafting compromises between privacy and law-enforcement interests and in dictating the nature of procedural safeguards on the use of surveillance technologies.

D. Overlapping jurisdictions and Cumulative Surveillance: Can the Code of Criminal Procedure Supply a Solution?

For all its concern with technological encroachments on privacy, however, the FCC decision provides little guidance on whether and how the legislature should regulate those forms of surveillance that do not yield prosecutions.[15] The Criminal Procedure Code does not regulate so-called "preventive" police operations, which aim to identify threats, keep public order, and forestall future crimes. Germany's police laws, which vary from state to state, authorize the police to conduct covert surveillance in their preventive, order-maintenance capacities, while the federal procedural code regulates only the "repressive" powers of the police, that is their prerogatives to solve past and ongoing crimes in their law-enforcement capacity. And neither the federal criminal procedural code nor the state police laws regulate the powers and prerogatives of the *Länder* and federal *Verfassungsschutz* or Germany's other intelligence agencies (whose powers are governed by separate *Länder* and federal laws.) Thus, as the petitioner argued in his appeal to the Court, the Federal Criminal Procedure Code is neither designed nor equipped to deal with privacy intrusions that do not yield prosecutions. No suppression remedy will deter abuses that are not designed to produce evidence. Nor is it clear that the Court would in fact suppress evidence which the police stumble upon while monitoring suspects in their *preventive* capacity, or which the *Verfassungsschutz* collects in accordance with the laws that govern their own surveillance activities. The strictures of Section 100(c)(1)(b) would simply not apply to such operations.

The court does acknowledge that, in extreme cases, the cumulation of surveillance tactics may exceed constitutional limits in the aggregate even when individual modes of intrusion can be justified in isolation. Yet the court does little to identify or suggest safeguards against that risk. Prosecutors have little or no role to play in

---

[15] Of course, one might question whether the FCC *could* provide such guidance without violating the principle of separation of powers. Presumably, however, surveillance that does not produce prosecutions would result from powers which the police exercise in their preventive capacity or which the Verfassungsschutz acquire from their own statutory mandate; to the extent these powers infringe constitutional rights, *some* court, whether state or federal, should have the authority to pass on the lawfulness of what enabling legislation authorizes or on the legality of what the authorities interpret these laws to allow.

many preventive police investigations, unless the operation is on the verge of yielding seizures or arrests. The opinion does not make it clear whether the police must notify prosecutors of the results of purely preventively conducted surveillance operations once the police initiate a full-fledged criminal investigation. If they do not do so, then prosecutors may not be able to present judges with a complete picture of all surveillance activities that have gone before when they seek approval for additional forms of monitoring. While the opinion suggests the need to inform intelligence agencies about the surveillance activities of the police, it says nothing about whether intelligence agencies must themselves disclose to police or prosecutors that they are monitoring some suspect in whom law enforcement authorities have also taken an interest. If intelligence agencies have no such obligation, then the task of avoiding unnecessary duplication remains entrusted exclusively to the intelligence community, providing prosecutors and judges with no way of knowing about or remedying excesses of cumulative monitoring. This risk may be particularly troublesome given that each of the German states has its own *Verfassungsschutz* agency, which may be hesitant to share information not only with the police but with the *Verfassungsschutz* of other *Länder* or the federal government, or with Germany's other intelligence agencies. (Indeed, in this very case, the Court noted that the investigative agencies included both the *Bundeskriminalamt* and the *Verfassungsschutz* agencies of two separate states. The opinion does not make it clear whether these agencies knew about each other's involvement or coordinated their activities with each other.)[16] But that larger problem of coordination is not one which the Federal Criminal Procedure Code can solve. Nor did the FCC confront the problem of duplication and excess in this case. What the court did make clear, however, is that coordinating police and intelligence responses to national security threats remains essential to the protection of privacy interests.

[16] The failure to coordinate surveillance among different branches of government can produce dramatic results. In 2003, the FCC rejected the government's petition to ban an extremist political party after it turned out that the leadership had been thoroughly infiltrated by APC operatives from different state and federal agencies. BVerfGE 107, 339-395 (2003). Together, these informants had played important roles in setting the party's agenda and publicizing its goals—though it remained disputed whether they had done so after they had stopped working together with the APCs and whether they had influenced the party's defense strategy in the government's proceedings against it. Because the state and federal intelligence agencies had not known about each other's informants, their joint petition to ban the party had in fact relied at least in part on party propaganda that had been crafted by the APCs' own former informants. The German Supreme Court ultimately dismissed the government's petition because the dangers that the political organization posed without the influence of APC infiltrators proved almost impossible to determine.