German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance

by
PAUL M. SCHWARTZ*

Introduction

The legal systems of Germany and the United States contain detailed rules that regulate the surveillance of telecommunications by domestic law enforcement agencies.[1] One initial question about this surveillance

 I wish to thank the American Academy in Berlin for their support while I was a Berlin Prize Fellow there in Fall 2002. I also wish to thank the German Marshall Fund for a research fellowship and their offer of a residency at their Transatlantic Center, Brussels, Belgium in Spring 2003. This work also benefited from the support of Dean John Wexler and the Dean's Research Fund of Brooklyn Law School.

John Bauman III, Hans-Peter Bull, Alexander Dix, Mark Eckenweiler, Chris Hoofnagle, Robert Gellman, Hansjörg Geiger, Michael Gerhardt, Ted Janger, Orin Kerr, Lance Liebman, Viktor Mayer-Schönberger, Spiros Simitis, Daniel Solove and Stefan Walz made helpful comments on earlier versions of this Article. This work was presented at the Enforcing Privacy Conference on November 14, 2002, in San Francisco, California, which was sponsored by the *Hastings Law Journal*; the Samuelson Law, Technology and Public Policy Clinic at the University of California (Boalt Hall) School of Law; and the Institute for Law and Economic Policy. It was also presented on December 10, 2001 at the American Academy in Berlin. I am grateful for suggestions and comments made on both occasions. Unless otherwise noted, all translations are my own.

1. This Article's examination of telecommunications surveillance will be restricted to activities carried out by domestic law enforcement agencies in enforcing criminal law. Surveillance also takes place in Germany and the United States alike under separate foreign intelligence statutes; the issues concerning that kind of surveillance are sufficiently distinct, however, to require separate analysis. Two of the key statutory regulations regarding surveillance in the context of foreign intelligence agencies are the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1803 (2003); and the "Article 10 Statute," Gesetz zu Artikel 10 Grundgesetz, v. 26.6.2001 (BGBl I S.1254), as amended 9.1.2002 (BGBl. I S.361). It proved difficult, however, for this Article to cabin off entirely the topic of intelligence agencies. Some of the most important judicial decisions in Germany concerning telecommunications surveillance emerged in cases involving that country's intelligence agencies. Since that case law also has much to say about surveillance by domestic law enforcement agencies, this Article discusses these opinions.

concerns the relative levels of such activity in Germany and the United States. This Article demonstrates, however, that the available statistics do not permit the drawing of conclusions about the relative amount of surveillance activities in the two countries.[2] Any comparison based on these data sets proves to be illusory—the statistics measure different phenomenon.

Despite an absence of a basis for an empirical exploration of the relative levels of telecommunications surveillance in Germany and the United States, it is nevertheless possible to compare the legal regulation of telecommunications surveillance in the two countries. In Part I, this Article considers the comparative scholarship—and methodology—of James Q. Whitman. Whitman's scholarship concerning the "law of civility" offers a profound reminder that even "cultural near neighbors," such as Germany and the United States, can have deep-seated differences in their legal cultures—and ones that can prove difficult to explain.[3] In its own exploration of differences in U.S. and German telecommunications privacy law, this Article examines countries that have two great similarities: both Germany and the United States are democracies and have technologically advanced telecommunications systems.[4]

In Parts II and III, this Article considers the comparative constitutional law for telecommunications privacy in these two nations. It begins with U.S. law and in Part II analyzes a series of decisions by the U.S. Supreme Court that have taken it largely out of the business of developing constitutional standards for telecommunications privacy. The Supreme Court has interpreted the Fourth Amendment, the critical part of the U.S. Constitution in this regard, as protecting neither stored data in the control of third parties nor information that falls short of being the "content" of conversations carried by telecommunications.[5] Such non-content, or as this Article refers to these data, "telecommunication attributes," are generally free from Fourth Amendment protection.[6]

2. *See infra* Part I.

3. James Q. Whitman, *Enforcing Civility and Respect: Three Societies*, 109 YALE L.J. 1279, 1282 (2000).

4. As the Central Intelligence Agency states, "Germany has one of the world's most technologically advanced telecommunications systems." Germany: Communications, *in* Central Intelligence Agency, World Factbook (2002), *available at* http://www.cia.gov/cia/publications/factbook/gm.geos/html#Comm [hereinafter C.I.A World Factbook]. For the United States, the same source states that this country has "a very large, technologically advanced, multipurpose communications system." United States: Communications, *in* C.I.A., World Factbook, *supra*, *available at* http://www.cia.gov/cia/publications/factbook/geos/us.html#Comm.

5. For analysis of the text of the Fourth Amendment, *see* text accompanying note 63.

6. I use the term "telecommunications attributes" in the same sense that Susan Freiwald defines "communication attributes": rather than content, telecommunications attributes are "all the other characteristics of a communication that can be learned about it." Susan Freiwald, *Uncertain Privacy: Communication Attributes After the Digital Telephony Act*, 69 S. CAL. L.

In Part III this Article finds that, in marked contrast to U.S. law, German constitutional law regarding telecommunications surveillance is well thought out as a doctrinal matter—indeed, it is based on paradigms likely to lead to more useful judicial review of telecommunications statutes in our Information Age than the U.S. constitutional regime. The postwar German constitution, the Basic Law, protects telecommunications secrecy in its Article 10.[7] In a series of important decisions, the German Constitutional Court has interpreted Article 10 as protecting not only telecommunications content but also telecommunications proceedings. The Constitutional Court has been squarely involved in judicial review of measures that affect telecommunications privacy.

Part IV of this Article shifts from constitutional to statutory law. and compares the statutory law for telecommunications privacy in Germany and the United States. At the statutory level, the two legal systems share both similarities and dissimilarities. Part IV evaluates the regulation of the two countries by examining six categories: (1) legal protection for customer information; (2) legal protection for connection data; (3) legal protection for stored data; (4) legal requirements for data retention or data erasure; (5) legal protection for contents of telecommunications; and, finally, (6) the nature of available remedies.[8]

One set of findings for Part IV follows logically enough from the respective constitutional law in the two countries. Just as German constitutional law does not rely on a distinction between content and non-content, its statutory law does not draw on radically different tests for judging law enforcement requests for content or connection data. To be sure, German law does allow law enforcement greater flexibility in obtaining connection data than content. Yet, German law also provides connection data with relatively higher legal safeguards before disclosure than U.S. law provides to similar information. Moreover, stored data, which are free from Fourth Amendment safeguards in the United States, do not represent a constitutional or statutory category in Germany. This category, which proves quite significant in U.S. statutory law, is not a jurisprudential category in German telecommunications privacy law.

The final finding of this Article's Part IV concerns data erasure and data retention. In the United States, the law requires neither erasure nor retention of telecommunications data. Under current German

REV. 949, 953 (1996). She adds: "These attributes include the existence, duration and subject matter of a communication, the identities of the parties to it, their physical locations and their electronic addresses." *Id*.

7. For analysis of the text of Article 10, Basic Law, *see* text accompanying notes 110–19.

8. For five of the six categories, I proceed in a similar fashion. I first discuss the basic category (e.g., what is "customer data"?) and then examine the legal test for obtaining the information in Germany and the United States. The issue of data retention or data erasure does not involve a test for obtaining information, however, but rather certain obligations placed on the use of information. Hence, this section follows a different format.

telecommunications law, in contrast, a general requirement exists for erasure. As a specific example, telecommunications connection data must be erased after no longer than six months. At present, German law has no requirement of mandatory data retention, but this area is one of current controversy. Indeed, the controversy is occurring not only in Germany, but in the European Union and beyond. The U.S. government is taking a role as an international lobbyist for such a data retention requirement in other countries.[9]

Finally, Part V analyzes other areas of possible influence on the United States and German "clay" of telecommunications surveillance law. The telecommunications law on the books may not be the only influence on law enforcement behavior within the two countries; other "X" factors might be at work. In particular, three other possible influences may exist on telecommunications surveillance in the United States and Germany beyond telecommunications law.[10]

I. Whitman's World of "Civility" and Comparative Wiretap Statistics

In both the United States and Germany, a well developed law of "information privacy" exists. In process-oriented terms, information privacy represents the creation and maintenance of rules that structure and limit access to—and use of—personal data.[11] These rules are sometimes found in social norms, such as the idea of limits on sharing intimate information about one family member with non-family members (gossip).[12] Rules of information privacy are also found in constitutional and statutory law. This Article will compare German and U.S. approaches to a small subset of information privacy law—telecommunications surveillance.

A. Whitman's World of "Civility" and Comparative Law Methodologies

How does one assess telecommunications privacy in two countries on a similar yardstick? One comparative method centers on law—and it is this

9. *See* Richard Norton-Taylor & Stuart Millar, *Privacy Fear over Plan to Store Email*, GUARDIAN, Aug. 20, 2002 (noting that the United Kingdom, "encouraged by Washington, has been pushing for a compulsory E.U.-wide data retention regime"), *available at* http://www.guardian.co.uk/netprivacy/article/0,2763,777574,00.html.

10. *See infra* Part V.

11. For a discussion of this process-oriented definition, see PAUL SCHWARTZ & JOEL REIDENBERG, DATA PRIVACY LAW 5–6 (1996). For a normative definition, see Paul M. Schwartz, *Internet Privacy and the State*, 32 CONN. L. REV. 815, 834–43 (2000) [hereinafter Schwartz, *Privacy and the State*]; Paul M. Schwartz, *Privacy and Democracy in Cyberspace*, 52 VAND. L. REV. 1609, 1658–66 (1999) [hereinafter Schwartz, *Privacy and Democracy*].

12. Interestingly enough, and as a contrasting view to this example, norm theorists sometimes like gossip and dislike privacy, which is considered as merely an obstacle to norm formation. *See, e.g.*, ROBERT ELLICKSON, ORDER WITHOUT LAW 285 (1991) (calling for "improved circulation of accurate reputational information").

Article's approach. This Article discovers that, at least in certain ways, Germany has created a superior legal regime for regulating telecommunications surveillance. In certain other respects, however, the legal regulations of Germany and the United States prove quite similar.

But can one go beyond the letter of the law and engage in any broader sociological observations regarding telecommunications surveillance and telecommunications privacy? For example, can one compare the relative amount of wiretapping activity in Germany and the United States? This Article finds that making this kind of empirical comparison is not possible at present. This Part discusses the difficulties in finding an empirical basis for a comparative sociology of telecommunications surveillance law in Germany and the United States. I first discuss and draw contrasts with James Q. Whitman's comparative project concerning the "law of civility."[13] I then analyze the difficulties in drawing empirical conclusions regarding the relative amounts of telecommunications surveillance in Germany and the United States.

In an insightful work of comparative law scholarship, Whitman examined the law of insult, hate speech, and sexual harassment, and found that Germany has a historical tradition of protecting "honor" for which no equivalence exists in the United States.[14] Whitman describes, for example, how the German law of insult criminalizes the lack of respect for another person.[15] It might even be possible to be punished by the German legal system for making a gesture called the "bird": "the tapping of the index finger on the forehead" to indicate "that another is mentally defective."[16]

In dialogue form, Whitman reports a conversation that he had more than once with Germans:

> American: You mean it's illegal to make a gesture like that in Germany?
>
> German: You mean it's not illegal in America?[17]

Whitman's work is a profound reminder that even cultural near neighbors, such as Germany and the United States, can have legal differences that prove difficult to explain. As noted in this Article's introduction, Whitman sagely observes, "[t]he clay of one place is not much like the clay of another."[18] This Article will attempt to explore the differences in United States and German "clay" regarding telecommunications surveillance. It begins this exploration by considering a methodological question that Whitman's article does not directly

13. Whitman defines the law of civility as "the practices that involve showing respect to others." Whitman, *supra* note 3, at 1289. He distinguishes this behavior from decency, which involves "practices that aim to avoid giving offense or calling attention to gross or bestial aspects of life." *Id.*

14. *Id.* at 1295–1343; 1371–90.

15. *Id.* at 1296.

16. *Id.*

17. *Id.* at 1297.

18. *Id.* at 1296.

address—how does one demonstrate that the "clay" of one place is different than another's?

In his analysis of Germany and the United States, Whitman carefully traces differences regarding civility in different legal systems.[19] In other words, Whitman's "clay" largely consists of laws and legal mechanisms in the different countries. Thus, he looks at German statutes that penalize the lack of respect for another person and shows that no such equivalent legal regulation exists in the United States. Whitman also engages in a fascinating historical exploration of the roots of the different conceptions of civility in Germany and the United States and also considers novels and newspaper accounts.[20] A reader is soon convinced that Whitman has sifted through and weighed everything that relates to his topic.

Yet, Whitman does not marshal compelling evidence to prove that Germans are indeed more civil than Americans.[21] At one point, he complains:

> My goal . . . is to show that the United States displays a relative lack of civility, both in its social practices and in its law. Showing such relative differences is the great strength of comparative law; showing such differences does not, of course, imply that the United States has any absolute lack of civility. To readers to whose minds exceptions spring, let me therefore emphasize: This is a comparative study![22]

One wonders what the term "comparative study" is intended to excuse. And, regarding a counter-example, my own preference would certainly be to wait on line in a store in any city in the United States rather than in one in Germany.[23] Moreover, judging from my wife's experience, the comparative readiness to help a mother traveling with a baby in a stroller in public areas in New York, yes, New York, far exceeds that of Berlin or its suburbs. And if this issue is not one of civility, what is?

To be sure, Whitman does attempt to locate empirical evidence. For example, he points to statistics showing a rapid increase in insult citations and complaints during the 1990s in Berlin.[24] One wonders, nevertheless, whether such litigation points to interpersonal conflicts that find release in

19. Whitman's article also contains an analysis of civility law in France, *id.* at 1344–71, but I concentrate here on his look at Germany and the United States.

20. Whitman also analyzes relevant legal texts from antiquity, *see, e.g.*, *supra* note 16.

21. Indeed, his article at times appears to reason back from a conclusion regarding comparative civility levels in different countries. Thus, he writes, "America is a place where interpersonal relations have always been a bit rough by comparison with many other parts of the world." Whitman, *supra* note 3, at 1280. Whitman also dismisses possible counter-examples prophylatically in language that I have cited in the text. *See* text accompanying note 22.

22. Whitman, *supra* note 3, at 1372.

23. John Bauman III, my editor at the *Hastings Law Journal*, based on his own time spent living in Germany, agrees with me regarding the comparative merits of waiting in line in the two countries. This phenomenon may relate to different concepts of personal space in the two countries.

24. *Id.* at 1300 n.58.

other legal venues in the United States. Next door neighbors in Marin County, California who insult each other following a dispute over a fence, for example, may simply sue each other regarding the borders of their property rather than the words that each person said.

The fence example also leads to a final methodological point. Robert Ellickson's pathbreaking study of law and norms in rural Shasta County, California discovered a strong norm *against* litigation of interpersonal disputes between neighbors in that area.[25] The fence example makes one wonder whether remaining distinctions in the law of civility that Whitman discovers are largely a result of contemporary Germany being generally less rural and more urban, or put differently, far more densely populated than the United States.[26] German civility law may reflect not only a particular German legal history, but also serve a unique role in a highly urbanized and densely populated contemporary Germany.[27]

At any rate, civility is a tough matter to prove or disprove. What about telecommunications privacy? One would think that evaluating comparative levels of telecommunications surveillance activity in any two countries to be an easy task. This assumption proves, alas, false—at least when the two countries in question are Germany and the United States. The next section discusses why comparison of the respective levels of surveillance activity in these nations proves impossible.

B. Some Comparative Statistics

According to Mark Twain, the British Prime Minister Benjamin Disraeli once remarked upon three kinds of falsehoods: "lies, damned lies, and statistics."[28] Official yearly statistics are in fact available that report upon the judicial orders issued for surveillance of the "content" of telecommunications in Germany and the United States. Yet, profound differences exist in both the underlying respective legal regimes for telecommunications surveillance and the way that statistics for German and United States telecommunications surveillance activity are collected. As a

25. ELLICKSON, *supra* note 12, at 184–91.

26. The F.R.G. is a country slightly smaller than Montana. Its population is eighty-three million people; Montana, according to the 2000 Census, has 902,000 residents. MONT. DEP'T OF COMMERCE, CENSUS AND ECON. INFO. CTR., POPULATION OF COUNTIES IN MONTANA, 1890 TO 2000, *at* http://ceic.commerce.state.mt.us/Demg/historic/Censuscounty1890-2000.pdf.

27. As possible corroboration of this point, Whitman cites in a footnote to a German study that identified the most frequent setting for insults in Germany that led to litigation. The study, which looked at cases between 1957 and 1965, found the most frequent setting for an insult to be "the common area of an apartment building." Whitman, *supra* note 3, at n.45. This same study found that cases of insult also most often arise both "in the month of August when warmer weather is conducive to more frequent social interaction" and "between the hours of 4 p.m. and 8 p.m. when the pent-up frustrations of the day are finally released." *Id.* at n.71.

28. MARK TWAIN, THE AUTOBIOGRAPHY OF MARK TWAIN 149 (Charles Neider, ed., 1990) (1959).

consequence, any comparison of the relative level of activity in the two countries would belong in the Twain-Disraeli category of "lies" and "damned lies."

As an initial observation and on a more positive note, however, certain comparisons *are* possible based on the statistics in Germany and the United States concerning telecommunications surveillance. First, in both countries, investigations relating to narcotics violations generate the highest percentage of surveillance orders.[29] In Germany, violations of the narcotics law provided justification in fifty-nine percent of the proceedings in 2000 in which wiretaps or other telecommunications are sought.[30] In contrast, the three categories of crimes that generated the second and third highest percentages of surveillance orders were (1) murder, manslaughter, or genocide at seven percent; (2) robbery or theft at six percent; and (3) criminal violations of the asylum and refugee statutes at six percent.[31] In the United States, with the most recent statistics dating from 2001, seventy-eight percent of all applications for interceptions cited drug offenses as the most serious offense being investigated.[32] The highest percentage of drug-related interceptions in that year (sixteen percent of the total) came from the New York City Special Narcotics Bureau.[33] The second and third most prevalent type of offense investigated with wiretap orders were gambling (5.5 percent) and racketeering (five percent).[34]

Second, in both countries, law enforcement agencies in certain geographic areas generate a disproportionate amount of surveillance orders. In the United States, state law enforcement officials generate far more wiretaps than federal officials, and a few states are responsible for the most wiretaps.[35] For example, state judges authorized 1,005 of the 1,491 wiretaps issued.[36] Seven states were responsible for ninety-three percent of all authorizations by state judges: New York (425 applications), California (130 applicants), Illinois (128 applications), New Jersey (99 applications), Pennsylvania (54 applications), Florida (51 applications), and Maryland (49 applications).[37] In Germany, data are available that break down state-by-state the number of criminal trials in which wiretap evidence has been used in a given year. These data have then been further ranked by the

29. Johann Bizer, Praxis der TK-Ueberwachung, 26 Datenschutz und Datensicherung 216, 218 (2002); ADMIN. OFFICE OF THE U.S. COURTS, 2001 WIRETAP REPORT 10 (2001) [hereinafter 2001 WIRETAP REPORT]; ADMIN. OFFICE OF THE U.S. COURTS, 2000 WIRETAP REPORT 10 (2001) [hereinafter 2000 WIRETAP REPORT].

30. Bizer, *supra* note 29 at 218. In these German statistics, it is possible for a single proceeding in which a wiretap was authorized to involve several crimes. *Id*.

31. *Id.* at 218.

32. 2001 WIRETAP REPORT, *supra* note 29 at 9.

33. *Id.*

34. *Id.*

35. 2001 WIRETAP REPORTS, *supra* note 29, at 7. *Id*.

36. *Id*

37. *Id*.

relative population of each state (trials with wiretap evidence per 100,000 inhabitants). In the year 2000, these ranged from a high of 8.27 for such trials in Hamburg, to 4.04 in Berlin, and 2.23 for North Rhine-Westfalia.[38] Johann Bizer observes that these differences cannot be alone attributed to the varying "population structures" in the different states (as Hamburg, for example, has a similar population makeup to Berlin). Bizer also points to significant statistical differences in surveillance rates between states with similar conservative governments, such as Baden-Württemburg (5.15 trials with wiretap evidence per thousand inhabitants) and Bavaria (3.53 trials). These differences indicate that in both Germany and the United States law enforcement requests for telecommunications surveillance are driven by local enforcement norms as well as any law on the books.

To turn to an exploration of the difficulties of a statistical comparison concerning relative levels of surveillance, one can begin by noting that yearly statistics are collected in both Germany and the United States regarding the judicial orders that authorize surveillance of telecommunications "content." An initial glance at the numerical data would also leave one sanguine as to the possibilities of comparison. Particularly promising in this regard is that both countries define the term "content" in a similar fashion. The United States Code defines "content" of telecommunications as "any information concerning the substance, purport, or meaning" of "any wire, oral or electronic communications."[39] Germany utilizes a similar concept of "content," although the term itself is not defined in German statutory law.[40] In Germany, surveillance of the content of communications is primarily regulated by section 100a of the Federal Code of Criminal Procedure (*Strafprozessordnung*).[41] The equivalent regulation in the United States is found in Title III of the Omnibus Crime Control Act of 1968.[42]

Relative population statistics should also be noted at this point. The United States has 287 million residents, more than three times more than Germany, with 83 million residents.[43] The population figures appear, at least initially, significant because the raw (and, as we shall see, misleading) comparative statistics seem to indicate that, even without adjusting for population differences, German law enforcement agencies engage in far more wiretapping.

38. Bizer, *supra* note 29, at 218.

39. 18 U.S.C. § 2510(8) (2003).

40. For a discussion, see *infra* Part IV.E.

41. § 100a StPO. For concise analysis of this section of the law, see GERD PFEIFFER, STRAFPROZESSORDNUNG, § 100a, at 206–13 (4th ed. 2002).

42. 18 U.S.C. §§ 2510–22.

43. All population figures are from the C.I.A., World Factbook, *supra* note 4. For Germany, see People: Germany, *available at* http://www.cia.gov/ciapublications/factbook/geos/gm.html#Intro. For the United States, see People: United States, *available at* http://www.cia.gov/ciapublications/factbook/geos/us.html#People.

During the year 2001, the last period for which we have statistics for both countries, Germany issued 23,806 surveillance orders for telecommunications content, whereas the United States issued 1,405 orders.[44] The comparative statistics for past years are similar: in 2000, Germany issued 15,741 surveillance orders, and the United States 1,910.[45] In 1999, Germany issued 12,651 surveillance orders, and the United States, 1,350.[46] In 1998, Germany issued 9,802 surveillance orders, and the United States, 1,327.[47] Finally, in 1997, Germany issued 7,762 surveillance orders, and the United States, 1,149.[48] Yet, as noted, these statistics can not be compared to one another because they measure different phenomena.

To begin with, the United States statistics require certain "back of the envelope" adjustments. One such adjustment is needed because the United States data likely do not completely reflect state, as opposed to federal, surveillance activities. With the pro bono support of the law firm Morrison & Foerster, the bipartisan "Constitution Project" recently carried out a survey of state developments regarding surveillance law.[49] The Constitution Project noted that only twenty-five of the forty-six states that permit surveillance reported their activities in 2001 to the Administrative Office of the Federal Court.[50] It may be that all, some, or none of these states engaged in telecommunications surveillance. The Administrative Office of U.S. Courts does not require reports to be filed if there is no interception activity in a state during a given year.[51] The Constitution

44. 2001 WIRETAP REPORT, *supra* note 29, at 9. The U.S. Wiretap Reports are posted online at http://www.uscourts.gov/wiretap.html. For the German statistics for 2001, see Regulierungsbehörde für Telekommunikation und Post, Jahresstatistik nach § 88 Abs. 5 TKG (2002) (on file with *Hastings Law Journal*).

45. For the United States, the information is found in the 2000 WIRETAP REPORT 5 (2001). For the German statistics, see Bizer, *supra* note 29, at 217.

46. ADMIN. OFFICE OF THE U.S. COURTS, 1999 WIRETAP REPORT 5 (2000); Bizer, *supra* note 29, at 217.

47. ADMIN. OFFICE OF THE U.S. COURTS, 1998 WIRETAP REPORT 5 (1999); Bizer, *supra* note 29, at 217.

48. ADMIN. OFFICE OF THE U.S. COURTS, 1997 WIRETAP REPORT 5 (1998); Bizer, *supra* note 29, at 217.

49. For more information, see The Constitution Project, Liberty and Security Initiative Main Page: Privacy and Technology, *at* http://www.constitutionproject.org/ls.index.html.

50. Charles H. Kennedy & Peter P. Swire, State Wiretaps and Electronic Surveillance After September 11, 54 HASTINGS L.J. 971, 972–73. The paper commented that reporting of state interception activities may be less thorough than reporting of federal intercepts." *Id.* at 973. *See also* 18 U.S.C. 2519(1) (requiring filing of reports with the Administrative Office of the U.S. Courts requiring each order or extension that has been requested).

51. Admin. Office of the U.S. Courts, Reporting Requirements on Intercepted Wire, Oral, or Electronic Communications 2 (on file with *Hastings Law Journal*). The statutory requirements for filing reports obligate judges who issue or deny surveillance orders as well as state prosecuting attorneys and other officials to file information about these orders. 18 U.S.C. § 2519 (2003).

Project was unable, at any rate, to discover the level of surveillance in the missing states.

As a rough "back of the envelope" revision, one might simply double the number of state wiretaps in the United States and adjust the total number of U.S. wiretaps upwards. Such a relative hefty adjustment may be justified due to the large increase in recent years in *state* as opposed to *federal* surveillance orders in the United States.[52] As already noted, in 2001, for example, state judges authorized 1,005 of the 1,491 wiretaps approved in the United States in that year.[53] A further adjustment upwards also appears necessary because the data for the United States do not include order extensions, which are included in the German numbers. Fortunately, the order extensions are listed—albeit as a separate item—in the annual reports on wiretap activities from the Administrative Office of the Courts.[54] All of these adjustments to the U.S. data set are possible and would seem to leave the number of U.S. surveillance orders significantly below the German numbers.

Ultimately, however, any attempt at an empirical comparison collapses due to three differences in how the statistics in the United States and Germany are maintained. These differences reflect underlying distinctions in the legal regulation of telecommunications surveillance in the two countries. We will consider these differences in ascending order according to the difficulty that they present to drawing conclusions about the relative levels of surveillance activity in the two countries.

First, roving wiretaps are permitted in the United States, but not in Germany. Since 1986 U.S. law has permitted domestic law enforcement agencies to issue these orders, which are centered around a suspect and not any specific telecommunications connection.[55] The USA PATRIOT Act in 2001 granted roving wiretap authority to intelligence agencies.[56] In contrast, a suspect in Germany with access to numerous telecommunications devices (such as multiple fixed line telephones in different locations, cell phones, e-mail accounts, pager devices) cannot be made subject to a single surveillance order tied to her person.[57] As a result, a single roving wiretap order in the United States involves activity that is counted by several surveillance orders in Germany. Although judges issue only a small amount of roving wiretap orders in any given year in the

52. 2001 WIRETAP REPORT, *supra* note 29, at 5.

53. *Id.*

54. For the 2001 extensions, see *id.* at 8. In 2001, 1,008 extensions were requested and authorized. *Id.*

55. The United States permits waiving the requirement that the government specify the facilities to be subject to a court order when "there is probable cause to believe that the person's actions could have the effect of thwarting interception from a specified facility." 18 U.S.C. § 2518(11) (2003).

56. USA PATRIOT Act § 206, codified at 50 U.S.C. § 1805(c)(2)(B) (2003).

57. *See* Bizer, *supra* note 29.

United States, there is also an absence of data about how many devices are included per roving wiretap order in the United States.[58] Thus, I have chosen to list this issue on the far side of the "comparative statistics" divide.

Second, German wiretap statistics reflect a separate counting for each time that a telecommunications connection (*Anschluss*) is placed under surveillance. In other words, the German law enforcement statistics, which are issued by the Regulatory Authority for Telecommunications and Mail (*Regulierungsbehörde für Telekommunikation und Post*), do not count merely the *orders* that are issued, but the *connections* that are placed under surveillance. In contrast, in the United States, a single judicial order can be used to place surveillance on multiple lines. As the 2001 Wiretap Report concisely states, "[n]o statistics are available on the number of devices installed for each authorized order."[59] In other words, the annual reports in the United States do not provide any breakdown as to the number of connections placed under surveillance—only on the number of judicial orders. A single wiretap order in the United States can reflect one, three, eight, or more connections being placed under surveillance.

Third, Germany does not allow a "consent" exception to its requirement for surveillance orders. In Germany, constitutional protection remains in place unless *all* parties to a communication consent to surveillance.[60] This result follows because Article 10 of the German constitution safeguards confidentiality for participants in telecommunications. In contrast, under U.S. constitutional and federal statutory law, any single individual's consent to surveillance of telecommunications to which she is a party releases the government from any obligation to seek a judicial order.[61] Consequently, an unknown number of "consent" wiretaps in the United States fall outside of the U.S. statistics whereas in Germany similar law enforcement activities are counted in the national wiretap statistics.

Thus, the German statistics include numerous surveillance requests that are not included in the U.S. statistics. The respective German and U.S. statistics regarding surveillance orders end by measuring different phenomena. Moreover, it is not possible to adjust the respective data sets to account for the underlying differences. As a result of these difficulties with the data, one cannot make any judgments regarding the respective levels of domestic surveillance activity in Germany and the United States.

58. Thus, in 2001, sixteen roving wiretaps were authorized in the United States. 2002 WIRETAP REPORT, *supra* note 29, at 9.

59. 2001 WIRETAP REPORT, *supra* note 29, at 6. Moreover, the Administrative Office of the United States Courts explicitly requests that the reports filed with it *not* include the phone numbers of persons intercepted. ADMIN. OFFICE OF THE U.S. COURTS, *supra* note 51, at 5.

60. *See infra* Part I.A.

61. *See infra* Part II.

As a modest proposal, however, one can suggest that the collection of the United States data be altered to include the number of connections that are placed under surveillance.[62] Until the U.S. statistics include this information, they measure less the amount of surveillance undertaken by law enforcement agencies than the amount of instances of surveillance oversight by the judicial branch. Furthermore, the law in the United States should require all states to file an annual report with the responsible federal official even if no surveillance activity takes place in a particular year. Having noted the absence of adequate comparative statistics, this Article now turns to the different aspects of the constitutional and statutory law regulating telecommunications surveillance in the United States and Germany. Finally, Part V of the Article considers three additional areas that may exert influence on the two regimes of telecommunications surveillance.

II. U.S. Constitutional Law and Telecommunications Privacy: Non-Content Data, Stored Information, and the Fourth Amendment

In American law, the Fourth Amendment is the critical constitutional provision regarding telecommunications surveillance. The Fourth Amendment first establishes the right of the people to be secure from "unreasonable searches and seizures" in their "papers, and effects." It also prohibits the issuing of search warrants on less than "probable cause." The text of this Amendment raises numerous interpretative issues, not the least of which is the relationship between the "unreasonable search" prohibition and the "probable cause" requirement for search warrants.[63] For our purposes, however, the most important issue for telecommunications privacy concerns the kind of behavior that is considered a search for Fourth Amendment purposes.

In two areas, the Supreme Court has interpreted the Fourth Amendment in a fashion that leaves telecommunications surveillance largely free from constitutional restrictions. The first set of relevant decisions finds the Fourth Amendment to be inapplicable to data stored in the control of third parties. The second set of decisions declares this amendment inapplicable to telecommunications attributes that fall short of

62. Improvements are also possible in the German telecommunication surveillance statistics. For example, Bizer wishes to see a breakdown that includes the name of the state officials who sought the surveillance order and the alleged crime investigated. Bizer, *supra* note 29, at 218. This kind of information would give a sense of whether certain jurisdictions within a state were generating a disproportionate number of wiretap orders.

63. For a discussion of the relationship between these two clauses, see Silas J. Wasserstrom & Louis Michael Seidman, *The Fourth Amendment as Constitutional Theory*, 77 GEO. L.J. 19, 80–84 (1988); Silas J. Wasserstrom, *The Incredible Shrinking Fourth Amendment*, 21 AM. CRIM. L. REV. 257, 281–304 (1984).

being the "content" of a telephone conversation. The Supreme Court had articulated the controlling case law by the end of the 1970s. Barring a reversal of both strands, the most critical decisions regarding telecommunications privacy will necessarily take place on the statutory level and free from constitutional constraints.

Why is the Fourth Amendment not applicable to data stored in the control of third parties? Why does it not apply to a wide range of telecommunications attributes, which become mere non-content within the logic of the current constitutional privacy paradigm?

Concerning data stored in the control of third parties, the Supreme Court addressed this issue in 1976 in *United States v. Miller*.[64] The defendant claimed a Fourth Amendment interest in bank records, whether consisting of microfilms, checks, deposit slips or other records.[65] The defendant's claim before the Supreme Court was that the bank records were "merely records of personal records that were made available to the banks for a limited purpose and in which he has a reasonable expectation of privacy."[66] The *Miller* Court rejected this argument—it stated that there was no "legitimate 'expectation of privacy' in the particular documents."[67] These documents were not private papers, but merely "the business records of the banks."[68]

The Court based its finding regarding the lack of a privacy interest in bank records on a "risk" analysis. As Justice Powell wrote for the majority, "[t]he depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[69] Thus, the Court was not interested in the subjective privacy expectations of the bank depositor; the Court was unmoved by the defendant's argument that he had revealed the data "on the assumption that it will be used only for a limited purpose and that the confidence will not be betrayed."[70] The bank customer bears the risk that the government may prove interested in her banking records. As Daniel Solove summarizes the Court's logic, "since information maintained by third parties is exposed to others, it is not private, and therefore not protected by the Fourth Amendment."[71]

The "risk analysis" also suggests the absence of constitutional protection if a party to a communication offers her consent to state surveillance. In the United States, one bears the risk that any party to whom one reveals her affairs will share this information with the

64. 425 U.S. 435 (1976).
65. *Id.* at 440–42.
66. *Id.* at 442.
67. *Id.*
68. *Id.* at 440.
69. *Id.* at 443.
70. *Id.* at 442.
71. Daniel Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1087 (2002).

government. For example, if one party consents to telecommunications surveillance, the government need not obtain a judicial order to engage in wiretapping. Beyond "risk analysis," the Supreme Court has also justified the "consent exception" in a different fashion. This judicial analysis occurred in a case involving a consent to a search of shared physical premise, but is equally applicable to the telecommunications context. In that case, the Court found that permitting third-party consent to searches by government bolstered a societal interest in discovering and punishing crime as well as the citizen's interest in aiding law enforcement.[72]

Statutory law provides no more protection than constitutional law regarding a single party's consent to government surveillance of telecommunications.[73] As the Department of Justice's manual on obtaining electronic evidence notes, the relevant statutory language authorizes monitoring "when one of the parties to the communication consents to the interception."[74] Consent can be either express or implied.[75]

The lack of a constitutional privacy interest in third party records also played an important role in the establishment of the Supreme Court's distinction between "content" and telecommunications attributes. This distinction emerged over the course of several opinions, the most important of which were *Katz v. United States*, decided in 1967, and *Smith v. Maryland*, decided in 1979.[76] Other significant cases in this series are *Berger v. United States* (1967), and a decision I have already mentioned, namely *Miller v. United States* (1976).[77]

The first step in drawing the content/non-content distinction was *Katz v. United States*, in which the Court decided that a device for recording conversations placed on the outside of a public phone booth implicated the Fourth Amendment.[78] It stated that the "Fourth Amendment protected people, not places," and found that this Amendment's protections extended to communications which the individual "seeks to protect as private, even in an area accessible to the public."[79] In entering the phone booth, the petitioner had sought to exclude "the uninvited ear" from hearing the

72. Schneckloth v. Bustamonte, 412 U.S. 218 (1973). For further analysis, see Mary I. Coombs, *Shared Privacy and the Fourth Amendment, or the Rights of Relationships*, 75 CAL. L. REV. 1593, 1640–42 (1987).

73. 18 U.S.C. § 2511(2)(c) & (d) (2003).

74. U.S. DEP'T OF JUSTICE, COMPUTER CRIME AND INTELLECTUAL PROPERTY SECTION, CRIMINAL DIVISION, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS § IV(3)(b) (July 2002), *available at* http://www.cybercrime.gov/s&smanual2002.html [hereinafter DOJ, SEARCH & SEIZURE MANUAL].

75. *Id.*

76. Katz v. United States, 389 U.S. 347 (1967); Smith v. Maryland, 442 U.S. 735 (1979).

77. Berger v. United States, 388 U.S. 41 (1967); United States v. Miller, 425 U.S. 435 (1976).

78. *Katz*, 389 U.S. at 348.

79. *Id.* at 351–52.

content of his conversation.[80] As a result, the petitioner was "entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world."[81]

In *Berger*, another case from 1967, the Supreme Court defined the constitutional parameters for surveillance of the content of communications. It found the Fourth Amendment to require the interposition of "a neutral and detached authority" between the police and the public before the issuing of a order for surveillance of content.[82] The *Berger* Court also articulated a particularization requirement regarding the crime to be investigated and the conversations sought to be captured. Surveillance is also permissible only when subject to a termination date.[83] Congress quickly reacted to *Katz* and *Smith* and enacted Title III of the Omnibus Crime Control Act of 1968. Title III expressed statutory guidelines, pursuant to *Katz* and *Berger*, that set conditions for the wiretapping of telephone conversations.[84]

The next stage in the development of the Court's jurisprudence of telecommunications privacy occurred in 1979 with *Smith v. Maryland*.[85] This case saw the full and final emergence of the Supreme Court's distinction between "content" and "non-content," or in the terminology of this Article, between "content" and "telecommunication attributes." *Smith* concerned law enforcement use of a "pen register," a device for recording telephone numbers dialed.[86] A similar device, the "trap and trace" device, is used by law enforcement agencies to capture the numbers received by a telephone.[87]

In *Smith*, the police had placed a pen register on the phone of a person accused of making threatening phone calls.[88] Thus, in contrast to *Katz*, the *Smith* Court addressed police behavior that captured the numbers dialed from a phone, but not the words spoken in a conversation. In the judgment of the Supreme Court, installation of a pen register did not constitute a search within the meaning of the Fourth Amendment.[89] Reaching back to Justice Harlan's concurrence in *Katz*, the *Smith* Court noted that the application of the Fourth Amendment depended on "whether the person

80. *Id.* at 352.

81. *Id.*

82. *Berger*, 388 U.S. at 54.

83. *Id.* at 60.

84. Title III is now codified at 18 U.S.C. §§ 2510–22 (2003).

85. Smith v. Maryland, 442 U.S. 735 (1979)

86. *Id.* at 736 n.1.

87. For discussion of the two devices, see Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't*, 97 NW. U. L. REV. 607, 631–33 (2003). Susan Freiwald has noted the expanded capacity to record new kinds of telecommunication attributes of new generation pen registers for use in surveillance of pagers and cellular phones. Freiwald, *supra* note 6, at 987–99.

88. *Smith*, 442 U.S. at 737.

89. *Id.* at 742–45.

invoking its protection can claim a 'justifiable,' a 'reasonable' or a 'legitimate expectation of privacy.'"[90] The Court made further use of Harlan's opinion by accepting his division of the necessary inquiry into two distinctive elements.[91] The first element looked to the presence of a "subjective" expectation of privacy. Did an individual exhibit a personal belief that his behavior was private? Or, to put the inquiry slightly differently, had the individual "shown that 'he seeks to preserve [something] as private'"?[92] The second inquiry considers whether the individual's subjective expectation of privacy was "reasonable."[93] Was the individual's subjective expectation of privacy, "viewed objectively," one that was "'justifiable' under the circumstances"?[94]

In *Smith*, the Court rejected the idea that either a *subjective* or *objective* expectation of privacy existed in the phone number that one dialed. Both questions were not, however, of equal importance for the *Smith* Court. Indeed, the Court applied the first question in a fashion that collapsed it into the second question. The *Smith* Court looked less for any subjective expectation of the specific defendant than for a subjective expectation of the *reasonable* telephone consumer.

In answering the first question, in other words, the Court evaluated only the basic structure of telephony as it then existed.[95] The *Smith* Court helpfully summarized its findings on this score: "telephone users, in sum, typically know that they must convey numerical information to the phone company; that the phone company has facilities for recording this information; and that the phone company does in fact record this information for a variety of legitimate business purposes."[96] In other words, a reasonable telephone consumer would not have a reasonable expectation of privacy.[97] The answer to the first question, therefore, sounds

90. *Id.* at 740–41. For criticisms of the Court's lack of a methodology for finding a legitimate expectation of privacy, see Wasserstrom & Seidman, *supra* note 63, at 29–32.

91. *Smith*, 442 U.S. at 741.

92. *Id.*

93. *Id.*

94. *Id.*

95. A result of this technical structure is that "[a]ll telephone users realize that they must 'convey' phone numbers to the telephone company, since it is through telephone company switching equipment that their calls are completed." *Id.* at 742. The *Smith* Court continued its analysis of subjective expectations by pointing to other elements in the structure of telephony that prevented any subjective expectation of privacy. Thus, all who used the telephone were obliged to realize that the phone company made permanent records of the numbers that they dialed. After all, phone consumers "see a list of their long-distance (toll) calls on their monthly bills." *Id.* The *Smith* Court also observed that public phone directories informed consumers that the telephone company would be able to help identify persons making annoying phone calls. This announcement pointed as well to a collection of the dialed numbers by the phone company. *Id.*

96. *Id.* at 743.

97. The Supreme Court seemed indecisive, in some of its language as to whether a subjective expectation rested on behavior or belief. After all, the petitioner in the case insisted that he in fact

a lot like the answer to the second question, which concerned the presence of an objective privacy expectation.

Not surprisingly then, the *Smith* Court also found the absence of any objective privacy expectation. In making this evaluation, the Court relied on *Miller* and subsequent decisions that rejected any privacy expectation in information that "a person . . . voluntarily turns over to third parties."[98] At this point, we see the long reach of *Miller*. The *Smith* Court viewed the telephone consumer in terms similar to the banking customer in *Miller*: "[P]etitioner voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business."[99] He bore the risk, in turn, that "the company would reveal to police the numbers he dialed."[100]

Thus, while the Fourth Amendment protects content, as per *Katz*, it reaches neither stored data nor non-content. The results of these cases have been to remove stored content in the control of third parties, non-content, and an ever expanding range of telecommunication attributes from the zone of Fourth Amendment constitutional protection. Speaking of the consequences of this regime for cyberspace, Orin Kerr states, "[t]he Supreme Court's interpretation of the Fourth Amendment has left Internet surveillance law to develop as a primarily statutory field."[101] In broader terms, Solove notes, "we are becoming a society of records, and these records are not held by us, but by third parties."[102] The removal of these records from Fourth Amendment protection means that constitutional strictures do not apply to most of the law of telecommunications privacy in the United States.[103]

This constitutional jurisprudence is problematic. The available kinds of telecommunication attributes are more detailed today than had been possible at the time of *Smith*. These data, the collection of which we will analyze in Part IV, can include: "records of session times and durations"; "any temporarily assigned network address,"; "any credit card or bank account number" used for payment (examples of "customer information" from United States law); and "dialing, routing, addressing and signaling

had enjoyed a subjective expectation of privacy. *See, e.g.*, *id*. From a certain perspective then, the Court was telling him that he did not have the belief that he claimed. *See id.*

98. *Id.* at 743–44.

99. *Id.*

100. *Id.* at 744.

101. Orin Kerr, *Lifting the "Fog" of Internet Surveillance*, 54 HASTINGS L.J. 805, 843 (2003).

102. Solove, *supra* note 71, at 1089. *See* SCHWARTZ & REIDENBERG, supra note 11, at 63 ("[A] precondition to modern life is that increasing amounts of personal information be stored outside an individual's control.").

103. To be sure, the Supreme Court does remain involved so long as the content of telecommunications is involved. *See, e.g.*, Bartnicki v. Vopper, 532 U.S. 514 (2001) (civil damage action under Title III concerning a radio commentator playing a tape of conversation that he had reason to know was illegally intercepted).

information" that is in transmission (examples of "connection data" from United States law).[104]

We should therefore again ponder the *Smith* Court's decision that a list of phone numbers dialed are outside the protection of the Fourth Amendment. Justice Stewart's dissent objected in commonsense terms to the "content" versus "non-content" distinction seized upon by the majority. He wrote, "[t]he numbers dialed from a private telephone—although certainly more prosaic than the conversation itself—are not without 'content.'"[105] Stewart reached this conclusion because a list of this information, even if it were not incriminating, "easily could reveal the identities of the persons and the places called, and thus reveal the most intimate details of a person's life."[106] This observation, already true in 1979 at the time of *Smith*, has only become more telling following the development of digital telephony and mobile telephony.[107]

For Raymond Ku, the Fourth Amendment should play an important role in "preserving the people's authority over government—the people's sovereign right to determine how and when government may intrude into the lives and influence the behavior of its citizens."[108] Ku envisions this authority being exercised through judicial review of the use of new technologies that intrude on the public.[109] However, the Supreme Court's interpretation of the Fourth Amendment in the context of telecommunications surveillance has removed a critical category of searches from constitutional scrutiny.

III. German Constitutional Law and Telecommunications Privacy

We begin our examination of German constitutional law by looking at the relevant constitutional text. Article 10 of the Basic Law, the postwar German constitution, contains both language dating from the initial enactment of the document in 1949 and language added to it through constitutional amendment in 1968. The original text is now found in Article 10(1) and the start of Article 10(2); the language of the 1968 amendment was added to the end of Article 10(2).

In Article 10(1), the German constitution, in language from 1949, declares: "The secrecy of letters, as well as of the post and

104. 18 U.S.C. §§ 2703, 3121 (2003), *see infra* Part IV.

105. *Smith*, 442 U.S. at 748 (Stewart, J., dissenting).

106. *Id.*

107. Susan Freiwald has made a similar point in cataloging the expanded capacity of newer generation "pen registers" in the digital age. Freiwald, *supra* note 6, at 987–89.

108. Raymond Shih Ray Ku, *The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 MINN. L. REV. 1325, 1326 (2002).

109. *Id.* at 1350–67.

telecommunications, is inviolable."[110] At the start of Article 10(2), the Basic Law continues, also in language from 1949: "Restrictions may only be ordered pursuant to a statute."[111] Thus, from the time of the German constitution's promulgation, telecommunications secrecy has been both a fundamental right and one subject to statutory limitations.

Our evaluation of Article 10's original concept of postal and telecommunications secrecy also requires examination of certain other aspects of the Basic Law. In particular, the German constitution places three substantial limits on the ability of the legislature to enact laws that limit Article 10 or other basic constitutional rights. First, statutory law or constitutional amendments in Germany are limited by Article 19's prohibition of constitutional alterations that infringe upon the essence (*Wesensgehalt*) of a fundamental right.[112] Thus, even if made in a procedurally perfect fashion, a statute or a constitutional amendment is nevertheless void if it infringes upon Article 10's core protections for telecommunications privacy.

Second, the "Eternity Clause" of the Basic Law, expressed in Article 79(3), prohibits amendment to the constitution or enactment of statutes that infringe upon the "principles laid down in Articles 1 and 20" of the Basic Law.[113] Of these two provisions, Article 1 has been of the greatest significance in the context of telecommunications secrecy. Article 1 of the Basic Law protects human dignity and places it at the center of the German constitutional order.[114] Article 79(3)'s Eternity Clause forbids any wiretapping or surveillance statute that infringes upon human dignity as protected by the Basic Law.

Finally, the German constitution shapes Article 10 through a requirement that any statute infringing upon a fundamental right be consistent with the constitutional principle of the "rule of law" (*Rechtstaatlichkeit*). The idea of the rule of law finds one of its most important expressions in Article 20, which binds all legislation "to the constitutional order" and the executive and judiciary to "law and justice."[115] The Constitutional Court has used the concept of the "rule of law" to develop the further "principle of proportionality" (*Grundsatz der Verhältnismäßigkeit*).[116] It has developed a three prong test for evaluating

110. § 10 Nr. 1 GG.

111. § 10 Nr. 2 GG.

112. § 19 GG. For a discussion, see HANS D. JARASS & BODO PIEROTH, GRUNDGESETZ FÜR DIE BUNDESREPUBLIK DEUTSCHLAND 471 (2002).

113. § 79 Nr. 3 GG. For a discussion, see JARASS & PIEROTH, *supra* note 112, at 894–97.

114. § 1 GG.

115. § 20 GG. Another important mention of the "rule of law" in the Grundgesetz is found at § 28 GG, which concerns the individual states.

116. For application of the test by the Constitutional Court, see BVerfGE, 100 (1999), 313 (373, 390–96). For a discussion, see JARASS & PIEROTH, *supra* note 112, at 530–34; INGO RICHTER ET AL., CASEBOOK VERFASSUNGSRECHT 22–29 (4th ed. 2001).

the proportionality of legislation. First, a court asks whether the means chosen are suitable (*geeignet*). Second, a court inquires whether the means chosen are necessary (*erforderlich*). Finally, the court examines whether the means chosen are reasonable (*zumutbar*).[117]

Thus far, we have considered the original language of Article 10 and aspects of German constitutional law that limit alterations to it. As noted, however, Article 10 also contains language added to the Basic Law in 1968 through constitutional amendment.[118] This constitutional amendment, the text of which was added to the end of Article 10(2), permits: (1) surveillance to occur without the affected person ever being informed of it; and (2) surveillance without judicial review, but through "a review of the case by bodies and auxiliary bodies appointed by Parliament."[119] However, this amendment permits these two measures only if necessary to protect "the free democratic basic order or the existence or security of the Federation or a state."[120] In sum, the 1968 amendments permit secret surveillance without notice to the affected party and creation of a new governmental body to oversee certain wiretap requests, but only when the national security is at stake.

As one might imagine, there is a story behind this amendment to Article 10. After the Allied Powers defeated the Third Reich in 1945, they carried out surveillance of letters and telecommunications in Germany based on their status as occupying powers.[121] The so-called "Western" Allied Powers, namely, Britain, France and the United States, continued this surveillance within the territory that became the Federal Republic of Germany ("F.R.G.") even after the F.R.G. assumed sovereignty under the Basic Law in 1954.[122] In the Germany Treaty of 1952, the "Western" Allied Powers declared, however, that they would stop surveillance activities in the F.R.G. as soon as the respective German authorities received similar powers under German law.[123]

117. The first test, the idea of suitability, requires legislation to choose means that promote the sought-after objective in some way. This hurdle is the least rigorous of the three; it is similar to rational basis review in U.S. constitutional law. Second, the concept of necessity means that there must be no way to meet the legislative objective that would be less injurious to the citizen's rights. Thus, if enforcement of certain provisions in German criminal law would be possible without telecommunications surveillance, this activity would not be allowed. Finally, the idea of reasonableness, also termed "proportional in the 'narrow sense,'" requires consideration of whether the interference will be commensurate with the sought-after objective. This final branch of the proportionality test requires evaluation of the relation between the selected means and the goals. JARASS & PIEROTH, *supra* note 112, at 530–34; RICHTER ET AL., *supra* note 116, at 22–29.

118. For a discussion by the Constitutional Court, see BVerfGE, 30 (1970), 1 (4–5, 17–19).

119. § 10 Nr. 2 GG.

120. *Id.*

121. BVerfGE, 30, at 4–5.

122. *Id.*

123. *Id.* The promise was not kept. Through an electronic system often referred to as Echelon, the United Kingdom, the United States, and other nations engage in top secret automated interception of telecommunications on a global basis. For an official study of Echelon,

In 1968, the German legislature created such authority for surveillance in German law. It enacted both the amendment to Article 10, discussed above, and a bill, the "Statute for Article 10" (*Gesetz zu Artikel 10*).[124] Following a constitutional challenge to the amendment and statute, the Constitutional Court upheld the constitutional amendment and most of the statute in 1970 in its "Monitoring" opinion (*Abhörurteil)*.[125] The rest of this Part considers this opinion and two other important decisions of the Constitutional Court relating to telecommunications privacy: the "Connection Capture" (*Fangschaltung*) opinion from 1992 and the "BND" (*Bundesnachrichtendienst*) opinion from 1999.[126]

A. The "Monitoring" Opinion

In this decision, the German Constitutional Court began by noting that the Basic Law established a state that was meant to be a "combative democracy" (*streitbare Demokratie*).[127] This constitutional requirement calls for the democratic order to be capable of defending itself from any who would destroy it.[128] The German Court noted that, consistent with this constitutional orientation, it would not allow "[o]pponents of the constitution" to make use of constitutional freedoms "to endanger, harm or destroy the further existence of the state."[129] In the United States, Abraham Lincoln had used similar language and logic to justify his suspension of the writ of habeas corpus during the South's armed attack on the Union and its attempt to destroy the constitutional order of the United States.[130]

Beyond the idea of the "combative democracy," the Constitutional Court observed that the Basic Law, read in its full context and taken as a textual whole, viewed the individual not as an isolated, sovereign entity, but a person anchored in a community.[131] Quoting an earlier case, the Constitutional Court noted that the Basic Law resolved "the tension individual-community in the sense of the communal connection and the communal dependence of the person, without infringing upon the intrinsic value of" human worth.[132] The notion of the "combative democracy" and the communal connection of the individual provided key points in the

carried out on behalf of the European Parliament of the European Union, see Development of Surveillance Technology and Risk of Abuse of Economic Information, Working Document for the STOA Panel, Luxembourg, Oct. 1999.

124. BVerfGE, 30, at 4–5.

125. *Id.*

126. BVerfGE, 85 (1992), 386 ("connection capture" case); BVerfGE, 100 (1999), 313 ("BND" case).

127. BVerfGE, 30, at 19.

128. *Id.* at 19–20.

129. *Id.* at 20.

130. Abraham Lincoln, Message to Congress in Special Session (July 4, 1861), *in* THE PORTABLE ABRAHAM LINCOLN 209, 215–16 (Andrew Delbanco ed., 1992).

131. BVerfGE, 30, at 19.

132. *Id.* at 20.

Constitutional Court's upholding of all of the 1968 amendment to Article 10 and most, but not all, of the "Statute for Article 10."

In general, the Constitutional Court found the part of the constitutional amendment and statutory provisions that exclude those under surveillance from notification to be constitutional. This restriction was seen as meeting all necessary constitutional safeguards, including those of Article 79(3) regarding the "Eternity Clause" of the constitution. The Court stated: "In the present context, the exclusion of the notification is not an expression of a disdain for the human person and her worth, but a burden that falls on the citizen and is demanded of her on account of the protection of the stability of her State and the free democratic order."[133]

The Court also found permissible the recourse in the amendment and the statute to a non-judicial governmental body, rather than the ordinary judiciary, for oversight of certain foreign intelligence wiretaps.[134] The German legislature had decided that the wiretaps of intelligence agencies were not to be reviewed by the normal judiciary. While judicial review was not necessary, oversight of this surveillance was needed. In the absence of oversight, the Court stated it would be unconstitutional to subject an affected party to "the arbitrariness of the administrators."[135] The Court observed, however, that this impact would not occur when there was a substitute body consisting of independent members and providing as effective material and procedural control of the surveillance as the judiciary provided for wiretaps sought under the authority of criminal law.[136] The organ set up for such review of requests for wiretaps by an intelligence agency is the so-called "G-10 Group" (*G-10 Gremium*). In the United States, the Foreign Intelligence Surveillance Act ("FISA") has also established a special body to review requests for intelligence agency surveillance.[137] In contrast to Germany's non-judicial body, the United States makes use of a special FISA trial court, as well as a FISA appeal court, consisting of Article III judges.[138] These judges are all appointed by the Chief Justice of the United States Supreme Court; in Germany, the G-10 Group has its members appointed by Parliament.[139]

While the "Monitoring" Opinion found the constitutional amendment to Article 10 permissible, it declared one aspect of the accompanying

133. *Id.* at 20–21.

134. *Id.* at 20–24.

135. *Id.* at 27.

136. *Id.* at 23.

137. The FISA courts have recently made news with their first reported opinions. *In re* All Matters Submitted to Foreign Intelligence Surveillance Court, 218 F. Supp. 2d 611 (Foreign Intel. Surv. Ct. 2002); *In re* Sealed Case, 310 F.3d 717 (Foreign Intel. Surv. Ct. 2002).

138. 50 U.S.C. § 1803 (2003).

139. 50 U.S.C. § 1803; Gesetz zu § 10 GG, v. 26.6.2001 (BGBl I S.1254), as amended on Sept. 1, 2002 (BGBl. I S.361).

statute to violate the "principle of proportionality."[140] The Statute for Article 10's section 5(5) prohibited informing affected parties of surveillance under all circumstances.[141] The Constitutional Court found that such secrecy regarding surveillance was proper only so long as the interests of the State justified secrecy. The Constitutional Court declared this part of the statute void due to its "exclusion on informing the affected party about the restrictive measures also when it can occur without endangering the goal of the restriction."[142]

The "Monitoring" Opinion shows the Constitutional Court squarely involved in judicial review of measures that affect telecommunications privacy. The Constitutional Court saw itself as necessarily involved in reviewing the constitutionality of any laws that placed limits on Article 10. Indeed, the Constitutional Court has continued its oversight of telecommunications privacy legislation since this decision in 1970.

An important aspect of the different scope of telecommunications privacy in Germany and the United States concerns the "consent" exception for surveillance. As already noted, the United States allows a single party to consent to telecommunications and other kinds of surveillance. Such searches can take place without a judicial order. In Germany, in contrast, the constitutional protection that extends to telecommunications continues until *all* the parties to the communication consent. The German Constitutional Court made this point explicitly in the "Connection Capture" case. The German court stated: "If the goal of telecommunications secrecy rests in protecting the records and content of communications from governmental seizure, every governmental intervention (*Einschaltung*) that does not follow from the agreement of both communications partners is a violation of constitutional rights."[143]

B. "Connection Capture" Opinion

The "Connection Capture" decision concerned the German equivalent of the pen register. As we have seen, the United States Supreme Court decided in *Smith v. Maryland* in 1979, that a pen register, which captured the telephone numbers that one dialed, did not implicate the Fourth

140. BVerfGE, 30, at 21.

141. *Id.* at 21–22.

142. *Id.* at 32. The "Monitoring" opinion was a 5-3 opinion, with three dissenting judges arguing, among other points, that the constitutional amendment of 1968 was itself unconstitutional under Article 79(3)'s "Eternity Clause." *Id.* at 38–44. The dissenting judges also objected to the lack of explicit provisions for independence of the G-10 Group in the Article 10 statute as written as well as its allowing for secret procedures that excluded the affected party. *Id.* at 44–47. Finally, the dissenting judges objected to the use of the concept of "combative democracy" by the majority; in their view, the danger was that if the legislator ignored the value of individual rights, the "combative democracy" would end by being turned against itself. *Id.* at 45.

143. BVerfGE, 85 (1992), 386 (399).

Amendment.[144] In the "Connection Capture" opinion, the Constitutional Court came to a different conclusion regarding similar practices under Article 10.[145] Similar to the pen register in the *Smith* case, the "Connection Capture" decision concerned a tracing of phone calls to stop threatening calls that were being made anonymously.[146]

The Constitutional Court found that just as the German constitution protected "communications *content*," it also protected "communications *proceedings*" (*Kommunikationsvorgang*).[147] The Court explained, "[t]he protection [of the constitution] extends . . . to communication *proceedings*. Protected are the specific circumstances of the telecommunications relationship."[148] It found that telecommunications privacy even extended to the fact that a call had been attempted, but never completed.[149] The Court was breaking no new ground for German law.[150] One scholar has even traced such respect for communications privacy back to a Prussian Statute that required the Post Office, among other mandatory dimensions of postal secrecy, to maintain silence about the name of the persons to whom letters were sent.[151] Thus, a clear distinction exists between the broad scope of telecommunications privacy in German constitutional law and the narrow scope in United States constitutional law, which protects only telecommunications content.

In the "Connection Capture" case, the Constitutional Court also found that an adequate statutory basis did *not* exist for collection of telephone numbers with the device under scrutiny in the case.[152] To the extent that any legal justification existed for use of the device, it consisted of general statutory laws concerning the use of personal data by the Post Office and Deutsche Telekom, the traditional provider of telephony in Germany, as well as a regulation that granted Deutsche Telekom the power to investigate misuse of its services.[153] The Constitutional Court demanded the enactment of a "legal authorization for intervention" (*gesetzliche Eingriffermächtigung*) as soon as possible, but also permitted the practice to continue until this legal authority was in place.[154] Its grounds for doing so

144. 442 U.S. 735, 742–45 (1979). The *Smith* decision is discussed in Part II, *supra*.

145. BVerfGE, 85, at 386. The Constitutional Court described the practice at stake in this fashion: "connection capture permits the participant, by dialing a number issued to him, to maintain a connection during a telephone call and to allow the ascertaining of the number from which he was being called." *Id*. at 392.

146. *Id.* at 390.

147. *Id.* at 396 (emphasis in original).

148. *Id*.

149. *Id.*

150. For an earlier decision along similar lines, see BVerfGE, 67 (1984), 157 (171–72).

151. Joachim Riess, *Vom Fernmeldegeheimnis zum Telekommunikationsgeheimnis*, *in* DATENSCHUTZ IM TELEKOMMUNIKATIONS 127, 138 (Alfred Büllesbach ed., 1997).

152. BVerfGE, 85, at 398–99.

153. BVerfGE, 100 (1999), 313 (387–90).

154. *Id*. at 400–02.

shows how the Court's telecommunications jurisprudence must consider other constitutional values in addition to Article 10.

The Constitutional Court noted that threatening calls, if left unchecked, posed a threat to certain aspects of the Basic Law. The first threat was to the general right of personality, which the Court in previous decisions identified in the Basic Law's Article 2(1) and Article 1(1).[155] The second was a right to corporal integrity, expressed in the Basic Law's Article 2(2).[156] Pointing to a significant "gap in protection" (*Schutzlücke*) of the right to corporal integrity that would open if this practice was forbidden, the German Court stated that "Connection Capture" could continue for a limited time even without an adequate statutory basis.[157]

C. "BND" Opinion

In this opinion, the Constitutional Court reviewed the constitutionality of legislation that allowed the Federal Intelligence Service (*Bundesnachrictendienst* or "BND") to engage in surveillance of international telecommunications and to share the resulting information with other agencies.[158] The legislation in question dated primarily from 1994; it had widened the scope of the BND's area of surveillance over international telecommunications.[159] In its opinion, the Constitutional Court found numerous aspects of the statute unconstitutional.[160]

At this point, a few words should be said about German law regarding telecommunications surveillance carried out by intelligence agencies. The BND is one of several different German intelligence agencies; its job is to collect and analyze information about foreign countries that are of importance for the foreign policy and security of the F.R.G.[161]

The BND and other German intelligence agencies are permitted to engage in surveillance of letters, conversations, or telecommunications by two paths. First, the surveillance can take place as an "individual investigation," which involves the collection of personal data to investigate criminal behavior that threatens the survival of the F.R.G. or its democratic order.[162] Second, the surveillance can take place as "strategic surveillance."[163] As an example of strategic surveillance, the BND uses

155. *Id*. at 400.

156. *Id*. at 400–401.

157. *Id*. For a discussion of the current regulation of this practice, see BECK'SCHE TKG-KOMMENTAR 1451–52 (Wolfgang Büchner et al. eds., 2000) [hereinafter TKG TREATISE].

158. BVerfGE, 100, at 313.

159. *Id.* at 317–23.

160. *Id.* at 358–403.

161. Bundesnachrichtendienst, Der BND als Informationsdienstleiter, *at* http://www.bundesnachrichtendienst.de/auftrag/index.htm.

162. BVerfGE, 100, at 316.

163. *Id.*

certain search terms in examining telegram traffic to and from Germany.[164] In the "BND" case itself, the strategic surveillance involved observation of telegram, fax, and, to a lesser extent, telephone traffic transmitted via satellite.[165] The Constitutional Court also noted that the government had admitted in oral argument before it that plans were also being made for surveillance of e-mails, but the Court did not provide further details about this project.

Prior to statutory amendments in 1994, strategic surveillance was permitted only for the purpose of early recognition and prevention of an armed attack on the F.R.G.[166] More specifically, the primary focus of German strategic surveillance during the Cold War was the armed forces of Warsaw Pact nations. However, by 1994 Germany had been re-unified, and the Cold War was winding down. In that year, the German legislature reacted to new threats to the F.R.G. by enacting the "Crime Fighting Statute" (*Verbrechensbekämpfungsgesetz*), which widened the grounds for "strategic surveillance."[167] This statute permits surveillance of international telecommunications to gain information about: (1) international terrorism; (2) drug smuggling into Germany; (3) illegal arms trafficking; and (4) international money laundering and counterfeiting operations.[168] The statute also allows information garnered through this surveillance to be shared with security and law enforcement agencies to prevent, solve, and prosecute criminal activity.[169]

In its "BND" opinion of 1999, the Constitutional Court first found that the protections of Article 10 were not limited merely to communications that took place entirely within the national borders of Germany. As long as enough of a nexus existed between the surveillance and German territory, the protections of Article 10 of the constitution were applicable.[170] Such a nexus was found in the present case, where the governmental surveillance activity occurred from within Germany and at least part of the communications ended or originated from within Germany.[171]

The Constitutional Court also found that the dangers of such surveillance were considerable.[172] Most importantly, it pointed to the risk that such surveillance would lead to "a nervousness in communication, to disturbances in communication, and to behavioral accommodation, in

164. *Id.* at 379–80.
165. *Id.* at 380.
166. *Id.* at 318–20.
167. *Id.* at 317–18.
168. *Id.* at 318.
169. *Id.*
170. *Id.* at 363–64.
171. *Id.*
172. *Id*. at 381.

particular to avoidance of certain content of conversations or terms."[173] Put concisely, the threat was to social communication.

There are strong parallels here, as the Constitutional Court itself noted with its earlier decision in the "Census Case" of 1983. In that famous opinion, the Court articulated "the right of informational self-determination," which it identified in Articles 1 and 2 of the constitution.[174] The German right of informational self-determination protects an individual from borderless collection, storage, application, and transmission of personal data.[175] It prevents any processing of personal data that leads to an inspection of or an influence upon a person that is capable of destroying an individual capacity for self-governance.[176] Moreover, this right places an obligation on the State to organize data processing so that personal autonomy will be respected.[177] Finally, the right of informational self-determination is not merely an individual right, but one that seeks to protect a certain communicative capacity within society.[178] As the *Census* Court noted, "[t]he individual does not have a right in the sense of an absolute, unlimitable mastery over 'his' data; he is rather a personality that develops within a social community and is dependent upon communication."[179] Information relating to a person depicts "an image of social reality that the concerned party cannot exclusively coordinate."[180]

Interestingly enough, the right of informational self-determination was not directly applicable in the "BND" case. As an established matter of German constitutional jurisprudence, the Constitutional Court was obliged to center its opinion on the specific provisions of Article 10 rather than the general right of personality and the related right of informational self-determination.[181] At the same time, however, the Court in the "BND" case did not hesitate to draw parallels between the right of informational self-determination and the protections that it identified in Article 10. As I have noted, the first such parallel concerned the connection between information privacy and free societal communication; this link is discussed in both the

173. *Id.*

174. BVerfGE, 65 (1983), 1. For a proposal to draw on the right of information self-determination in modernizing the German concept of information privacy, see ALEXANDER ROSSNAGEL ET AL., MODERNISIERUNG DES DATENSCHUTZRECHTS 45–48 (2001).

175. *Id.* at 42.

176. *Id.*

177. *Id.* at 46–52.

178. Spiros Simitis, *Das Volkszählungsurteil oder der lange Web zur Informationsakese*, 83 KRITISCHE VIERTELJAHRESSCHRIFT 359, 368 (2000).

179. BVerfGE, 65, at 44.

180. *Id. See* Paul M. Schwartz, *The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination*, 37 AM. J. COMP. L. 675, 690 (1989) ("the right of informational self-determination compels the State to organize data processing so that personal autonomy will be respected").

181. BVerfGE, 67 (1984), 157 (171); BVerfGE, 6 (1954), 32 (37).

"Census" and "BND" opinions.[182] Second, and as a related point, the Constitutional Court in both cases observed how the negative impact of surveillance would be felt not only by the individual, but by society as a whole.[183] Indeed, in the "BND" decision, the Court observed that in its case law regarding the right of individual self-determination, it had identified a similar "connection to the common good" (*Gemeinwohlbezug*).[184]

After noting that the data collected in the "BND" case raised threats to societal communication, the Constitutional Court nevertheless found the surveillance to have a strong justification. The activity to be placed under observation "affected the foreign and security politics of the Federal Republic . . . to a significant extent."[185] The law permitted the collection of information necessary to detect dangers to Germany; as a result, the Constitutional Court generally found that the statute was generally "not improper."[186]

The Constitutional Court did go on, however, to find several aspects of the statute to be unconstitutional.[187] Among the elements of the law found unconstitutional were certain provisions concerning transfer of the personal data by the BND to other agencies. These transfers were only permissible when the controlling legislation fulfilled the principle of proportionality.[188] The Constitutional Court decided that, as a general matter, it was constitutional for the BND to share information gained from its surveillance of telecommunications traffic with other agencies to the extent that the data in question revealed criminal behavior. However, the statute did not limit these data transfers in a permissible fashion. The Court called for restrictions on data sharing to instances in which serious crimes had been committed, as opposed to more minor delicts, and it also demanded standards for intelligence agencies that restricted transfer of information in a manner similar to domestic law enforcement agencies when engaged in the "individual investigation path."[189]

182. BVerfGE, 65, at 1, 43; BVerfGE, 100, at 381.

183. BVerfGE, 65, at 1, 43.

184. BVerfGE, 100, at 381.

185. *Id.* at 382.

186. *Id.* at 384–85

187. For example, the statute's section 3(1)(2)(5) permitted international surveillance to investigate counterfeiting of currency. The Constitutional Court found that the statutes allowing surveillance to prevent this crime did not follow the principle of "proportionality." *Id.* at 385. It noted, however, that such surveillance would be constitutionally permissible if the strategic surveillance was limited to cases that threatened "the stability of the value of the currency of Germany and thereby the economic power of the country." *Id.*

188. *See* text accompanying note 116.

189. BVerfGE, 100, at 385–86.

V. U.S. and German Statutory Law: Six Categories of Comparison

Thus far, this Article has noted significant differences between the constitutional regimes regarding telecommunications privacy in the United States and Germany. The Constitutional Court has actively reviewed statutes that affect telecommunications secrecy. In contrast, the United States Supreme Court has developed doctrines that have taken it out of the business of constitutional review of laws regarding the processing, collection, and sharing of telecommunication attributes. This Part considers the comparative legislative regimes for telecommunications privacy in Germany and the United States.

My analysis concentrates on six areas of the two legal regimes: (1) the extent of legal protection for *customer information* (such as one's name, address, telephone number, or non-dynamic IP address); (2) the extent of legal protection for *connection data* (such as the telephone numbers called; time and length of connection; one's dynamic IP address); (3) the extent of legal protection for *stored* data; (4) the extent of legal requirements placed on telecommunications providers for *data retention or data erasure*; (5) the extent of legal protection for the *content* of telecommunications; and, finally, the (6) nature of available *remedies* (e.g., the exclusionary rule, civil damages, or both).

A. Legal Protection for Customer Information

The legal tests for governmental access to customer information are dissimilar in Germany and the United States, but so are the underlying categories. In Germany "customer information" is easier to obtain than in the United States, but the German category is far narrower. Thus, at the start of this discussion, one must explain the categorical differences in the two countries.

(1) Defining the Category

In Germany, customer information is defined in the applicable law as extending only to information such as name, address, telephone number, and non-dynamic IP address.[190] These data are literally termed "inventory information," (*Bestandsdaten*), which is a narrower concept than the closest equivalent under U.S. law, especially in light of post 9-11 amendments to the law made through the USA PATRIOT Act.

Before enactment of the USA PATRIOT Act, "customer information" in the United States included data such as name, address, telephone number, billing records, and types of services.[191] The USA PATRIOT Act

190. § 90 Telekommunikationsgesetz (TKG). For a discussion of the limited data to be included in this category, see TKG TREATISE, *supra* note 157, at 1503–04.

191. 18 U.S.C. § 2703(c)(2)(A) & (B) (Supp. 2002).

broadened this category to include records of session times and durations, any temporarily assigned network address (i.e., dynamic IP address), and any credit card or bank account number used for payment.[192] The differences in the German and U.S. concept of customer information should be kept in mind as we consider the legal tests in the two countries to obtain access to the data.

(2) Tests for Obtaining Access to the Information

In Germany, it is quite easy to obtain "inventory information." Law enforcement officials can request it when required for discharge of "their legal functions,"[193] and judicial review of this request does not occur. Moreover, under one path for obtaining this information, the telecommunications provider or ISP does not even process the request.

German law requires telecommunication providers to maintain automated data banks that contain "inventory information."[194] Law enforcement requests for it are made to a special independent "regulatory authority," which is located within the Federal Ministry of Economics.[195] The regulatory authority responds to law enforcement requests for customer information by retrieving inventory information. The authority is required by law to maintain a log of the information demands.[196] In 2002, an administrative law court in Northrhine-Westfalia extended this obligation regarding collection of inventory information to mobile telephony providers who sold pre-paid products; the court decided that the statute required these providers to collect the standard set of "inventory information."[197]

German law also permits direct requests for customer information to be made to telecommunications providers. The providers are to turn over customer information in individual cases if necessary for "the prosecution of criminal and administrative offenses, for averting danger to public safety or order, or for the discharge of legal functions."[198] The direct requests, like requests to the automated data banks, can be made by a wide array of German law enforcement and intelligence agencies.[199] Also like requests to the automated data bank, the direct requests are free of judicial review.

In the United States, the statutory requirements for obtaining access to customer information are higher than in Germany. The legal test for customer information requires proof of "specific and articulable facts

192. *Id.* § 2703(c)(2)(C)–(F).

193. § 90 TKG.

194. *Id.*

195. § 66 TKG.

196. § 90 TKG.

197. Oberverwaltungsgericht Nordrhein-Westfalen, Beschluß, v. 17.5.2002, *in* 26 DATENSCHUTZ UND DATENSICHERHEIT 563 (2002).

198. § 89 Nr. 6 TKG.

199. *Id.*

showing that there are reasonable grounds to believe that the . . . records or other information sought are relevant and material to an ongoing criminal investigation."[200] Note, however, that this test is a lower one than the full "probable cause" requirement in place in the United States before access to "content" can be granted.[201] Also in contrast to Germany, a court order is required for disclosure of customer information in the United States.[202]

B. Legal Protection for Connection Data

Germany and the United States have developed similar definitions for connection data. Hence, a comparison in this area is easier than for customer information and leads to the conclusion that law enforcement authorities in the United States face lower hurdles in obtaining connection information than their German counterparts.

(1) Defining the Category

In Germany, "connection data" (*Verbindungsdaten*) includes telephone numbers called, time and length of the connection, the IP address of services used, one's dynamic IP address, and certain limited information garnered from URL's visited, such as data pertaining to services used (e.g., "http"; "ftp"; and "pop server") and the name of the host server (IP address and domain name).[203]

In the United States, the concept of "connection data" emerged as a result of the *Katz* and *Smith* decisions, discussed above. In response to these decisions, Congress enacted the Pen Register Act to regulate access to telephone numbers collected by pen registers and trap and trace devices.[204] More recently, the category of "connection data" has been expanded by enactment of the USA PATRIOT Act, which extends the Pen Register Act to "dialing, routing, addressing, [and] signaling information."[205]

(2) Tests for Obtaining Access to the Information

In Germany, access to connection data is regulated by two parts of the Code of Criminal Procedure (*Strafprozeßordnung*), namely sections 100g and 100h. Connection data can be obtained both *retrospectively* and, due

200. 18 U.S.C. § 2703(d) (Supp. 2002).

201. For the "probable cause" test for content, see 18 U.S.C. § 2518(3) (2003).

202. *Id.* § 2703(a).

203. § 100g Nr. 3 StPO; § 6 Nr. 1 Telekommunikationsdatenschutzverordnung ("TDSV"); § 6 Nr. 3 Teledienstdatenschutzgesetz. For an analysis, see Pfeiffer, supra note 41, at 225; THOMAS KÖNIGSHOFEN, TDSV: KOMMENTAR 63–68 (2002); Alexander Dix & Peter Schaar, *TDDSG-Kommentar*, *in* RECHT DER MULTIMEDIA-GESETZE (Alexander Rossnager ed., forthcoming 2003).

204. 18 U.S.C. §§ 3121 (2003).

205. 18 U.S.C. § 3127(3) (Supp. 2002).

to changes to this statute made after 9-11, *prospectively*.[206] An order (*Anordnung*) for a wiretap must come from a judge unless there is imminent danger (*Gefahr in Verzug*).[207] An order for connection data requires a suspicion based on "determinate facts" that the person whose data will be collected is a perpetrator or participant in a serious offense (*eine Straftrat von erheblicher Bedeutung*), especially an offense listed in section 110a of the Code of Criminal Procedure, or an offense committed with use of a telecommunications device, such as a telephone or computer.[208] The idea of restricting surveillance to investigations of certain serious "listed crimes" is also used in the United States, where the equivalent term of art is "predicate offenses." The German test allows law enforcement officials greater flexibility in obtaining connection data than content—as we shall see later, a surveillance order for content can only be made if a listed criminal offense is involved. In contrast, connection data can be obtained for any serious offense or offense made with use of a telephone or computer.[209] The idea, as this statute also explicitly states, is to allow the investigation of crimes committed over the telephone or on the Internet.[210] As an example of such a crime, one German treatise points to the making of insulting telephone calls.[211]

In the United States, connection data is also easier to obtain than in Germany. Under the Pen Register Act, this information can be obtained after law enforcement officials file an order with a court that states that the "information likely to be obtained . . . is relevant to an ongoing criminal investigation."[212] There is no independent judicial investigation of the merits of such a request. The court is to approve requests filed with it.[213] Here, the USA PATRIOT Act enacted one minor—but positive—change that improves the reporting requirements regarding such orders under the Pen Register Act. The Pen Register Act requires the Attorney General to file an annual report with Congress on the number of pen register orders. The USA PATRIOT Act mandates further specification regarding the precise contents of these reports.[214] Moreover, the extension of the Pen Register Act to the Internet has also been accompanied with detailed requirements for a paper trail following official use of such a device.[215]

206. § 100g–h StPO . For a concise analysis, see Johann Bizer, *Verpflichtung zur Herausgabe von TK-Verbindungen an den Staatsanwalt*, 26 DATENSCHUTZ UND DATENSICHERUNG 237 (2002). The relevant statute is valid only until December 31, 2004. *Id.*

207. § 100h StPO. For a discussion of the emergency exception, see Pfeiffer, *supra* note 41, at 225–26.

208. § 100g StPO.

209. *Id.*

210. *Id.*

211. Pfeiffer, *supra* note 41, at 224.

212. 18 U.S.C. § 3123(a)(1) (Supp. 2002).

213. Freiwald, *supra* note 6, at 972; 18 U.S.C. § 3123(a)(1)–(2).

214. 18 U.S.C. § 3126 (2000).

215. *Id.* § 3123(a)(3)(A).

C. Legal Protection for Stored Data

Thus far, we have examined one category, customer data, that is defined differently enough in Germany and the United States to make comparisons between legal regimes difficult. This Article's next area for consideration, stored data, also reveals significant differences. In fact, it is a category that exists only in United States telecommunications law.

(1) Defining the Category

In Germany, stored data is not a legal category. This result is not surprising in light of the Constitutional Court's case law, which has never found stored data to be subject to lesser or different protection than information within the control of the individual to whom it refers. Thus, the relevant German categories concern "customer information," "connection data," and "content."

In the United States, the concept of stored data dates at least back to the Supreme Court's *Miller* and *Smith* opinions.[216] As a consequence of these opinions, information stored in the control of the third parties is free from the protection of the Fourth Amendment. At least in partial reaction to these opinions and also as a result of technological developments in electronic communications, Congress carried out a major revision to the Wiretap Act of 1968 (which had represented its first step at regulating telecommunications surveillance) and enacted the Electronic Communications Privacy Act of 1986 ("ECPA").[217] The technological advance in question was computer-assisted communication, which in 1986 generally meant only computer bulletin boards, but by 2002 would mean the Internet.

In the ECPA, Congress decided to allow the stricter standards of the Wiretap Act to apply only to electronic communications during their *transmission*.[218] As a result, stored data are generally subject to a statutorily lower level of protection. As discussed below, however, Congress also made an important exception to this rule for content in storage fewer than 180 days.[219] Finally, non-content information in storage at a service provider is subject to tests similar to those under the Wiretap Act for non-content intercepted while in transmission.[220]

216. *See* Part II *supra*.

217. ECPA is codified at 18 U.S.C. §§ 2701–11 (2003). For a discussion of the background of the Act, *see* Freiwald, *supra* note 6, at 969–95; Kerr, *supra* note 101, at 814–15.

218. *Compare* 18 U.S.C. § 2511 (2003) (regulations regarding interception during transmission) *to* 18 U.S.C. § 2701 (regulations regarding unlawful access to stored communications).

219. 18 U.S.C. § 2703(a) (Supp. 2002).

220. *Id.* § 2703(c).

(2) Tests for Obtaining Access to the Information

As noted, Germany makes no use of the concept of "stored data" in its telecommunications privacy law. In the United States, content found in storage for fewer than 180 days is subject to the same "probable cause" requirement as found in the Wiretap Act.[221] After 180 days, however, content can be obtained "with prior notice from the governmental entity to the subscriber or customer" if the government obtains an administrative or judicial subpoena.[222] Non-content information in storage can also be obtained pursuant to a subpoena; the law requires a showing of "specific and articulable facts showing that there are reasonable grounds to believe . . . contents . . . are relevant and material to an ongoing criminal investigation."[223]

D. Legal Requirements for Data Retention and/or Erasure

The fourth category concerns whether German or the United States law places requirements on telecommunications providers either to maintain telecommunications information for a certain period or to erase it after a certain period. As an example, a legal system might only require data retention. Thus, the law might mandate telecommunications traffic data to be stored for a year. A country might also combine both requirements: it might require ISPs to store e-mail content for all customers for a certain period and also require that all such information be destroyed after that time.

We will now reverse this Part's usual order of analysis and begin with the United States. In the United States, there is neither a data retention nor an erasure requirement for telecommunications information.[224] Other areas of U.S. privacy law do contain data erasure requirements. These include the Video Privacy Protection Act,[225] and the Cable Communication Policy Act.[226] Another United States statute, the Fair Credit Report Act takes a different tack; it excludes from inclusion in a "consumer report," various kinds of information according to different expiration dates.[227] Thus,

221. *Id.* § 2703(a).

222. *Id.* § 2703(b)(1)(B).

223. *Id.* § 2703(d).

224. *See* ARTICLE 29 WORKING PARTY, OPINION 5/2002 ON THE STATEMENT OF THE EUROPEAN DATA PROTECTION COMMISSIONERS AT THE INTERNATIONAL CONFERENCE IN CARDIFF (9-11 SEPTEMBER 2002) ON MANDATORY SYSTEMATIC RETENTION OF TELECOMMUNICATIONS TRAFFIC DATA (Oct. 11, 2002), *at* http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2002/wp64_en.pdf (noting the lack of data retention in the United States at the same time as E.U.-wide proposals are circulating for data retention).

225. 18 U.S.C. § 2710(e) (2003) (destruction of information after one year).

226. 47 U.S.C. § 551 (2003) (destruction of information "if the information is no longer necessary for which it was collected").

227. 15 U.S.C. § 1681b (2003)

excluded from consumer reports are: bankruptcy reports that are ten years old or more; paid tax liens that are seven years old or more; and "any other adverse information," which "antedates the report by more than seven years."[228] In contrast, telecommunications providers are generally under no legal obligation to store any set of information or to erase it after a set time. The lack of any such requirement in the United States has been noticed by German telecommunication providers, who argue that introduction of a data retention requirement in Germany would put them at a competitive disadvantage.[229]

In summary, the current regime in the United States requires neither data erasure nor storage. Germany has no data storage requirement but does have a strong data erasure requirement. The chief German requirements for data erasure are found in different statutes depending on whether the party concerned is deemed a "teleservice provider," which is a party offering services over the Internet (such as Amazon Germany), or a "telecommunication service provider," which is a party providing telecommunication services (such as Deutsche Telekom).[230] The two statutes reach the same result concerning data retention: teleservice providers and telecommunication service providers alike may retain connection data necessary for billing for no longer than six months.[231] Of course, teleservice providers and telecommunication service providers may also choose to store information for shorter periods because, as noted, Germany has no data retention requirement. Finally, other information, such as certain connection data that is not needed for billing purposes, is to be erased at once by telecommunications providers.[232]

However, the topic of required data storage is currently the subject of significant political debate at present in Germany, the European Union, and beyond. Even prior to the terrorist attacks on 9-11, certain European nations had considered or adopted a data retention requirement. As an example of such a requirement adopted prior to 9-11, Belgium mandated a one year traffic retention requirement in a computer crime law enacted on November 28, 2000.[233] Post 9-11, Denmark has enacted a requirement that ISPs retain traffic data.[234] As a final example, and one for a nation outside

228. 15 U.S.C. § 1681c(a) (2003).

229. *See infra* text accompanying note 246.

230. The *Teledienstedatenschutzgesetz* ("TDDSG") regulates teleservice providers. The *Telekommunikationsdatenschutzverordnung* ("TDSV") regulates telecommunications service providers.

231. § 6 (2) 1-2 TDDSG; § 7 (3) TDSV.

232. § 6 (3) TDSV. For a discussion of this obligation, see TKG TREATISE, *supra* note 157, at 1481.

233. Projet de Loi relatif à la criminalité informatique, Art. 14, Doc 50, 0213/007 (Mar. 30, 2000).

234. GENERAL SECRETARIAT, COUNCIL OF THE EUROPEAN UNION, MULTIDISCIPLINARY GROUP ON ORGANISED CRIME, ANSWERS TO QUESTIONNAIRE ON DATA RETENTION (2002)

the European Union, Switzerland has enacted a requirement for ISPs not only to record traffic data, but also e-mail content and to store this information for at least six months.[235]

The United States government has emerged as a behind-the-scenes voice in favor of E.U. countries adopting data retention requirements.[236] In contrast, European data protection commissioners are strongly opposing the creation of such a data retention requirement in the European Union.[237] The E.U. Directive on privacy and electronic communications, which takes effect on October 31, 2003, contains two provisions concerning data storage. Recital 26 requires that data relating to subscribers to electronic communications networks be stored "only to the extent that is necessary for the provision of the service for the purpose of billing and for interconnection payments, and for a limited time."[238] Yet, the Directive's Article 15 allows E.U. Member States to "adopt legislative measures providing for the retention of data for a limited period" for protection of national security and prosecution of crimes.[239] The Working Group of E.U. data protection commissioners has issued an opinion stating that the routine storage period for billing purposes should generally be for "a maximum of 3-6 months."[240]

Germany is also now considering a data retention requirement. German law enforcement agencies are demanding legally mandated data retention with the claim that their work has been hindered by the lack of such a requirement.[241] Opposed to such a requirement are the nation's data protection authorities at the federal and state levels. In a Resolution issued at the Sixty-Fourth Annual Conference of German Data Protection Authorities, the commissioners spoke of "the meaning of telecommunications secrecy as an inalienable prerequisite for a free,

[hereinafter E.U., QUESTIONNAIRE ON DATA RETETENTION], *at* http://www.effi.org/eu-2002-11-20.htm.

235. Eugene Oscappella, *Swiss Surveillance Law Will Hit ISPs*, PRIVACY LAWS & BUS. INT'L NEWSL. 24 (Sept. 2002).

236. Norton-Taylor & Millar, *supra* note 9, at 1.

237. ARTICLE 29 DATA PROT. WORKING PARTY, *supra* note 224. At the same time, evidence exists of plans for mandatory data retention underway at the E.U.-level. A framework document of the Eurpean Union's Justice and Home Affairs Minister has been leaked to Statewatch, a European human rights organization. The framework document plans "compulsory" data retention for twelve to twenty-four months. *EU: Data Retention To Be "Compulsory" for 12–24 months*, STATEWATCH NEWS ONLINE, Aug. 23, 2002, *at* http://www.statewatch.org/news/2002/aug/05datafd1.htm.

238. Council Directive 2002/58/EC 2002 O.J. (L 201) 37–47 (concerning the processing of personal data and the protection of privacy in the electronic communications sector).

239. *Id.* at Art. 15.

240. ARTICLE 29 DATA PROT. WORKING PARTY, OPINION 1/2003 ON THE STORAGE OF TRAFFIC DATA FOR BILLING PURPOSES 7 (Jan. 29, 2003), available at http://europa.eu.int/comm/internal_market/privacy/docs/wpdocs/2003/wp69_en.pdf. Data may be stored for a longer period if, for example, there is a dispute regarding a bill. *Id*.

241. E.U., QUESTIONNAIRE ON DATA RETENTION, *supra* note 234, at 27.

democratic communicative society" and pointed to possible constitutional barriers to any data retention requirement.[242] In its Census Decision, which established the right of informational self-determination, the Constitutional Court had explicitly noted the unconstitutionality of a "collection of data in a stockpile (*Daten auf Vorrat*) for indeterminate or not yet determined goals."[243] In that opinion and others, the Constitutional Court has looked for a limitation on data being collected to the "legally determined goal."[244] Should a law mandating data retention be enacted, constitutional litigation is likely to follow.[245]

Finally, as noted above, German telecommunication providers have raised an objection to a data retention requirement on economic grounds. As summarized by the German delegation to a Council of Europe Multidisciplinary Group on Organized Crime, these telecommunication providers "are afraid of being at a competitive disadvantage vis-à-vis foreign service providers and having to pay high costs for storing data."[246] To the extent that European-wide data retention requirements for storage are now being considered, the competitive disadvantage will not be with other European telecommunication companies but with companies in the United States, who are free of any data storage obligation.

E. Legal Protection for Telecommunications Content

Both the United States and Germany provide similar definitions for telecommunications content. In addition, both countries require judicial involvement in the issuing of surveillance orders unless there is an emergency. All and all, the tests for obtaining content information in Germany and the United States are similar.

242. ENTSCHLIEßUNG DER 64. KONFERENZ DER DATENSCHUTZBEAUFTRAGTEN DES BUNDES UND DER LÄNDER VOM. 24.10.–25.10.2002 [hereinafter RESOLUTION OF DATA PROTECTION COMMISSIONS], *at* Datenschutz-Berlin, http://www.datenschutz-berlin.de/doc/de/konf/64/internet.htm (homepage of the Berlin Data Protection Commissioner). The Federal Data Protection Commissioner has also individually expressed his opposition to data retention. Pressmitteilung, Der Bundesbeauftrage für den Datenschutz, Bundesratsmehrheit plant unakzeptable "Vorratspeicherung" für Internet- und Telekommunikationsdaten (May 5, 2002), *available at* http://www.bfd.bund.de/Presse/pm20020531.html (last visited May 13, 2002).

243. BVerfGE, 65 (1983), 1 (44).

244. BVerfGE, May 15, 1984, NEUE JURISTISCHE WOCHENSCHRIFT 2271 (1984) (Flickauschuß); BVerfGE, June 27, 1991, NEUE JURISTISCHE WOCHENSCHRIFT 2129, 2132 (1991).

245. The Data Protection Commissioners have also called for the leaders of the German government to provide more information about any negotiations with other European governments and demanded that the German government oppose the introduction of a Europe-wide uniform data retention requirement. RESOLUTION OF DATA PROTECTION COMMISSIONERS, *supra* note 242, at 2.

246. E.U., QUESTIONNAIRE ON DATA RETENTION, *supra* note 234, at 30.

(1) Defining the Category

German telecommunications law does not explicitly define the term "content," but clearly uses the concept in a similar fashion to the United States. Perhaps the best evidence of the similarity of the concept is the fashion in which the "Capture Connection" decision analyzed the meaning of "communication content" and "communications proceedings."[247] This decision demonstrates that German law uses the term, "content" to mean the substance of a communication.[248] In a similar fashion, under United States telecommunications privacy law, "contents" means "any information concerning the substance, purport, or meaning" of "any wire, oral or electronic communication."[249]

(2) Tests for Obtaining Access to the Information

In Germany, obtaining wiretaps for content requires use of a somewhat similar test as for connection data. The connection data that is sought must be "necessary" for an investigation of a listed criminal offense, and a judge must also find that "determinate facts" indicate that the person whose data will be collected is a perpetrator or participant in such a listed offense.[250] The listed offenses are found in section 100a of the German Code of Criminal Procedural.[251]

Similar to the increase in "predicate offenses" in the United States, the "listed offenses" have expanded in Germany.[252] In the latest expansion, which occurred after 9-11, membership in a terrorist organization was added to the listed offenses for which one can get a surveillance order.[253] Unless imminent danger exists, an order for a wiretap must come from a judge.[254] Finally, and as noted above in Part I, Germany does not allow roving wiretap orders. As the Federal Code of Criminal Procedure section 100b makes clear, each surveillance order must include the name and

247. BVerfGE, 85 (1992), 386.

248. *Id.* at 396.

249. 18 U.S.C. § 2510(8) (2000).

250. § 100a StPO.

251. *Id.* at § 100a Nr. 1.

252. According to Johann Bizer, the German list of crimes serious enough to justify telecommunications surveillance has been expanded nineteen times since 1968. Johann Bizer, *Telekommunikation und Innere Sicherheit 2001: Neue Entwicklungen im Telekommunikationsrecht, in* JAHRBUCH TELEKOMMUNIKATION UND GESELLSCHAFT 2002 (Herbert Kubicek, ed, forthcoming 2003) (manuscript at 9) [hereinafter Bizer, *Telekommunikation und Innere Sicherheit 2001*] (as of 2001, section 100a St PO expanded seventeen times); Johann Bizer, TK-Überwachung in Deutschland: Arten-Umfang 6 (Oct. 21, 2002) (on file with *Hastings Law Journal*) (section 100a StPO expanded nineteen times).

253. Bizer, *Telekommunikation und Innere Sicherheit 2001*, *supra* note 252 (manuscript at 12).

254. § 100b Nr. 1 StPO.

address of the written party and the telephone connection to be made subject to the measure.[255]

In the United States, law enforcement agencies that engage in surveillance of telecommunications content must meet a full "probable cause" requirement to obtain a search warrant from a judge. The requirement of "probable cause" occurs at three levels. A judge must find probable cause regarding a belief: (1) that the person "is committing, has committed, or is about to commit" a predicate offense; (2) that "particular communications concerning that offense will be obtained through such interception;" and (3) that "the facilities from which, or the place where" the communications are to be intercepted are used in connection with the commission of the offense or are used by the person named in the wiretap order.[256]

Moreover, wiretap orders for content are only permitted if normal investigative procedures have already been used, are unlikely to succeed, or will be too dangerous.[257] In an important change to United States law, the USA PATRIOT Act expanded the list of predicate offenses for content wiretaps. It added crimes of terrorism; production or dissemination of chemical weapons; and felony violations of the law related to computer fraud and abuse to the list of predicate offenses.[258] An emergency exception also exists in the United States to the requirement that a judge issue the surveillance order.[259] Finally, roving wiretaps are permitted in the United States in cases where "specification of the facilities from which . . . the communication is to be intercepted" proves to be "not practical."[260]

In both Germany and the United States, applications for wiretap orders are almost never refused by the responsible judge or magistrate. In Germany, precise figures are not available regarding refused wiretap orders, but occasional comments appear in the legal literature in Germany regarding the ineffectual nature of judicial oversight.[261] In the United

255. § 100b Nr. 2 StPO.

256. 18 U.S.C. § 2518(3)(a)(b) & (d) (2000).

257. *Id.* § 2518(1)(c).

258. The amendments introduced by the USA PATRIOT Act are codified at 18 U.S.C. § 2516(1) (Supp. 2000).

259. 18 U.S.C. § 2518(7).

260. *Id*. § 2518(11).

261. For criticism of the judicial oversight, see Edda Wesslau, *Gefährdung des Datenschutzes durch den Einsatz neuer Medien im Strafprozeß*, ZEITSCHRIFT STRAFRECHT UND WIRTSCHAFT 681, 683 (2001). A valuable empirical study of judicial oversight of wiretaps has been carried out by a team at the University of Bielefeld. The "Backes Study" found only a single judicial refusal for the 307 requests for surveillance examined in this project. OTTO BACKES ET AL., WIRKSAMKEITSBEDINGUNGEN VON RICHTERVORBEHALTEN BEI TELEFONÜBERWACHUNGEN 4 (Dec. 2002), *at* http://www.uni-bielefeld.de/Universitaet/Aktuelles/pdf/backes_kurzfassung_telefonueberwachung.pdf (on file at *Hastings Law Journal*). Prosecutors told the researchers, moreover, that they could get any order so long as they sent their request to the judge along with a

States, a refusal of requests for surveillance orders is a rare event. According to the account of the Electronic Privacy Information Center, ("EPIC") out of the over 20,000 surveillance requests made between 1968 and 1996, judges refused only twenty-eight.[262]

F. The Nature of Available Remedies

The remedies in Germany and the United States for violations of surveillance statutes are notably similar. A consideration of legal reality in both countries finds further similarities in the significant gaps in the remedies and their relatively modest utilization.

(1) Defining the Category

Remedies are available in the United States and Germany should statutory rules not be followed by law enforcement authorities or telecommunication providers. The remedies in both countries include both damage awards and exclusion of the material collected by the authorities.

(2) Tests for Obtaining the Different Remedies

In Germany, both exclusion of material (*Verwertungsverbot*) and civil damages are available. Yet, exclusion is available only in narrow circumstances. Thus, one court has called for limiting suppression to instances where there was a "complete circumvention" (*völlige Umgehung*) of the relevant statute.[263] Another justification for suppression of material would be a surveillance "order issued under conscious infringement of the law."[264] As we shall see, the similarity is great with the limited current reach of the exclusionary rule in the United States.

German law also permits damages for violations of its telecommunications surveillance law. The applicable statute makes reference to the general remedies found in the Federal Data Protection Statute.[265] These remedies include criminal penalties, including up to a year in prison, and money damages for unauthorized storage, alteration or transfer of protected personal data.[266]

One final German institution regarding remedies should be mentioned. The Federal Data Protection Commissioner has authority to investigate violation of telecommunications privacy law in connection with

draft of a judicial order. *Id*. Finally, the study found that only a quarter of the judicial orders met the full statutory requirements. *Id.* at 3–4.

262. EPIC, TITLE III WIRETAP ORDERS DENIED 1968–1996, *at* http://www.epic.org/privacy/wiretap/stats/taps_denied.html.

263. BGH 31, 304 (1985) (concerning § 100a StGB) . For a case excluding the results of a secretly placed "bug" inside a living area, see BGHSt 42, 372 (377) (1997).

264. *Id.*; BGH 32, 68. For cases drawing further limits on the suppression remedy, see BGH 42, NEUE JURISTISCHE WOCHENSCHRIFT, 961 (1999); BGHSt 35, 32 (34) (1987).

265. TKG TREATISE, *supra* note 157, at 1464.

266. §§ 43–44 BDSG.

commercial telecommunication services.[267] This power gives the Commissioner, the head of an independent federal privacy agency, the ability to carry out preventative, "data protection audits."[268]

In the United States, the remedies scheme for law enforcement violations of telecommunications surveillance statutes is highly complex. Regarding surveillance of the Internet, Orin Kerr concludes that the applicable law of remedies "remains unusually obscure, and the rare judicial decisions construing the statutes tend to confuse the issues, not clarify them."[269] In particular, the division between suppression remedies and civil damages can be difficult to follow. At the risk of possible oversimplification, here is a path through this aspect of telecommunication privacy law in three easy steps.

First, an aggrieved party's ability to have material excluded—that is, suppressed—from use in court cases is legally limited to the content of conversations. Further, suppression is available only when the content is captured in transmission.[270] Money damages are also available for such illegal interceptions.[271] A complete defense to actions brought either for exclusion or for civil damages is supplied by a "good faith" test, following the United States Supreme Court's decision in *United States v. Leon*.[272] Similar to German law, considerable restrictions exist on the ability to exclude from use in court any material garnered through illegal surveillance.[273]

Second, an aggrieved party in the United States can obtain monetary damages for illegal surveillance of stored communications. A court assesses "the sum of the actual damages suffered by the plaintiff and any profits made by the violator as a result of the violation, but in no case shall a person entitled to recover receive less than the sum of $1,000."[274] Courts are also permitted to assess punitive damages for violations that are "willful or intentional."[275] And criminal remedies, mostly misdemeanor crimes, are also present for illegal access to stored communications.

267. § 91 Nr. 4 TKG. For a discussion of this authority, see TKG TREATISE, *supra* note 157, at 1465.

268. *Id.*

269. Kerr, *supra* note 101, at 807.

270. 18 U.S.C. § 2518(10) (2000).

271. *Id.* § 2520 (Supp. 2002).

272. United States v. Leon, 468 U.S. 897 (1984).

273. Following *Leon*, the "good faith" test is expressed in statutory language at 18 U.S.C. § 2520(d). One part of it permits a complete defense based on law enforcement's "good faith" belief that an authorized party had consented to the surveillance. 18 U.S.C. §2520(d)(3). Another such defense is provided by law enforcement's "good faith" reliance on "a court warrant or order, a grand jury subpoena, a legislative authorization, or a statutory authorization." 18 U.S.C. § 2520(d)(1).

274. *Id*. § 2707(c) (2000).

275. *Id.*

Third, and finally, violation of the requirements regarding use of pen registers is a misdemeanor crime.[276] The statute permits imprisonment for not more than one year, a fine, or both.[277] It is not clear, however, whether a civil remedy is present for violations of the Pen Register Statute. As Kerr notes, "[w]hether the Pen Register statute could support a private right of action is unclear; apparently no such suit has ever been brought."[278]

V. The Limits of Law and Possible "X" Factors

This Article has traced complex patterns of similarities and differences in United States and German telecommunications surveillance law. In this final section, I wish to go beyond telecommunications law and consider additional areas of law that may affect activity in this area. This section considers three "X" factors that may shape the larger legal context of telecommunications surveillance in the two countries.

At this moment, we return to James Whitman's insightful exploration of German "civility" law. After an examination of case law, statutes, and historical sources, Whitman finally attributes the differences in the two legal cultures regarding civility to a "leveling up" in Germany and a "leveling down" in the United States.[279] In particular, he finds that the German law of civility has its roots in conflict between aristocracy and the State. In brief, the German State first used law to displace dueling conflicts into courts, and then over a century or more, "leveled up" so that all Germans, and not just aristocrats, could seek recourse to harms to their honor.[280] No equivalent process took place in the United States; rather, according to Whitman, a "culture of disrespect" exists in the United States in which egalitarianism is demonstrated by all people being obliged to accept rough and ready manners.[281]

Whitman's scholarship leads one to wonder whether a similar or parallel explanation might be possible for differences in German and American practices regarding telecommunications privacy. Has there been a "Whitman Effect," i.e., a "leveling up," for telecommunications privacy in Germany and a "leveling down" in the United States? The short answer appears to be that one cannot say "yes" or "no." A highly significant problem, as I noted at the start of this Article, is that it is impossible at present to draw any empirical conclusions about the relative amounts of telecommunications surveillance. Moreover, the respective laws have numerous similarities and, in the absence of empirical data, it is difficult

276. *Id*. § 3121(d) (2000).
277. *Id*.
278. Kerr, *supra* note 101, at 818.
279. Whitman, *supra* note 3, at 1290.
280. *Id*. at 1300–20.
281. *Id*. at 1343.

ultimately to say whether the final effect of the German and U.S. legal regulations leaves practices in the two countries more similar or dissimilar.

Although one can not identify a "Whitman Effect" in comparing the telecommunications privacy law of Germany and the United States, it is possible to broaden the immediate field of scrutiny and consider, if only briefly, three additional areas that may have an impact in the two countries. Earlier in this Article, I suggested that Whitman's own findings regarding the law of civility may in some measure reflect not only law and history, but also differences in population density in the Germany and the United States.[282] What are possible "X" factors that affect telecommunications surveillance in Germany and United States?

Three additional areas that may affect surveillance activity in different ways are:

1. The United States views information privacy as more of an individual right; Germany as more of a group right.
2. The United States has "privatized" its telecommunications surveillance by encouraging providers to "voluntarily" surrender information.
3. Law enforcement officials in Germany face greater restrictions on arresting people than U.S. officials do. Thus, a source of pressure to engage in telecommunications surveillance order exists in Germany that does not occur in the United States.

I will now briefly assess each of these areas.

A. Privacy as an Individual Right/Privacy as a Group Right

In German constitutional law, as this Article has explored, the Constitutional Court views telecommunications privacy not as a mere individual right of privacy, but rather as an interest based in needs for societal communication and public participation. These concerns not only make information privacy a key concern for a democratic order, but also lead to limits on privacy. As the German court noted in its "Census" decision, information relating to a person depicts "an image of social reality that the concerned party cannot exclusively coordinate."[283]

In America, in contrast, the right of information privacy has often been seen as an individual right of control.[284] This aspect of privacy has led to a chorus of academic criticism.[285] As Priscilla Regan wrote in 1995,

282. *See supra* text accompanying note 26.

283. BVerfGE, 65 (1983), 1 (44).

284. For a discussion of scholars and caselaw that adopt the perspective that I elsewhere have termed, "privacy-control," see Schwartz, *Privacy and the State*, *supra* note 11, at 820–21.

285. *See* COLIN J. BENNET & CHARLES D. RAAB, THE GOVERNANCE OF PRIVACY: POLICY INSTRUMENTS IN GLOBAL PERSPECTIVE 26 (forthcoming 2003) (noting that "promotion of privacy can itself be socially important"). This important comparative work, by political scientists working in Canada and Scotland, identifies and faults the individualistic strand in Anglo-American privacy jurisprudence. *Id.* at 20–27.

for example, "[m]ost privacy scholars emphasize that the individual is better off if privacy exists; I argue that society is better off as well when privacy exists."[286] My own voice has been raised in this chorus. I have proposed that information privacy be seen as protecting both deliberative autonomy and deliberative democracy.[287] The latter interest points to a notion of privacy as a socially-based right. As I have written, "the law must structure the use of personal information so that individuals will be free from state or community intimidation that would destroy their involvement in the democratic life of the community."[288]

Comparative telecommunications privacy might, therefore, present an important area for American professors skeptical of an individual right of privacy-control. Through a "Whitman Effect," the German group-based right might be said to have led to a "leveling up" of privacy. Or, to express this idea differently, everyone's shared privacy right might be more difficult to diminish than an individually-based right. As in Aesop's *Fable of the Sticks*, where the bundled sticks could not be broken, there may be strength in numbers.[289] And, indeed, beyond telecommunications privacy, the German concept of privacy appears to have led to a higher level of privacy than in the United States in certain areas of data collection and processing. Sectors in which the level of privacy in Germany is generally held to be higher than in the United States include health care and employment.[290] Yet, again, we simply do not know if significant

286. PRISCILLA REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY 221 (1995).

287. Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 554, 560–61 (1995). For a different attempt to develop a similar American right, see Edward J. Eberle, *The Right to Information Self-Determination*, 2001 UTAH L. REV. 965.

288. Schwartz, *Privacy and the State*, *supra* note 11, at 561. In a later article, I called for information privacy rules to shape "the terms and conditions under which others have access to our personal data" to allow cyberspace to be "a place where we develop our commonality through democratic discourse." Schwartz, *Privacy and Democracy*, *supra* note 11, at 1652. In related work, Mary Coombs considered the idea of "shared privacy" in the context of the Fourth Amendment. Mary I. Coombs, *Shared Privacy and the Fourth Amendment, or the Rights of Relationships*, 75 CAL. L. REV. 1593 (1987). Her focus, however, is on third-party consent cases rather than telecommunications privacy. For other works by U.S. privacy scholars who have discussed a group-based right of privacy, see Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087 (2002); Daniel Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393 (2001); Julie E. Cohen, *Examined Lives: Information Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 (2000); Paul M. Schwartz, *Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy-Control, and Fair Information Practices*, 2000 WISC. L. REV. 743 (2000).

289. THE BUNDLE OF STICKS, AESOP FABLES, *in* 17 HARVARD CLASSICS (1909–14 ed.), *at* http://www.bartleby.com/17/1/72.html.

290. Regarding health data in Germany, see PAUL M. SCHWARTZ, EUROPEAN DATA PROTECTION AND MEDICAL PRIVACY IN GENETIC SECRETS: PROTECTING PRIVACY AND CONFIDENTIALITY IN THE GENETIC ERA 329 (Mark A. Rothstein ed., 1997). On the low level of health privacy protection in the United States, in particular in the aftermath of the Health

differences exist in comparative rates of telecommunications surveillance in Germany and the United States.

B. "Privatization" of Telecommunications Surveillance

As a second influence in this area, it might be that law enforcement officials are encouraging non-state actors to carry out surveillance. Both the USA PATRIOT Act in 2001 and the more recent Homeland Security Act in 2002 took modest steps to encourage telecommunication providers and ISPs to voluntarily turn over customer information to law enforcement.[291]

In current U.S. law, two possibilities exist for such voluntary disclosure of telecommunications information to a law enforcement agency. First, the service provider may disclose content that it has inadvertently received and that "appear[s] to pertain to the commission of a crime."[292] Second, the service provider may disclose to law enforcement if it "in good faith believes that an emergency involving danger of death or serious physical injury to any person requires disclosure without delay of communications relating to the emergency."[293] These two statutory exceptions are, on their face at least, highly limited. As a result, claims of privatization of telecommunications surveillance in the United States would be overstated at present. The legal exceptions certainly do not seem tantamount to a privatization of surveillance.

Yet, this picture may be changing. A *New York Times* article in late 2002 found that forty-one percent of corporate security officers in the United States were willing to supply customer information to law enforcement officials and government agencies without a court order.[294] The practices of telecommunications service providers and other

Insurance Portability and Accountability Act of 1996 ("HIPAA") privacy standard, see Lawrence O. Gostin & James G. Hodge, Jr., *Modern Studies in Privacy Law: National Health Information Privacy Regulations Under HIPAA: Personal Privacy and Common Goods: A Framework for Balancing Under the National Health Information Privacy Rule*, 86 MINN. L. REV. 1439, 1478–79 (2002). Regarding employment data in the United States, see SCHWARTZ & REIDENBERG, *supra* note 11, at 349–77. Although employment data in Germany are subject to generally high standards, the application of telecommunications privacy to an employee's e-mail and phone conversations is subject to some controversy at present. Experts in Germany do agree that the principle of telecommunications secrecy should apply to non-business related telecommunications generated in the employment context. The controversy concerns how the idea of telecommunications secrecy applies to business communications. Johann Bizer, *Die dienstliche Telekommunikation unter dem Schutz des Fernmeldegeheimnisse*, 25 DATENSCHUTZ UND DATENSICHERHEIT 618–19 (2001).

291. Of particular interest in this context is the Homeland Security Act, which includes language to insulate from liability telecommunication companies that surrender a wide range of customer information. 18 U.S.C. § 2701(b)(6) (2003).

292. *Id*. § 2702(b)(7)(A)(ii).

293. *Id*. § 2702(b)(8)(C).

294. John Schwartz, *Threats and Responses: Some Companies Will Release Customer Records on Request*, N.Y. TIMES, Dec. 18, 2002, at A16.

companies with regard to telecommunication attributes may soon look quite different than the requirements of the law on the books. Moreover, it is difficult to identify a similar trend in Germany at this date. Nonetheless, the American attitudes present in the *New York Times* poll are of too recent vintage to have yet significantly shaped U.S. surveillance practices.

C. Police Practices Concerning Arrests

I have saved the strongest possible additional influence on surveillance activities for last. It concerns one aspect of the comparative culture of law enforcement authorities in each country. A common theme in my conversations with governmental officials in Germany has been the claimed comparative reluctance of law enforcement officials there to arrest people due to legal restrictions that reflect a strong societal desire to avoid false arrests. Compared to the United States, German prosecutors are said to be obliged to build a case slowly in order to justify arresting a suspect, and, as a consequence, to have a motivation to seek wiretaps that is absent in the United States.

One difficulty in trying to isolate this influence as a comparative matter is that law enforcement officials in the United States do not merely arrest a higher relative percentage of the U.S. population compared to other countries, but also convict and incarcerate more individuals than any other country in the world.[295] Put differently, the higher rate of incarceration in the United States is likely to also reflect a comparatively greater readiness to arrest people. Indeed, one might logically anticipate that in the United States the officials who are so eager to arrest will also be ready to engage in wiretapping so that suspects can be convicted. Moreover, in both the United States and Germany, strong regional variations exist regarding the relative amount of surveillance orders within the country.[296] This distinction points to the likely presence, as has been noted, of local law enforcement norms as an influence on the decision to ask for a surveillance order.

With these caveats having been expressed, the German law regarding arrest does appear to set higher requirements than similar U.S. law. Regarding Germany, its Federal Criminal Procedure Code's section 112(1) permits detention pending trial (*Untersuchungshaft*) only in cases of a party who is "strongly suspected" (*dringend verdächtig*) of committing a crime.[297] Moreover, an arrest is forbidden when it would be "out of proportion to the significance of the circumstance and to the expected

295. Comparative information can be found at the International Centre for Prison Studies, King's College, *at* http://www.kcla.ac.uk/depsta/rel/icps/worldbrief/north_america_records.php?code=4.

296. *See supra* text accompanying note 35.

297. § 112(a) StPO. For an overview, see Pfeiffer, *supra* note 41, at 278–82.

punishment."[298] This test, as well as the further ones at Criminal Code section 112(2) and section 112a, appear stricter than the comparable American standards.[299] The comparable U.S. standard is a requirement of "probable cause that a crime has been committed and that the person to be arrested committed it."[300]

Thus, German telecommunications surveillance may be driven by a reluctance to arrest in a way that is not present in U.S. law. Here is a possible German trade-off: law enforcement officials are more likely to wiretap than arrest because the violation of one's liberty involved in an unjustified telecommunications wiretap is less than in a false arrest. At times, however, this carefulness may mean that some criminals are not only left free from arrest, but will evade justice—perhaps by fleeing the F.R.G.[301] German law enforcement did arrest a terrorist involved in the 9-11 conspiracy, however, and a German court convicted him on February 19, 2003.[302] We are again left to wonder, in Whitman's term, about the "clay" of different places.

A final observation is also possible regarding the comparative constitutional standards for telecommunications surveillance. In a dyspeptic reading of U.S. constitutional law, Michael Klarman views the Supreme Court as, having at best (or perhaps at worst?), "imposed culturally elite values in marginally countermajoritarian fashion."[303] Yet, the Supreme Court has not taken even such limited action regarding telecommunications attributes; it has resolutely taken itself out of involvement in this area. As a result, the comparative U.S.-German landscape regarding telecommunications surveillance may one day look quite different than the portrait that this Article has drawn. It will depend on the merits of the statutes that the two countries enact or do not enact in the next years.

298. *Id*.

299. § 112 Nr. 2 StPO; § 112a StPO. For an overview, see Pfeiffer, *supra* note 41, at 278–82, 283–85.

300. WAYNE LAFAVE & JEROLD H. ISRAEL, CRIMINAL PROCEDURE 146 (3d ed. 2000). For Supreme Court cases finding arrests to have been made "at large" or otherwise without probable cause, see Mallory v. United States, 354 U.S. 449 (1957); Johnson v. United States, 333 U.S. 10 (1948).

301. *See* Desmond Butler, *Terror Suspect's Departure From Germany Raises Concern in Other Nations*, N.Y. TIMES, Dec. 23, 2002, at A14 (German prosecutors note insufficient evidence to prevent suspect in Djerba bombing from leaving Germany for Saudi Arabia.), *available at* http://www.nytimes.com/2002/12/24/international/europe/24BERL.html.

302. Peter Finn, *Moroccan Convicted in Sept. 11 Attacks*, WASH. POST, Feb. 19, 2003, at A1, *available at* http://www.washingtonpost.com/wp-dyn/articles/A32352-200Feb19.html.

303. Michael J. Klarman, *What's So Great About Constitutionalism?*, 93 NW. U. L. REV. 145, 146 (1998).

Conclusion

A U.S. Secretary of State during the 1920s, Henry Stimson, dissolved a small codebreaking unit in the government with these words, "[g]entlemen do not read each other's mail."[304] Those days are gone. In Germany and the United States today, surveillance is an accepted part of the behavior of law enforcement officials with an ongoing increase in the grounds under which telecommunications surveillance, in particular, is justified.

This Article began by exploring difficulties in reaching any judgment about the relative amounts of telecommunications surveillance in Germany and the United States. Due to differences in the way that the respective national statistics are maintained, which in turn reflect underlying distinctions within the legal regimes, the available data measure different phenomenon. In response, this Article has made a modest proposal that the collection of U.S. wiretap statistics be expanded to include the number of connections subject to surveillance. It has also proposed that all states should be required to file an annual report with the responsible federal official regardless of whether surveillance activity has taken place. Such filing of reports would resolve any doubts about incomplete U.S. surveillance statistics. Yet, even though an empirical basis is absent at present for comparisons, one can still examine and evaluate legal aspects of the respective German and U.S. legal regulations for telecommunication surveillance.

At the constitutional level, this Article found that the U.S. Supreme Court has developed a restrictive vision of the Fourth Amendment that has generally meant that telecommunications attributes are not protected by the U.S. Constitution. In Germany, in contrast, Article 10 of the Basic Law contains protections for communications privacy that the Federal Constitutional Court has explicitly extended to telecommunications attributes.

My chief findings regarding statutory law are as follows: statutory law in Germany provides somewhat more flexibility for law enforcement agencies to obtain connection data than content, but the former kind of telecommunication attributes still receive relatively higher legal safeguards in Germany than in the United States. Moreover, stored data, an important concept in U.S. law, is not a jurisprudential category in German telecommunications privacy law. Finally, U.S. law requires neither retention nor erasure of telecommunications data. In contrast, current German law generally requires telecommunications connection data to be erased after no longer than six months. Like the United States, German law has no requirement for mandatory data retention, but this area is one of current controversy there and elsewhere in Europe.

304. DANIEL KAHN, THE CODEBREAKERS 360 (1967).

In this Article's final section, I analyzed three additional areas of influence upon the comparative regimes of telecommunications surveillance in Germany and the United States. Perhaps the most intriguing of these are the contrasting legal regulations regarding the arrest of suspects. In Germany, law enforcement officials face considerable limits on their ability to arrest and, as a result, may have relatively greater pressure to use telecommunications surveillance. A strong influence on German telecommunications surveillance may be the desire to avoid violations of civil liberties through false arrests.