REGULATING GOVERNMENTAL DATA MINING IN THE UNITED STATES AND GERMANY: CONSTITUTIONAL COURTS, THE STATE, AND NEW TECHNOLOGY

PAUL M. SCHWARTZ*

* Professor of Law, Berkeley Law School; Director, Berkeley Center for Law & Technology. This paper greatly benefitted from comments and suggestions made at the William & Mary School of Law's Symposium, *Constitutional Transformations: The State, the Citizen, and the Changing Role of Government*, and at workshops of Fordham Law School's Information Policy Law Center and Loyola Law School Los Angeles. For their invitations to participate in these events, I thank the *William and Mary Law Review*, Neal Devins, Joel Reidenberg, and Jennifer Rothman. Unless otherwise noted, all translations are my own.

INTRODUCTION

For the anthropologist Clifford Geertz, law is "part of a distinct manner of imagining the real."[1] In *Local Knowledge*, he argues that, at a fundamental level, legal systems create a way of envisioning the world and then develop different kinds of "techniques"—whether through legal institutions, methods, or doctrines—that make this vision the correct one.[2] The consequence is, of course, that the law in different countries will "see" different things. This point proves applicable to the study of comparative privacy law. Building on Geertz's insight, this Article searches for distinct as well as shared aspects of one area of law in two countries. It seeks to determine whether German and American lawyers, judges, and policymakers are seeing the same or different things when regulating one form of technology—namely, data mining.

As a further matter, current privacy scholarship has a great need for targeted studies that look at specific areas of information use in different countries. After a first generation of broader comparative studies, today's privacy scholarship needs more targeted analysis of specific areas of data use. As Spiros Simitis has argued, "[e]ffectiveness of data protection law crucially depends on the ability to react in a fashion that focuses on concrete situations of processing, and the ones that are especially important from the perspective of the affected party."[3] In such a fashion, this Article will look at how the legal systems of Germany and the United States respond to the use of data mining by the government for law enforcement and national security purposes.

As an initial matter, it is important to establish certain basic terminology. Americans commonly refer to "data mining"; in Germany, the standard reference is to "*Rasterfahndung*," which literally means "a screening search."[4] In this Article, I use data mining as the general term of art and to refer to the practice in the United

1. CLIFFORD GEERTZ, LOCAL KNOWLEDGE 173 (3d ed. 2000).

2. *Id.*

3. Spiros Simitis, *Einleitung* [Introduction] to BUNDESDATENSCHUTZGESETZ 127 (Spiros Simitis ed., 6th ed. 2006) (Ger.).

4. *See infra* Part I.B.

States. In discussing German law, I refer to this practice as "data screening." This term is a closer translation of the German concept, and its use will permit a reader to know at a glance that a reference is to Germany. Another benefit of this approach is that it avoids an assumption that American and German jurists are using the same mental map when they speak of "data mining" or "data screening," respectively.

Although this Article employs these two terms, a computer remains a computer, whether in the United States or Germany, and the underlying technology in both countries is the same. One can, therefore, provide a unitary definition of data mining as a series of techniques for extracting knowledge from large stores of digital data. Alternative terms for this technique include "knowledge mining from data, knowledge extraction, data/pattern analysis, data archaeology, and data dredging."[5] Another definition views data mining simply as involving "a diverse set of tools for mathematical modeling."[6]

Part I of this Article explores the basic regulation of this technique in Germany and the United States. It finds a long engagement with data screening in Germany, one that dates back to the battle against the Red Army Faction in the 1970s. German law also regulates this practice in both federal and state statutes. In contrast, decisions of the U.S. Supreme Court from the 1970s have created a constitutional jurisprudence that frees the use of this process from the strictures of constitutional law. At the statutory and administrative level, moreover, there is scant regulation of this practice. Part II then examines the German Federal Constitutional Court's *Data Screening* decision of 2006.[7] In this decision, the German court read strict constitutional requirements into any use of data screening for so-called "preventive purposes." Finally, Part III contrasts the German and American legal approaches to this

5. JIAWEI HAN & MICHELINE KAMBER, DATA MINING: CONCEPTS AND TECHNIQUES 5 (2d ed. 2006).

6. NAT'L RESEARCH COUNCIL, PROTECTING INDIVIDUAL PRIVACY IN THE STRUGGLE AGAINST TERRORISTS: A FRAMEWORK FOR PROGRAM ASSESSMENT 20 (2008) [hereinafter PROTECTING INDIVIDUAL PRIVACY].

7. Bundesverfassungsgericht [BVerfG] [Federal Constitutional Court] Apr. 4, 2006, 115 ENTSCHEIDUNGEN DES BUNDESVERFASSUNGSGERICHTS [BVERFGE] 320 (para. 8, at 323, para. 28-33, at 329).

new technology for law enforcement and intelligence agencies. This Article draws comparative lessons about the differences between the U.S. Supreme Court's hands-off approach, and the "new constitutionalism" of Germany, which features a constitutional law court that concentrates solely on interpreting and developing a constitution. This Article further highlights two contrasting approaches, at the substantive level, to a constitutional law of information privacy.

I. DATA MINING AND *RASTERFAHNDUNG* (DATA SCREENING)

This Part will explore the basics of German and American regulation of the state's data mining for law enforcement and intelligence purposes. In the United States, the practices of data mining are largely unregulated with the main focus placed on the initial collection of information and not on the processes to which it is subsequently put. In contrast, data screening is closely regulated in Germany. It is also organized along a distinction concerning whether this technique is used to investigate past crimes or to carry out a preventive response to potential crimes.

A. Data Mining in the United States

In the United States, legal policymakers draw a distinction between "subject-based" and "pattern-based" data mining.[8] In subject-based searches, law enforcement officers or intelligence agents use data mining to gather information about subjects that they already suspect of possible wrongdoing or that are otherwise of interest.[9] The National Research Council's blue ribbon report, *Protecting Individual Privacy in the Struggle Against Terrorists*, places subject-based data mining "[o]n the more routine end of the spectrum."[10] It observes that this technique involves "the searching of large databases for characteristics that have been associated with individuals of interest, that is, people who are worthy of further

8. PROTECTING INDIVIDUAL PRIVACY, *supra* note 6, at 20-24; *see also* TECH. & PRIVACY ADVISORY COMM. DEP'T OF DEF., SAFEGUARDING PRIVACY IN THE FIGHT AGAINST TERRORISM 45 (2004) [hereinafter SAFEGUARDING PRIVACY].

9. PROTECTING INDIVIDUAL PRIVACY, *supra* note 6, at 21-22.

10. *Id.* at 20.

investigation."[11] As a specific example, in subject-based data mining, officials seek data about "people who own cars with license plates that are discovered at the scene of a terrorist act or whose fingerprints match those of people known to be involved in terrorist activity."[12] This technique automates activities that a detective or intelligence analyst might otherwise have carried out manually when drawing on analog data.[13] Yet this technique also broadens and expands these activities by allowing officials to make use of the extensive databases of our Information Age.[14]

With pattern-based data mining, in contrast, the government investigator develops a model of assumptions about the activities and characteristics of culpable individuals or the indicators of criminal or terrorist plans.[15] The investigator then uses computer software to search databases containing transactional and personal information for "hits" or matches.[16] The search looks for a correspondence between a model of criminal or terrorist plans and the patterns created by data left by potentially culpable individuals.[17] This approach identifies the guilty by their data trails. Particularly important in pattern-based data mining is a mechanism for feedback so that learning over time is possible.[18] In particular, there is a need to test the assumptions upon which the pattern-based analysis rests.[19]

In the United States, constitutional law and criminal procedure leave data mining, whether subject-based or pattern-based, largely unregulated. Statutory law does place some limits on the government's initial ability to collect information.[20] There is, however, an exception to this rule of nonregulation, which concerns a small subcategory of data mining, one largely shrouded in secrecy. In the

---

11. *Id.* at 20-21.
12. *Id.* at 21.
13. *Id.*
14. *Id.*
15. Ira S. Rubinstein, Ronald D. Lee & Paul M. Schwartz, *Data Mining and Internet Profiling: Emerging Regulatory and Technological Approaches*, 75 U. CHI. L. REV. 261, 262-63 (2008); *see also* SAFEGUARDING PRIVACY, *supra* note 8, at 45.
16. Rubinstein, Lee & Schwartz, *supra* note 15, at 262-63.
17. *Id.*
18. PROTECTING INDIVIDUAL PRIVACY, *supra* note 6, at 22.
19. *Id.*
20. SAFEGUARDING PRIVACY, *supra* note 8, at executive summary 4-5.

Foreign Intelligence Surveillance Act of 1978 (FISA) Amendments Act of 2008, Congress created procedures for the National Security Agency's (NSA) surveillance of certain phone calls with a nexus to the United States.[21] At the same time, this statute does not regulate data mining per se.[22]

We begin, however, not with the exception, but with the rule. In American law, the Fourth Amendment is the critical constitutional provision regarding data mining. The Fourth Amendment establishes the right of the people to be secure from "unreasonable searches and seizures" in their "papers, and effects."[23] It also prohibits the issuing of search warrants for reasons less than "probable cause."[24] By the 1970s, the Supreme Court had developed the essential Fourth Amendment case law, and its opinions in *United States v. Miller* and *Smith v. Maryland* remain the leading cases in this area.[25] Due to the Supreme Court's interpretation of the reach of the Fourth Amendment, data mining is left free of constitutional restrictions.[26] The first restriction, from the *Miller* opinion, finds that the Fourth Amendment is inapplicable to stored data in the control of third parties.[27] The second restriction, from *Smith v. Maryland*, finds that the Amendment is inapplicable to any aspect of telecommunications that is not the "content" of a telephone conversation.[28]

In *Miller*, the Supreme Court declared that no "legitimate 'expectation of privacy'" existed in documents that an individual stored with a third party.[29] *Miller* concerned bank records, and the Court found that a "depositor takes the risk, in revealing his affairs to another, that the information will be conveyed by that person to the Government."[30] In *Smith v. Maryland*, the Supreme Court

21. Pub. L. No. 110-261, 122 Stat. 2436 (codified as amended in scattered sections of 18 and 50 U.S.C.).

22. *Id.*

23. U.S. CONST. amend. IV.

24. *Id.*

25. Smith v. Maryland, 442 U.S. 735 (1979); United States v. Miller, 425 U.S. 435 (1976).

26. Paul M. Schwartz, *German and U.S. Telecommunications Privacy Law: Legal Regulation of Domestic Law Enforcement Surveillance*, 54 HASTINGS L.J. 751, 764-65 (2003).

27. *Id.*

28. *Id.* at 764.

29. *Miller*, 425 U.S. at 442.

30. *Id.* at 443.

developed a "content" versus "non-content" distinction.[31] It found that the Fourth Amendment did not protect the phone numbers that one dialed.[32] The petitioner in the case "voluntarily conveyed numerical information to the telephone company and 'exposed' that information to its equipment in the ordinary course of business."[33] The Supreme Court drew a distinction in this case with its earlier opinion in *Katz v. United States*, in which it had decided that the Fourth Amendment safeguarded the words spoken during a call from a telephone booth.[34] In *Katz*, the Court found that the Fourth Amendment protected communication contents from the "uninvited ear."[35]

Miller and *Smith* effectively foreclosed the possibility of meaningful constitutional protections from governmental data mining in the United States. In its use of data mining, the government scrutinizes personal data, whether through subject-based or pattern-based searches, that is initially in the control of third parties, as in *Miller*. Moreover, this information is generally noncontent, that is, not the words spoken into a telephone, but various data crumbs that an individual created and left in the control of third parties, as in *Smith*. As the National Research Council's report summarizes, "Today, the *Miller* and *Smith* decisions allow the government to obtain the raw material on millions of individuals."[36]

At the statutory level, moreover, the law of criminal procedure simply does not consider data mining a "search." The logic of *Miller* and *Smith* has carried the day here as well. As an example, the FBI permits agents to carry out a so-called "assessment" even when there is "no particular factual predication" about a target.[37] Such an inquiry can include searching databases.[38] As a further matter, statutory law and regulations have encouraged and made routine a

31. 442 U.S. 735 (1979).

32. *Id.* at 743-44.

33. *Id.* at 744.

34. *Id.* at 739-42; *see also* Katz v. United States, 389 U.S. 347 (1967).

35. *Katz*, 389 U.S. at 352.

36. PROTECTING INDIVIDUAL PRIVACY, *supra* note 6, at 34.

37. FED. BUREAU OF INVESTIGATION, DOMESTIC INVESTIGATIONS AND OPERATIONS GUIDE 39 (2008), *available at* http://documents.nytimes.com/the-new-operations-manual-from-the-f-b-i.

38. *Id.*

widespread sharing of personal information by private sector institutions with the government.

In the context of financial information, we can consider the strict obligations that the law now places on banks and other entities to carry out due diligence about their customers and to report suspicious activities to the government. These obligations are considered essential steps in the prevention of terrorist financing, money laundering, and other illegal activities.[39] As a specific illustration of such a data flow, regulations promulgated under the Bank Secrecy Act require financial institutions and other regulated entities to file reports for every deposit, withdrawal, or other transfer of currency exceeding $10,000.[40] More broadly, these regulated entities must report all "suspicious activities" to the government by filing "Suspicious Activity Reports" (SARs).[41] The Financial Crimes Enforcement Network (FinCEN) of the U.S. Treasury Department receives the filed SARs. As the website of FinCEN states, "There are hundreds of thousands of financial institutions currently subject to [the Bank Secrecy Act's] reporting and record keeping requirements."[42]

Beyond the Bank Secrecy Act and FinCEN, a wide variety of federal and state statutes and regulations have standardized the process of widespread, large-scale transfers of data to the government.[43] This information can also be subject to pattern-based or subject-based data mining. There is one final area to be considered in a discussion of data mining in the United States, and it concerns

---

39. *See Oil-for-Food Program: Tracking the Funds: Hearing Before the H. Comm. on Int'l Relations*, 108th Cong. 51-52 (2004) (statement of Herbert A. Biern, Senior Assoc. Dir., Div. of Banking Supervision and Regulation, Fed. Reserve), *available at* http://www.federalreserve.gov/boarddocs/testimony/2004/20041117/default.htm.

40. 31 C.F.R. § 103.22(b)(1) (2010); *see also* Bank Secrecy Act of 1970, Pub. L. No. 91-508, 84 Stat. 1114 (codified as amended in scattered sections of 12 and 31 U.S.C.).

41. *See* 12 C.F.R. § 208.62 (2011).

42. *Forms*, FINCEN, U.S. DEP'T OF THE TREASURY, http://www.fincen.gov/forms/bsa_forms/ (last visited Oct. 31, 2011).

43. *See, e.g.*, Privacy Act, 5 U.S.C. § 552a (2006) (regulating use of personal information by federal agencies); I.R.C. § 6103 (2006) (establishing rules for disclosure of tax record to executive branch officials, federal officers, Congress, state tax officials, and state and local law enforcement agencies); DNA Identification Act, 42 U.S.C. §14131 (2006) (establishing rules under which the FBI indexes DNA identification records). For an analysis of the Internal Revenue Code's regulation of governmental access to tax return information, see Paul M. Schwartz, *The Future of Tax Privacy*, 61 NAT'L TAX J. 883, 892-95 (2008).

a specific activity carried out for national security purposes: the National Security Agency's widespread monitoring of signal traffic.

In December 2005, a front-page article in the *New York Times* first revealed the NSA's warrantless surveillance program. This agency was intercepting communications in which one party was located outside the United States and the other party was located inside the United States, and it was doing so without gaining warrants from the Foreign Intelligence Surveillance Court (FISC).[44] This activity proved highly controversial; although much about this surveillance remains secret, it is clear that the NSA failed to follow the requirements of the FISA for such surveillance.[45] Rather than seeking to amend FISA so that it would authorize such investigative authority, the Bush administration directed the NSA to carry out this activity secretly.[46] It even improvised a new kind of process to work around the later refusal of Attorney General Ashcroft and his deputy James Comey to assent to the NSA activity.[47]

It is also clear that the activities in question involved data mining: the NSA was subjecting data traffic to so-called "umbrella surveillance."[48] Under FISA, the FISC was required to make a probable cause determination regarding each "target," that is, each individual, and each "facility" of telecommunications before surveillance could be carried out.[49] In contrast, the NSA had engaged in a different approach, under which "the NSA would sweep in a wide amount of data up front and then sift through it."[50]

This process involved data mining. At the end of the sifting process, the FISC would review the NSA's judgment as to the captured data.[51] An anonymous official also explained at one point in the

---

44. James Risen & Eric Lichtblau, *Bush Lets U.S. Spy on Callers Without Courts*, N.Y. TIMES, Dec. 16, 2005, at A1.

45. *Id.*; *cf.* Foreign Intelligence Surveillance Act, 50 U.S.C. §§ 1801-1811 (2000).

46. *See* Risen & Lichtblau, *supra* note 44, at A1.

47. *See* Paul M. Schwartz, *Warrantless Wiretapping, FISA Reform and the Lessons of Public Liberty: A Comment on Holmes's Jorde Lecture*, 97 CALIF. L. REV. 407, 423 (2009).

48. *Id.* at 413-14.

49. *See* 50 U.S.C. § 1805(a); *see also* DAVID S. KRIS & J. DOUGLAS WILSON, NATIONAL SECURITY INVESTIGATIONS & PROSECUTIONS § 15:18 (2007).

50. Schwartz, *supra* note 47, at 414.

51. As Kris summarizes, the idea was "to move the individualized probable-cause determination from the front end, to the back end, of the FISA process." KRIS & WILSON, *supra* note 49, § 15:18.

controversy that the FISC ruling concerned cases "where one end is foreign and you don't know where the other is."[52] The Bush administration argued that the FISC's opinion impeded the government's ability to investigate threats of imminent terrorist attacks and necessitated amendment of FISA.[53]

Some courts have ruled on challenges to these practices, and some legal claims remain active. The path of litigation has been rocky, and the "state secrets" privilege has furnished one particularly significant obstacle for plaintiffs.[54] In the legislative arena, Congress largely ratified the Bush administration's path by enacting the FISA Amendment Act of 2008 (FAA), and even provided retroactive immunity for the telecommunication companies that participated in the warrantless wiretapping.[55] This statute, however, does create some additional procedural steps that provide safeguards against abuse of this procedure.[56] We will return to the FAA in Part III.

---

52. Greg Miller, *New Limits Put on Overseas Surveillance*, L.A. TIMES, Aug. 2, 2007, at A16.

53. *Id.*

54. *See* Schwartz, *supra* note 47, at 428 ("The state secrets privilege is a common law evidentiary privilege that has been interpreted by courts in a fashion that adds additional difficulties for the use of litigation to expose governmental abuses in areas that involve national security."). In a major empirical study of the state secrets privilege, Laura Donohue has demonstrated that both the government and private-sector companies alike are now relying on it in civil litigation as a powerful litigation tool. Laura K. Donohue, *The Shadow of State Secrets*, 159 U. PA. L. REV. 77 (2010). Finally, due to FISA's provision of remedies, the reward for even successful plaintiffs who surmount all litigation difficulties will likely be limited. In one case regarding the NSA's warrantless wiretapping, the government refused to participate in FISA-mandated discovery, and the federal district court decided to grant the plaintiff's motion for summary judgment. *In re* NSA Telecomm. Records Litig., 700 F. Supp. 2d 1182 (N.D. Cal. 2010). The result? The individual plaintiffs received $20,400 in liquidated damages pursuant to FISA 1801(a), which represented $100 a day for violations over a period of 204 days. *In re* NSA Telecomm. Records Litig., No. 06-1791, 2010 U.S. Dist. LEXIS 136156 (N.D. Cal. 2010). On a more positive note for litigators, the plaintiffs' attorneys received attorney fees of $2.5 million.

55. Specifically, the FAA prohibits a civil action against anyone for assisting the intelligence community in connection with an activity that falls within a defined safe harbor. *See* 18 U.S.C.A. § 2511(2)(a)(ii) (West 2010). This statutory provision led the district court handling consolidated claims against AT&T to dismiss the actions. *In re* NSA Telecomm. Record Litig., 633 F. Supp. 2d 949 (N.D. Cal. 2008).

56. *See* Schwartz, *supra* note 47, at 417.

B. Data Screening in Germany

The German discussion of data mining uses different terms and has developed along different organizational principles. To illustrate, we reference statutes at the federal and state levels that regulate the use of data screening. These laws do not draw a distinction between subject-based and pattern-based data mining, as in the United States, but distinguish between the use of "data screening" to (1) investigate past crimes, or (2) permit a prevention response to potential crimes. The latter technique is also called "strategic data screening."

In Germany, data screening is an established technique of law enforcement authorities. Its use by law enforcement dates back to the 1970s and the country's struggle against the Red Army Faction (RAF).[57] The German pioneer of this technique and its legendary champion was Horst Herold, head of the *Bundeskriminalamt*, or Federal Criminal Police Office (BKA). This federal agency is the national investigative police authority of Germany and is located within the Federal Ministry of the Interior. It is analogous to the Federal Bureau of Investigation in the United States.

The German neologism for data screening is "*Rasterfahndung*." "*Fahndung*" means to search; and a "*Raster*" is a screen. Thus, the term literally refers to a "screening search." In 1980, the Society for the German Language selected "*Rasterfahndung*" as the Word of the Year.[58] A classic example of a data screening by Herold's BKA occurred in 1979. Herold suspected that the RAF had one or more apartments in Frankfurt am Main that it was using for conspirative purposes.[59] Another German neologism describes such a dwelling. The applicable term is a "*konspirative Wohnung*," or conspirative apartment, which was the German Word of the Year in 1978.[60]

Herold decided, correctly as it turned out, that terrorists were likely to pay for electricity differently than most Germans.[61] In

57. *See* Francesca Bignami, *European Versus American Liberty: A Comparative Privacy Analysis of Antiterrorism Data Mining*, 48 B.C. L. REV. 609, 653 (2007).

58. *Wort des Jahres*, GESELLSCHAFT FÜR DEUTSCHE SPRACHE, http://www.gfds.de/index.php?id=11 (last visited Oct. 31, 2011).

59. DIETER SCHENK, DER CHEF—HORST HEROLD UND DAS BKA 399 (2000).

60. GESELLSCHAFT FÜR DEUTSCHE SPRACHE, *supra* note 58.

61. SCHENK, supra note 59, at 399.

his assessment, terrorists would be unlikely to transfer money directly from their bank account to a public utility's bank account.[62] In Germany, it is common to use bank-to-bank transfers (*Überweisungen*) to pay regularly occurring charges. A bank examines identity documents, however, when one opens an account with it. As a result, Herold thought terrorists would use cash and pay their electricity bill in person at the utility.[63] This tactic would keep their apartments associated with a false name.

Herold's operation involved a data screening of the list of approximately 18,000 utility customers who paid cash against various lists of "legal names."[64] These certified identities were collected by recourse to the data files of various agencies and organizations. The legal names included people listed at the Registration Office for Inhabitants (*Einwohnermeldeamt*), owners of automobiles, retirees, students receiving government scholarships, owners of real estate, purchasers of fire insurance, and people receiving health insurance from publicly-authorized companies.[65]

Pursuant to a court order, the electric company in Frankfurt am Main gave Herold computer tapes with the list of its cash paying customers.[66] Herold then screened these tapes against the computer tapes with the certified names. This process revealed two false names associated respectively with two apartments.[67] One false name proved to be used by a drug dealer, and the other was used by a terrorist that the BKA was seeking to arrest.[68] Shortly after the data match, law enforcement was able to arrest the terrorist, Rolf Heißler, in the "conspirative apartment."[69]

Today, data screening in investigations of past crimes, such as those investigations that Herold carried out, is regulated by various state laws and at the federal level by section 98a of the Criminal

62. *Id.*
63. *Id.*
64. *Id.*
65. *Id.* at 399-401.
66. *Id.*
67. *Id.*
68. *Id.* For an account of a similar investigative approach by Herold after the kidnapping of Hanns-Martin Schleyer, see STEFAN AUST, DER BAADER MEINHOF KOMPLEX 654 (3d ed. 2008) (Ger.).
69. SCHENK, *supra* note 59, at 399-400.

Procedural Code (*Strafprozeßordnung*).[70] The federal statute applies when the BKA takes a lead role in investigating crimes considered to be a federal matter. The Criminal Procedure Code's basic approach also reflects the approach the different state laws take, and our discussion can, therefore, concentrate on the federal statute.

C. The Statutory Regulation of Data Screening

In section 98a, the Criminal Procedure Code regulates the "automatic comparison and transfer of personal data."[71] It requires "sufficient factual indications to show that a criminal offense of significant importance has been committed."[72] Thus, this statute squarely requires proof of the existence of a crime. It can be used for subject-based or pattern-based investigations, to use the American concepts, but only under narrow circumstances. As section 98a of the Criminal Procedure Code indicates, this statute requires a sufficient level of proof both that a crime has been committed and that this crime is on a list of selected, significant predicate offenses. It also restricts use of data screening to situations in which "other means of establishing the facts or determining the perpetrator's whereabouts would be considerably less promising or would be much more difficult."[73] Further, section 98b mandates a judicial order for data screening, unless exigent circumstances exist.[74]

Thus, Criminal Procedure Code sections 98a-b indicate that German law cabins data mining carefully. The leading empirical examination of the practice of data screening found a significant

---

70. STRAFPROZEßORDNUNG [STPO] [CODE OF CRIMINAL PROCEDURE], 1 BUNDESGESETZBLATT [BGBL. I] 1074, § 98a (1987).

71. *Id.*

72. *Id.*

73. *Id.*

74. *Id.* § 98b. The statute also permits data screening to be carried out both for so-called "positive" screening, to identify potential suspects, or negative screening, to exclude people from a list of potential suspects. It states, "personal data relating to individuals fulfilling certain presumed characteristics of the perpetrator may be compared by machine with other data in order to exclude individuals not under suspicion or to identify individuals who meet other characteristics meaningful to the investigation." *Id.* As an example of a positive screening, under Herold's leadership, the BKA screened customers who paid their electricity bill with cash against certified names to find potential suspects. *See supra* text accompanying notes 61-69.

increase in the use of subject-based data mining since 2002.[75] Its most significant deployment was in cases involving murders or manslaughter, sexually motivated crimes, and serial criminal offenses.[76]

In contrast to federal law in Germany, there are state statutes that permit a preventive use of this practice.[77] To illustrate such a pattern-based approach, the police would start by considering the data trails left by the al-Qaeda terrorists who were responsible for the 9/11 attacks in the United States. The police would develop a computer model that captured these patterns and then run a search of recent data to identify suspects. Such an investigation would be a "preventive investigation" in the terminology of German law. In 2006, the German Federal Constitutional Court established significant limits on such law enforcement use of data screening.[78] We now turn to this decision.

II. THE FEDERAL CONSTITUTIONAL COURT'S *DATA SCREENING* OPINION

In this opinion, the Federal Constitutional Court found data screening to be constitutional only if justified by the existence of a "concrete danger" to the security of the country, an individual state, or the life of a citizen.[79] Most of the Constitutional Court's opinion explained why data screening posed a significant infringement upon the German constitutional right of informational self-determination and further developed its existing proportionality test as a constitutional yardstick for evaluating the permissibility of data screening.[80] This part of the opinion ultimately found the contested statute to be constitutional, and all justices joined this outcome. Nonetheless, in a second, shorter part of its judgment, the Constitutional Court declared unconstitutional a lower court's judgment upholding a data

75. DIRK PEHL, DIE IMPLEMENTATION DER RASTERFAHNDUNG 292 (2008) (Ger.).

76. *Id.*

77. *See, e.g.*, Polizeigesetz des Landes Nordrhein-Westfalen [PolG NW] [North Rhine-Westphalia Police Statute], 10 GESETZ- UND VERORDNUNGSBLATT FÜR DAS LAND NORDRHEIN-WESTFALEN [GV NRW] 70, § 31 (1990).

78. BVerfG Apr. 4, 2006, 115 BVERFGE 320.

79. *Id.*

80. *See infra* Part II.B.2.

screening operation in 2001 in North Rhine-Westphalia.[81] Two members of the Court dissented from its rejection of the holding of the lower court, and one of these judges, Justice Evelyn Haas, wrote a stinging dissent.[82]

A. Background of the Case

Immediately after the terrorist attacks in the United States on September 11, 2001, a committee of Interior Ministers of the German states, under the BKA's leadership, developed a plan for the state criminal police to carry out a data screening operation to discover cells of "sleeper" terrorists in Germany.[83] The criminal police collected personal data from universities, the Registration Office for Inhabitants, and the Central Register for Foreigners. According to the Constitutional Court, the different police headquarters received "data batches" (*Datensätze*) with information on 5.2 million persons.[84] The police then used computers to search through these data using the following criteria: men; age from eighteen to forty years old; student or former student; Islamic religion; land of birth or nationality in certain specific countries with a majority Islamic population.[85]

The information collected at the state level was then transferred to the BKA, where it was incorporated into a federal database termed "Sleepers." According to the BKA, this file included 31,988 entries.[86] The BKA screened this information against further data that it had collected.[87] Matching information was placed in a

81. *See infra* text accompanying note 98.

82. *See infra* Part II.C.

83. 115 BVERFGE 320 (para. 7-10, at 323-24).

84. *Id.* para. 8, at 323, para. 28-33, at 329.

85. *Id.* para. 26, at 328.

86. *Id.* para. 9, at 324.

87. In its opinion, the Constitutional Court cited an estimate by the Federal Data Protection Commissioner that the BKA's electronic dossier used in this comparison (*Abgleichsdaten*) contained information on about 200,000 to 300,000 persons. *Id.* The Constitutional Court did not provide complete details as to the contents of this second file; it did state, however, that among the contents was information on individuals who had applied for a pilot's license and persons that required a "Reliability Check" (*Zuverlässigkeitsprüfung*) under the Nuclear Energy Act because of involvement in maintaining or running nuclear plants or transporting nuclear material. *Id.*

"results file" (*Ergebnisdatei*) and made available to state offices of criminal police.[88]

The data screening was controversial and led to numerous media reports about it as well as protests on privacy grounds involving, among others, state data protection commissioners.[89] The data protection commissioners raised questions about whether law enforcement officials had followed constitutional and statutory norms in their data screening procedures.

The data screening also took place against a history of individuals and groups in Germany with ties to Osama bin Laden.[90] As the report of the 9/11 Commission in the United States later made clear, one such cell supplied key participants, including Mohamed Atta, for the 9/11 attacks on the United States.[91] Beyond the Hamburg cell, individuals with ties to bin Laden also lived in North Rhine-Westphalia, which was the locus of the data screening operation that the Constitutional Court of Germany evaluated in its opinion.[92] As we will see, the dissenting opinion in the Constitutional Court's *Data Screening* decision emphasized the significance of the presence of these individuals in the state as a justification for the contested law enforcement activity. Despite these terrorists' ties to Germany, however, the contested data screening was notably unsuccessful and all information in the results dossier was erased in 2003 and 2004.[93] As the Constitutional Court noted, "The data screening led in no instance, as far as is apparent, to the discovery of 'sleepers,' or, based on knowledge gained, even to charges against one of the registered persons, such as charges due to membership in or in support of a terrorist organization."[94]

---

88. *Id.* The Court also explained that the BKA considered a "hit" between the two dossiers to be any match in two parts of the file, "such as name and date of birth or name and land of birth." *Id.*

89. *Id.* para. 59, at 338.

90. *Id.* para. 25, at 328.

91. NAT'L COMM. ON TERRORIST ATTACKS UPON THE U.S., THE 9/11 COMMISSION REPORT 160-69 (2004).

92. 115 BVERFGE 320 (para. 11-33, at 324-31).

93. *Id.* para. 32, at 330-31.

94. *Id.* para. 10, at 324 (internal citation omitted).

B. The "Concrete Danger" Requirement

A former student at the University of Duisburg challenged the statutory authorization for the post-9/11 data screening operation. The plaintiff, who was of Moroccan nationality, was a member of the Muslim faith whose personal information had been included in the data screening operation.[95] North Rhine-Westphalia Police Statute Section 31 provided the authorization for the challenged activity.[96] As in numerous other German states, the critical statutory language allowed data screening when "necessary to defend against a present danger (*gegenwärtige Gefahr*) to the existence or the security of the federation or a state, or the body, life, or freedom of a person."[97] After losing his case before two lower courts, the plaintiff brought his claim to the Constitutional Court. The Constitutional Court found that the lower courts, in upholding this data screening operation, had interpreted the statute in a fashion that violated his constitutional right to informational self-determination.[98]

1. The Right to Informational Self-Determination

The right of informational self-determination is a special part of the German constitution's general right of personality, which is based on the Basic Law's Article 2(1) and Article 1(1).[99] The general right of personality, as the Constitutional Court noted in its *Data Screening* opinion, "is a gap-filling guarantee" that "is especially required against the background of novel dangers for the development of personality that appear in accompaniment to the progress of science and technology."[100] In response to such changes, the Constitutional Court has developed new, substantive elements of the right of personality. From the general right, the Constitutional Court has identified further individual interests, including a right

95. *Id.* para. 56, at 337.

96. *See supra* note 77.

97. *Id.*

98. 115 BVERFGE 320 (341-66).

99. *See* GRUNDGESETZ FÜR DIE BUNDESREPUBLIK DEUTSCHLAND [GG] [BASIC LAW FOR THE FEDERAL REPUBLIC OF GERMANY], 1 BUNDESGESETZBLATT [BGBL.I] 1 (1949).

100. 115 BVERFGE 320 (341-66). The Court had also made this point in an earlier decision. BVerfG Dec. 15, 1999, 101 BVERFGE 361 (380).

to a private sphere in which one is to be free to shape her life,[101] a right to one's spoken word,[102] and, of particular relevance in the *Data Screening* case, a right to informational self-determination.[103]

For the Constitutional Court, the data screening operation, like its earlier *Census* case,[104] raised issues concerning the threat of modern means of surveillance to an individual's underlying communicative ability. The concern was with a person "who is unable with sufficient security to assess the knowledge of information that concerns him in certain sectors of his social environment, who cannot to some extent estimate the knowledge of possible communication partners."[105] Electronic data processing systems raised special dangers in this regard: "At any time and regardless of physical distance, these data can subsequently not only be called up in seconds, but, moreover and above all, can be combined with other data collections through the construction of integrated information systems, which develops the possibility for multiple uses and connections."[106]

The right of informational self-determination protects the individual against such new technological threats. It safeguards the general ability to decide "when and within which borders, personal life facts are revealed."[107] At the same time, however, the right of informational self-determination does not create a right of absolute control over personal data. In 1983, in the *Census* decision, the Constitutional Court had already stated, "The individual does not have a right in the sense of an absolute mastery over 'his' data; he is rather a personality that develops within a social community and is dependent upon communication."[108] Information relating to a person, as the court observed in that case, depicts "an image of social reality that the affected party cannot exclusively coordinate."[109]

---

101. BVerfG Jan. 16, 1957, 6 BVERFGE 32.

102. BVerfG Jan. 31, 1973, 34 BVERFGE 238.

103. BVerfG Dec. 15, 1963, 65 BVERFGE 1.

104. *Id.*

105. 115 BVERFGE 320 (para. 69, at 341). The Court noted the danger that this person "can be fundamentally obstructed in planning or decision making based on his individual self-determination." *Id.*

106. *Id.* para. 70, at 342.

107. *Id.* para. 69, at 341.

108. 65 BVERFGE 1 (43-44).

109. *Id.*

The court repeated similar concerns in its *Data Screening* opinion. For example, it stated, "The fundamental right of informational self-determination is not guaranteed without limits. Rather, the individual must accept such limitations of his right that are justified by weightier public interests."[110]

2. Proportionality Review and the Failure of the Lower Courts

Thus, German constitutional law permits limits on the right of informational self-determination when there is some more significant public purpose. Yet constitutional law also obliges the lawmaker to express such limits on the right in a statute that meets the constitutional principle of proportionality. The established three-part test for proportionality requires the state to follow a legitimate goal with means that are (1) suitable, (2) necessary, and (3) proportionate in the narrow sense.[111] The third part of the test requires a choice of means that are commensurate with the benefits.[112] The Constitutional Court has employed this measure of judicial review frequently and in a variety of settings, which meant it had a well-developed jurisprudence upon which to draw in its *Data Screening* opinion.[113] Its proportionality review led, in turn, to the case's key holding, which is that a data screening statute is constitutionally permissible only when there is "a concrete danger" to a legal interest.[114]

---

110. 115 BVERFGE 320 (para. 81, at 344-45). In the *Census* decision itself, the Constitutional Court made this point at the same time as it identified the right of informational self-determination. 65 BVERFGE 1 (43-44). In fact, Hans-Peter Bull argues that the Constitutional Court has lost track of this part of its vision and has turned the right of informational self-determination into a more purely individualistic interest. In doing so, it ignores the role that security, personal and shared, plays in freedom. HANS-PETER BULL, INFORMATIONELLE SELBSTBESTIMMUNG—VISION ODER ILLUSION? (2009) (Ger.).

111. 115 BVERFGE 320 (para. 82, at 345).

112. *Id.* para. 88, at 345.

113. *See, e.g.*, BVerfG Jul. 18, 1973, 35 BVERFGE 382 (para. 63, at 400-01); BVerfG Mar. 5, 1968, 23 BVERFGE 127 (para. 19, at 133-34).

114. 115 BVERFGE 320 (para. 133-53, at 360-67); *see also* BVerfG Mar. 2, 2010, 125 BVERFGE 260 (para. 231, at 330) (telecommunications data retention); BVerfG Feb. 27, 2008, 120 BVERFGE 274 (para. 233-35, at 328-29) (online surveillance). Although Daniel Solove does not discuss the German cases in his scholarship, his most recent book advocates a similar approach. Solove indicates acceptance of data mining only "when there's a specific threat and specific information about the likely perpetrators." DANIEL J. SOLOVE, NOTHING TO HIDE 195

It would be useful at this juncture to provide a roadmap of the Court's path to its holding. It first considered the extent to which data screening represented a grave violation of an individual right. Drawing on examples from constitutional decisions about telecommunications surveillance and other areas of law, the Constitutional Court found that data screening represented a weighty invasion of the right of informational self-determination.[115] Nonetheless, it decided that this procedure was not per se disproportionate and, hence, not facially unconstitutional.[116] Yet before law enforcement officials could use this procedure, they had to demonstrate a concrete danger.[117] Finally, the Constitutional Court decided that although a constitutional application of the contested statute was possible, the lower courts in North Rhine-Westphalia had not interpreted it in the required fashion and held the state to the correct standard.[118]

Under proportionality review, an assessment of the permissibility of an invasion of a constitutional right begins with an assessment of the significance, or weight, of the harm to the interest.[119] A heavy interference with the right of informational self-determination would require, in turn, an equally serious justification, or it would be disproportionate. The Constitutional Court identified multiple reasons why the invasion of the right was highly significant, and, as we shall see, this very multiplicity of grounds led Justice Haas, in dissent, to express skepticism at an explanation that was too complicated for her taste. We remain for the time being, however, with the majority.

For the Constitutional Court, the first impact of the data screening was through its scrutiny of information about which

---

(2011).

115. *See, e.g.*, BVerfG July 27, 2005, 113 BVERFGE 348 (para. 139-46, at 382-84). In this case, the Constitutional Court held that a state law allowing preventive telecommunication surveillance (*vorbeugende Telefonüberwachung*) violated the privacy of telecommunications. It regarded the invasion as weighty because of its possibility of screening communication patterns, its great breadth (*große Streubreite*), and the lack of knowledge of the person concerned.

116. 115 BVERFGE 320 (para. 125, at 357).

117. *Id.* para. 158, at 368.

118. *Id.* para. 158-61, at 368-70.

119. *Id.* para. 136, at 360.

individuals had "an expectation of confidentiality."[120] The statute in North Rhine-Westphalia was broadly drafted to permit access to all "data necessary for the individual case."[121] This language proved extremely significant later in the opinion, as both constitutional and unconstitutional readings of it were possible. At this point in its opinion, however, the Court was interested in the language because of its sweep. According to it, the statute permitted access to such personal data in which the individual "possesses a high interest and on whose confidentiality he relies," including data about religious beliefs.[122]

There were additional reasons that the data screening had a significant impact on informational self-determination. As the Constitutional Court discussed, data screening created a dangerous potential for the "warehousing of personal data" and the creation of "personality profiles."[123] It would subject certain persons to further official investigations and stigmatize those persons whose information was swept up in the search. It was also carried out in secret, which increased its intensity for the individual.[124] Any legal protections for the individual would take effect only once the data screening was completed.[125] Finally, the data searches invaded a fundamental right without suspicion and in a manner of "great breadth" (*große Streubreite*).[126] Regarding the reach of the invasion, the Constitutional Court observed that the personal data of some 5.2 million people were involved and that the nature of data screening permitted the processing of "larger and more complex databases with greater speed and nearly at will."[127]

---

120. *Id.* para. 99, at 348.

121. *Id.* para. 101, at 349.

122. *Id.*

123. *Id.* para. 106, at 351; *see also* 113 BVERFGE 348 (para. 140, at 382-83) (preventive telecommunication surveillance); 120 BVERFGE 274 (para. 214, at 323) (online surveillance); 125 BVERFGE 260 (para. 211, at 319) (telecommunications data retention).

124. 115 BVERFGE 320 (para. 114, at 353).

125. *Id.*

126. *Id.* para. 116, at 354; *see also* 120 BVERFGE 274 (para. 143, at 323); 113 BVERFGE 348 (para. 142, at 383).

127. 115 BVERFGE 320 (para. 122. at 356). It also drew a contrast with "strategic surveillance" by the BND, with references to its case law in that area, and noted that the purpose of data screening was, from its start, to lead to investigations of specific individuals. *Id.* para. 139, at 362.

Despite the weightiness of the invasion of the right of informational self-determination, the Constitutional Court was unwilling to find data screening to be per se unconstitutional. As Dirk Heckmann summarized in his analysis of the opinion, "The constitutionality of data screening as such was not questioned."[128] Rather, the analysis concentrated on the conditions under which a preventive data screening could pass constitutional muster. The Court's lesson from its proportionality jurisprudence was that the legislature could permit a weighty invasion of a fundamental right only when a certain risk of danger had been reached. More specifically, when an action was to be taken "in advance" (*im Vorfeld*) of the harm, the Basic Law required the legislature to be concerned with the *probability* of the danger actually occurring.[129] The Constitutional Court also announced rules for the use of a "lasting danger" (*Dauergefahr*) as justification for data screening.[130]

In the absence of a concrete danger, data screening was constitutionally problematic.[131] As a result, the court reached a key part of its holding and required "a state of affairs, under which in the actual case there is a sufficient probability of a damage ... in the near future (*absehbarer Zeit*)."[132] Beyond such an "establishment of concrete dangers," the court also required a "prognosis of probability" based on facts that the predicted harm would occur.[133] The court added, "Vague clues or bare suppositions are not sufficient."[134]

A lasting threat could also constitute a concrete danger and justify data screening. Yet, the court cautioned, "Foreign political areas of tension that terrorists could use as an occasion for attacks

128. Dirk Heckmann, *Präventive polizeiliche Rasterfahndung*, jurisPR-ITR (6/2006).

129. 115 BVERFGE 320 (para. 140, at 361); *see also* 113 BVERFGE 348 (para. 151, at 386); 120 BVERFGE 274 (para. 227, at 327) ("The required probability and facts of the prediction have to be proportionate to the type and weightiness of the intrusion of the basic right. Even in the case of threatening severe intrusions to basic rights, the requirement of an adequate probability of occurrence (*hinreichende Eintrittswahrscheinlichkeit*) is indispensable.").

130. 115 BVERFGE 320 (para. 147, at 364).

131. *Id.* para. 138, at 362. Here, the Constitutional Court repeated many of its earlier arguments, or variations of them, about the heavy impact of data screening. For example, the procedure would sweep in many people, and without specific suspicion about each person. It also had a broad reach, and it could seize personal information with "an intensive reference to personality." *Id.*

132. *Id.* para. 144, at 364.

133. *Id.*

134. *Id.* para. 145, at 364.

always exist," and this state of affairs "can last a long time."[135] As a result, the Constitutional Court concluded:

> As a practical manner, it is never out of the question that terrorist actions can hit Germany or can be prepared there. A general threat situation, which has existed practically without a break since September 11, 2001, that is for more than four years now, or foreign tensions are not sufficient for the ordering of data screening.[136]

Due to its impact on the right of informational self-determination, the use of data screening required proof of actual preparations for a terrorist attack. The Court stated a requirement of "[t]he submission of further facts that would prove a concrete danger, perhaps through factual clues for the preparation of terroristic attacks or the presence in Germany of persons who are preparing terrorist attacks that in the near future will be perpetrated in Germany or elsewhere."[137]

At this point, the Constitutional Court had articulated a full set of constitutional requirements for the use of data screening under the proportionate standard of judicial review. It could now turn to the final question, which was the constitutional permissibility of the contested statute in North Rhine-Westphalia. In the constitutional law of Germany, as in the United States, there is an established doctrine that requires courts to interpret statutes, when alternative readings are possible, in conformity with the constitution.[138] A constitutionally permissible reading of the statute turned on a processing of data under the conditions of a "present danger" and access to only such data that were "necessary for the individual case." The Constitutional Court found that the statute would achieve "constitutionally sufficient certainty" when interpreted as requiring a concrete threat level, not merely "a general danger of

135. *Id.* para. 147, at 364.

136. *Id.* para. 147, at 364-65.

137. *Id.*

138. In the United States, Justice Louis Brandeis articulated this principle of judicial self-restraint in *Ashwander v. Tennessee Valley Authority*, 297 U.S. 288, 348 (1936). For a discussion of a similar doctrine in Germany, see DONALD KOMMERS, THE CONSTITUTIONAL JURISPRUDENCE OF THE FEDERAL REPUBLIC OF GERMANY 50-51 (2d ed. 1997).

terrorism," before permitting data screening.[139] In other words, the Constitutional Court read a requirement of "concrete danger" into the concept of "necessary for the individual case." Only when such a risk existed could the data screening be viewed as necessary.

The Court had reached the final step in its opinion. It declared that the lower courts had failed to interpret the statute in the fashion that the Basic Law required. For example, the Higher Regional Court had upheld the data screening with the argument that "the possibility of an especially grave occurrence of danger could not be excluded."[140] Yet it was not enough to identify the size of the damage that terrorism could cause; it was also necessary to evaluate the probability of the success of the measure that was used to defend against this harm. The Constitutional Court pointed to the need for "sufficiently concrete facts" that showed "in some way a probability of a preparation of terrorists attacks by persons, who could have been classified as terroristic 'sleepers' and, correspondingly, who could have been found through the data screening."[141]

C. The Dissent

In dissent, Justice Haas disagreed with the part of the majority opinion that found that the opinions of the lower court were unconstitutional.[142] For Justice Haas, moreover, there was a different path than the majority's to find the North Rhine-Westphalia statute to be constitutional. There was no need to read a "concrete danger" requirement into the statute; rather, it should have been upheld because of the constitutional obligation on the state to protect freedom, and, hence, security.[143]

Justice Haas first disagreed with the majority in her view that the data screening at stake in the case did not represent an especially onerous burden on any personal interest.[144] Beyond this point, she also pointed out that the majority had ignored strong constitu-

---

139. 115 BVERFGE 320 (para. 151, at 366).

140. Oberlandesgericht [OLG] Düsseldorf [Higher, Regional Court] Feb. 8, 2002, 3 WX 356/01 (para. 17) (unpublished).

141. 115 BVERFGE 320 (para. 160, at 369).

142. *Id.* para. 181, at 379 (Haas, J., dissenting).

143. *Id.* para. 182-84, at 380-81.

144. *Id.* para. 169-172, at 371-74.

tional interests furthered by the data comparison. In her view, the state's action "secured and furthered the freedom of the individual who was affected by the data comparison."[145] Statutes expanding the authority of government to engage in surveillance in Germany have been frequently justified by an appeal to the requirements of domestic security.[146] Her dissent in the *Data Screening* opinion sought to build these arguments into a doctrine of constitutional politics. She stated: "The fundamental right to freedom requires the guaranteeing of security by the State.... Security is the fundamental basis on which freedom can fully develop itself."[147] The true intimidation effect was created, Justice Haas added, not through a minor invasion of privacy by data screening, but through a "fear of people for their life and health" created by the threat of terrorism.[148]

From the centrality of this right to "freedom from fear," the dissent turned to four consequences of the law enforcement activity before the Constitutional Court. First, data screening was a complicated process that "required significant time until its conclusion."[149] In the case before the court, for example, the data screening operation took twenty months.[150] Such a "time-consuming type" of police activity simply could not be carried out within the framework of a "concrete" danger and a probability analysis.[151]

Second, a proportionality analysis should be based on the size of the possible damage. As Justice Haas summarized when stating her understanding of police law, "The greater the feared damage, the lower the requirements regarding the probability of the beginning of the harm to permit the police to become active."[152] In this context, it was important to remember that terrorists had already engaged in threats and also deeds with "consequences of a never-before experienced dimension (New York, London, Madrid) and more can

145. *Id.* para. 174, at 374.

146. For example, STPO, BGBL. I 1074, § 98a was codified in order to pursue drug trafficking and other organized crimes. *Id.* para. 4, at 321-22 (majority opinion).

147. *Id.* para. 174, at 374 (Haas, J., dissenting); *see also* 125 BVERFGE 260 (para. 315-36, at 367-80) (Schluckebier, J., dissenting).

148. 115 BVERFGE 320 (para. 175, at 375) (Haas, J., dissenting).

149. *Id.* para. 178, at 377.

150. *Id.*

151. *Id.*

152. *Id.* para. 179, at 378.

take place."[153] The need was to allow the police to develop their investigations in a "temporal corridor" before "the danger could occur or be directly imminent."[154]

Third, as the Higher Regional Court had emphasized, there were "actual leads that affirmed a terrorist threat, which justified the carrying out of the data screening."[155] Justice Haas noted that two of the participants in the attacks on September 11, 2001, in the United States had their residence in North Rhine-Westphalia and that the police also were aware of forty-two other contact persons or supporters of Osama bin Laden who were present in that German state.[156] Moreover, as a member of NATO, Germany had a responsibility to support the alliance's duty of collective self-defense and engage in measures against terrorism.[157] As a final matter, Justice Haas pointed to the judiciary's obligation to respect the division of power among the branches and to leave adequate decision-making authority in this area to the legislative branch.[158] The Basic Law assigned authority to the legislature to react to new situations and to provide "precautionary measures against risk."[159] Using the English term in parentheses, Haas concluded by discussing the need both for "*richterliche Zurückhaltung* ('judicial self-restraint')" and for respect for the "generative possibilities" of the democratically legitimized legislature.[160]

III. NEW TECHNOLOGY AND A TALE OF TWO CONSTITUTIONAL COURTS

In this final Part, I wish to contrast the intensive confrontation with new technology by the German Constitutional Court with the lack of a similar engagement by the U.S. Supreme Court. I will also

153. *Id.* para. 177, at 376.

154. *Id.*

155. *Id.* para. 181, at 379.

156. *Id.* Justice Haas also pointed out the majority opinion's failure to mention these links between North Rhine-Westphalia and these terrorists. *Id.*

157. *Id.*

158. For a law review article agreeing with this point, see Winfried Bausback, *Fesseln für die Wehrhafte Demokratie?*, 59 NEUE JURISTISCHE WOCHENSCHRIFT [NJW] 1922, 1922-23 (2006) (Ger.).

159. 115 BVERFGE 320 (para. 184, at 380) (Haas, J., dissenting).

160. *Id.* para. 184, at 380-81; *see also* 125 BVERFGE 260 (para. 326, at 373) (Schluckebier, J., dissenting).

link the German court's decision-making techniques to elements of a "new constitutionalism" in post-war Europe. I will follow this institutional analysis with a discussion of the differences between German and American approaches to informational privacy.

A. New Technology and the "New Constitutionalism" of Europe

The contrast could not be starker between the Federal Constitutional Court's significant involvement in regulating the government's data mining and the U.S. Supreme Court's hands-off approach. The Constitutional Court engaged in a careful analysis of the contested statute in its *Data Screening* case, evaluated the interpretation of the statute by lower courts, and developed a series of constitutional norms for use in this area. It even discussed the wide-reaching implications of its decision for other state statutes that regulated data screening.[161] The Constitutional Court also has demonstrated a similar level of significant involvement regarding law enforcement's collection and processing of information in other major decisions. These include a series of opinions regarding preventive telecommunications surveillance,[162] online surveillance,[163] and data retention.[164]

As this Article has also shown, by the 1970s, the U.S. Supreme Court developed a Fourth Amendment jurisprudence that has kept the judiciary on the sidelines concerning data mining. There is no American equivalent of the *Data Screening* opinion, and the conceptual space for such a decision does not exist so long as *Miller* and *Smith* stand. The differences in this respect clearly demonstrate the phenomenon of the rise of constitutional law within post-war Europe and the key role that specialized constitutional courts play in these legal systems. We can sketch three initial aspects of the constitutional law of Europe in the post-World War II period.

First, post-war constitutions are typically far more extensive and specific than a founding document from the eighteenth century,

---

161. For the clearest overview of the different measures of the statute data screening laws, see STEFAN MIDDEL, INNERE SICHERHEIT UND PRÄVENTIVE TERRORISMUSBEKÄMPFUNG 124-34 (2007) (Ger.).

162. 113 BVERFGE 348 (preventive telecommunications surveillance).

163. 120 BVERFGE 274 (online surveillance).

164. 125 BVERFGE 260 (telecommunications data retention).

such as the U.S. Constitution. As of April 2011, the German Constitution consists of 146 separate articles, which incorporate all post-1949 amendments, and uses 24,132 words.[165] In contrast, the U.S. Constitution consists of 7 articles and 27 amendments and uses 7622 words.[166]

Second, post-war E.U. constitutions typically contain more detailed rights provisions than the U.S. Constitution.[167] These interests are structured as both negative and positive rights. Negative constitutional rights, such as are found in the United States, only prevent the state from engaging in certain actions. Positive constitutional rights require the state to take certain positive, protective actions.[168] For the purpose of this Article, the most important such positive rights in Germany are the general right of personality and its sub-category, the right of informational self-determination.

Third, the post-war constitutions of Europe typically assign a central role in developing the higher law to a constitutional court that is separate from the rest of the court system. These specialized courts are assigned the task of being the final arbiter of all constitutional issues. In the analysis of Alec Stone Sweet, the European model of constitutional review has led to a "new constitutionalism."[169] In Germany, this new constitutionalism is demonstrated by the Constitutional Court's strong engagement in developing and shaping constitutional norms to respond to the threat of technological developments to civil liberties.

Sweet has drawn a clear picture of these powerful courts. In his description, the new constitutional courts "have links with, but are formally detached from, the judiciary and legislature."[170] This institution occupies its "own 'constitutional' space, a space neither clearly 'judicial' nor 'political.'"[171] Unlike the U.S. Supreme Court, these new higher law courts do not decide general legal matters as a court of last resort. Rather, their exclusive focus is on constitu-

165. *See supra* note 99, as last revised by article 1 of the law of July 21, 2010, 38 BUNDESGESETZBLATT [BGBL.I] 944.

166. *See* U.S. CONST.

167. For an illustrative table of "rights and responsibilities in European constitutions," see ALEC STONE SWEET, GOVERNING WITH JUDGES 42-43 tbl.2.1 (2000).

168. For a discussion, see KOMMERS, *supra* note 138, at 30-40.

169. SWEET, *supra* note 167, at 37.

170. *Id.* at 34.

171. *Id.*

tional matters—with decision making possible even without a "case or controversy" in the American sense.[172] These courts act as "specialized legislative organs."[173] The result has been, as Sweet observes, a shift in power to courts that have developed wide discretionary powers and have "judicialized" and "constitutionalized" policy areas.[174]

The *Data Screening* opinion contains all the hallmarks of the new constitutionalism that Sweet identifies. The Constitutional Court infused an area involving complex technology with its own interpretation and development of constitutional norms. As Sweet observes, these courts typically view "certain constitutional provisions as open-ended invitations to generate 'new' unenumerated rights."[175] Thus, the court's identification of the right of informational self-determination followed from its open-ended view of the general right of personality. In fact, two years after its *Data Screening* opinion, the Constitutional Court returned again to the right of personality and articulated a new right in its *Online Surveillance* decision: the right to "trust and integrity in information systems."[176]

In its *Data Screening* opinion, the Constitutional Court acted, moreover, through a technique that Sweet finds typical for such courts: a proportionality analysis.[177] Such techniques are highly indeterminate, which allow constitutional courts to weigh a broad set of factors and to leave options open for future decisions. Sweet also identifies a "principal-agent" strategy that these courts use based on courts that permit other governmental branches a "partial victory," but that also requires them to make changes in statutes or regulations.[178] The result is to infuse ever greater areas of law and policy with constitutional law. In its *Data Screening* opinion, the Constitutional Court favored just such a use of the "partial victory" as a savvy "principal" seeking to enlist "agents." It did not invalidate

172. *Id.*
173. *Id.* at 61.
174. *Id.* at 194-203.
175. *Id.* at 98-99.
176. 120 BVERFGE 274 (para. 166, at 302). For contrasting opinions of this decision, compare Oliver Lepsius, *Das Computer-Grundrecht*, *in* ONLINE-DURCHSUCHUNGEN 21, 52-54 (Fredrik Roggan ed., 2008) (skeptical), with Alexander Dix, *Neue Perspektiven für den Schutz Personenbezogener Daten?*, *in* ONLINE-DURCHSUCHUNGEN, *supra*, at 71 (positive).
177. SWEET, *supra* note 167, at 117, 142.
178. *Id.* at 88-90, 117.

the statute at hand, that of North Rhine-Westphalia, but faulted the decision of the lower courts that had interpreted it.[179] The Court also mentioned how its decision cast doubts on the validity of how other data screening statutes were applied.[180] But state legislatures and other courts were left the task of determining the precise application of the *Data Screening* decision to these laws.

As for the dissent, it found that the majority went too far in failing to defer to the legislative branch to make decisions about the use of data screening. Justice Haas did so on grounds regarding democratic legitimacy. Absent from the dissent was any language about need for deference to the police or other experts to gauge the efficacy of technology and techniques in maintaining public security. Indeed, even in the United States, where justices and judges sometimes defer to the expertise of law enforcement or national security experts, they tend to do so silently, or through rulings that serve to permit these officials flexibility.[181]

Finally, the Constitutional Court was equally confident in the strength of the democratic order in Germany and its capacity for survival. Despite the danger of terrorism, it viewed its commitment to the rule of law to be as necessary as it had ever been. In a long series of decisions, the German Constitutional Court developed the concept of a "militant democracy."[182] The constitutional order is entitled to defend itself against those who would attempt to destroy it.[183] Yet, as the Constitutional Court stressed, a militant democracy is permitted to use only measures consistent with the rule of law.[184] In reference to the danger from terrorism, the Constitutional Court stated in the *Data Screening* case: "The state may and must effectively confront terroristic efforts ... with necessary and constitu-

179. 115 BVERFGE 320 (para. 66-67, at 341).

180. *Id.* para. 157, at 367-68.

181. *See, e.g.*, Florida v. Riley, 488 U.S. 445 (1989) (permitting law enforcement to fly over private property without a search warrant when private flights are permitted and "there is no indication that such flights are unheard of" in the relevant location); *In re* Sealed Case, 310 F.3d 717, 746 (FISA Ct. Rev. 2002) (upholding USA PATRIOT Act's amendment to FISA and noting both that the case "may involve the most serious threat our country faces" and even if "the procedures and government showings" that FISA requires "do not meet the minimum Fourth Amendment warrant standards," they "certainly come close").

182. KOMMERS, *supra* note 138, at 37-38.

183. *Id.* at 38.

184. 115 BVERFGE 320 (para. 126, at 357).

tional measures reflecting the rule of law."[185] According to the court, the government demonstrated "the power of the constitutional state by its being bound to generally valid fundamental principles in its relations with its enemies."[186] In an aside, the court added that "absolute security" was, at any rate, impossible, and the role of the government was simply to provide the "greatest possible security under the actual circumstances."[187]

B. Two Approaches to Informational Privacy

The preceding section addressed the question of two constitutional courts' approaches through an institutional perspective. The new constitutionalism of a court designed only to interpret a constitution has encouraged intense judicial involvement in developing constitutional norms for preventive data screening. In this Section, I wish to draw a further contrast regarding differences in substantive legal approaches to informational privacy.

In the view of James Whitman, there are stark differences between Europe and the United States regarding privacy.[188] Whitman argues that "on the two sides of the Atlantic, there are two different cultures of privacy, which are home to different intuitive sensibilities, and which have produced two significantly different laws of privacy."[189] Europeans are concerned with dignity, and Americans are concerned with liberty.[190] As a result of these divergent sensibilities, "[m]ost especially, state action will raise American hackles much more often than European ones."[191] In contrast, "[c]ontinental Europeans are consistently more drawn to problems touching on public dignity."[192]

---

185. *Id.* For an earlier case making the same point, see BVerfG Aug. 1, 1978, 49 BVERFGE 24 (56).

186. 115 BVERFGE 320 (127). For earlier cases making similar points, see BVerfG June 23, 2004, 111 BVERFGE 147 (158); BVerfG Sept. 5, 2003, 2 BVERFGE 1 (5); BVerfG May 1, 2001, NJW 2076 (2077), 2001.

187. 115 BVERFGE 320 (127).

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

189. *Id.* at 1160.

190. *Id.* at 1164.

191. *Id.* at 1162.

192. *Id.*

Although an examination of contemporary continental privacy law is beyond the scope of this Article, it is fair to state that German law does not support these distinctions. The *Data Screening* case, and other recent cases of the Constitutional Court, reveal a legal system that is, in fact, highly concerned about the government's use of personal data. Indeed, Whitman also finds Americans most concerned about privacy in the home, but, here, too, German constitutional law reveals a heightened sensibility.[193] There are special constitutional rules for the use of wiretaps in residences, and these safeguards also played a role in 2008 in the Constitutional Court's decision concerning online surveillance.[194]

Moreover, the approach in the United States, whether at the level of the U.S. Supreme Court or Congress, appears far less concerned about liberty than permitting law enforcement a wide zone of freedom in selecting the tools that it considers necessary to protect public security. As a legislative example of such deference, we can return to, and indeed expand, the earlier account of the congressional response to the NSA's warrantless wiretapping after 9/11 in the FISA Amendments Act of 2008 (FAA).[195]

The FAA does not explicitly address the question of data mining. Its language is general, but it does permit the government to respond to uncertainty about the location of a target by drawing on the capacities of data mining. The statute does so by permitting "targeting of persons reasonably believed to be outside the United States" when a "significant purpose" of the surveillance is to acquire foreign intelligence information.[196] The FAA removes FISA's requirement of a judicial determination concerning the identity and location of a specific "target of the surveillance." Rather, the judicial determination need only be that a *process* of surveillance is able to target "persons reasonably believed to be located outside the United States to acquire foreign intelligence information."[197]

Moreover, to the extent that the FAA indirectly provides for regulation of data mining, the process occurs outside of direct

193. *Id.*

194. BVerfG Feb. 27, 2008, 120 BVERFGE 274.

195. *See supra* text accompanying note 44.

196. FISA Amendments Act of 2008, Pub. L. No. 110-261, § 702(g)(2), 122 Stat. 2436, 2438 (codified as amended in scattered sections of 18 and 50 U.S.C.).

197. *Id.* § 702(a).

congressional oversight. The statute assigns the critical roles to the Attorney General and the FISC.[198] The Attorney General evaluates the NSA's processes for minimization and targeting, and the FISC provides a further check on these processes.[199] The Attorney General's minimization procedures under the FAA, regarding the targeting of persons outside the United States, must comply with FISA's existing requirements.[200] The FAA also requires the Department of Justice (DOJ) and the Director of National Intelligence to certify that targeting and minimization procedures meet the statutory standards and that "a significant purpose" of the surveillance is to acquire foreign intelligence information.[201] As for the FISC, it is required to review the targeting and minimization procedures that are adopted.[202] If a certification does not "contain[] all the required elements," or the procedures "are [not] consistent with the requirements" of the FAA, the FISC must issue an order directing the government to correct any deficiencies.[203]

This process is far from the kind of constitutionalization and judicialization that is a hallmark of the German response to similar situations. In the FAA, Congress has deferred to the executive branch by assigning a role to the DOJ and the Director of National Intelligence. It also crafts a role for the judiciary and, in particular, the FISC, which serves as the final check on whether the NSA is following the mandate of the statute. As concerns the Constitution, the FAA does instruct the FISC to review whether it comports with the Fourth Amendment.[204] This language appears to represent a last-ditch effort by those dubious of the statute to encourage the FISC to approach it with some skepticism. Yet the bait has not been taken; the FAA stands, and if there has been a FISC opinion about any of its aspects, the court has not made it public.[205]

198. *Id.* § 702(d), (e).

199. *Id.*

200. *Id.* § 702(e)(1). As the leading FISA treatise explains, the idea of minimization generally is that electronic surveillance pursuant to FISA be implemented to ensure conformity to its "authorized purpose and scope" and in a fashion that requires the government to collect the least amount of "irrelevant information." KRIS & WILSON, *supra* note 49, § 9:1.

201. FISA Amendments Act § 701(i).

202. *Id.*

203. *Id.*

204. *Id.*

205. There has been an opinion, however, upholding the Protect America Act, a stopgap

Thus, we may have two cultures of privacy, but one of the most important dividing lines concerns constitutional law. It is also worth noting that both approaches appear stable at present within their own countries. Despite occasional complaints from German legal scholars and politicians about too much law coming from the Federal Constitutional Court, this institution enjoys a high level of prestige and acceptance. A general shorthand for the Constitutional Court's important role in Germany is the expression, the "Karlsruhe Republic." This term refers to the city in which the Constitutional Court justices sit. In 1999, at the fiftieth anniversary of the founding of the Federal Republic of Germany, *Der Spiegel* magazine predicted that the "Karlsruhe Republic" had reached its apex, and that the unification of Germany meant that a "Berlin Republic" would diminish its influence.[206] That has been far from the case. In his keynote address at the Constitutional Court's fiftieth anniversary in 2001, Gerhard Casper noted its great ability to engage in a "continual definition of the polity with reference to essential constitutional principles ... in a manner that has earned it attention and respect worldwide."[207] Casper called his speech "*The 'Karlsruhe Republic.*"[208]

To the extent that there is a threat to the stability of the German model of constitutionalism, it comes from without rather than within. As a result of European integration, the German Constitutional Court faces a new kind of challenge to its authority through the development of important supranational institutions, including the European Commission and European Court of Justice.[209] The

---

measure enacted before the FAA. *See In re* Directives, 551 F.2d 1004 (FISA Ct. Rev. 2008) (stating that the Protect America Act represented a sufficiently reasonable exercise of governmental power to satisfy the Fourth Amendment). In other litigation, a federal district court upheld the FAA as constitutional, *In re* NSA Telecomm. Record Litig., 633 F. Supp. 2d 949 (N.D. Cal. 2008), but the Second Circuit found standing for plaintiffs and permitted a lawsuit alleging the unconstitutionality of the FAA to go forward. Amnesty Int'l USA v. Clapper, 683 F.3d 118 (2d Cir. 2011).

206. Thomas Darnstädt, *"Mir hat keiner was zu sagen": Die Allmacht des Bundesverfassungsgerichts*, DER SPIEGEL, May 17, 1999, at 206.

207. Gerhard Casper, *The "Karlsruhe Republic" - Keynote Address at the State Ceremony Celebrating the 50th Anniversary of the Federal Constitutional Court*, 2 GER. L.J. para. 15 (2001), *available at* http://www.germanlawjournal.com/index.php?pageID=11&artID=111.

208. *Id.*

209. SWEET, *supra* note 167, at 153-65. For a brief discussion of these institutions within the context of data protection law, see CHRISTOPHER KUNER, EUROPEAN DATA PROTECTION

European Community legal system now has its own set of fundamental rights and its own obligations for member states.[210] The German Constitutional Court must navigate the requirements of European constitutionalism and interpret new constraints on its authority.[211] In the data protection area, these decision-making loci and new rivalries for authority have been most evident in the ongoing debate about data retention.[212] In the United States, there is a similar kind of internal stability—and an absence of external pressures in the form of supranational institutions. To be sure, legal scholars have challenged the wisdom of the applicable constitutional law decisions, with *Miller* and *Smith* in particular disfavor.[213] The exception that proves the rules comes from Orin Kerr, who has generally defended the merits of the Supreme Court's approach to new surveillance technology.[214] Despite the general unease of the

---

LAW 1-41 (2d ed. 2007).

210. SWEET, *supra* note 167, at 153-61.

211. The German Constitutional Court executes its jurisdiction in a cooperative relationship with the European Court of Justice. BVerfG Oct. 12, 1993, 89 BVERFGE 155 (para. 70, at 175). As long as the European Court of Justice or other institutions of the European Communities provide effective protection in this regard, the Constitutional Court will refrain from exercising its jurisdiction over basic rights violations by acts of the European Community. BVerfG Oct. 22, 1986, 73 BVERFGE 339 (para. 132, at 387).

212. A European Directive from 2006 requires Member States to enact national data retention statues. Directive 2006/24/EC, of the European Parliament and of the Council of 15 March 2006 on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC, 2000 O.J. (L 105) 54-63. In 2010, the German Constitutional Court invalidated the relevant German legislation. BVerfG Mar. 2, 2010, 125 BVerfGE 260. Subsequently, and despite much debate, the German legislature has been unable to enact a new data retention statute. The EU is now threatening Germany with sanctions for failure to enact such legislation. *EU leitet Verfahren gegen Deutschland ein*, DIE WELT (GER.), June 22, 2011, http://www.welt.de/politik/deutschland/article13443492/EU-leitet-Verfahren-gegen-Deutschland-ein.html.

Finally, there may be a decision about the Data Retention Directive itself at the European Court of Justice. The Irish High Court has asked the European Court of Justice to decide whether the Data Retention Directive itself violates the European Charter of Human Rights. Ian Brown, *Communications Data Retention in an Evolving Internet*, 19 INT'L J.L. & INFO. TECH. 95, 96 (2011). In its own expert opinion, the German Parliament has already found that the Data Retention Directive does not meet the requirements of the European Charter of Human Rights. ROLAND DERKSEN, WISSENSCHAFTLICHE DIENST, [BT], WD 11-3000-18/11, AUSARBEITUNG: ZUR VEREINBARKEIT DER RICHTLINIE ÜBER DIE VORRATSSPEICHERUNG VON DATEN MIT DER EUROPÄISCHEN GRUNDRECHTECHARTA (2011).

213. *See, e.g.*, Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 WM. & MARY L. REV. 2105 (2009).

214. For his most recent efforts in this regard, see Orin Kerr, *An Equilibrium-Adjustment*

academy, however, the Supreme Court seems unlikely to revisit these decisions, and Congress seems unwilling to bolster informational privacy vis-à-vis the state through any strong, new protections.

This study will conclude with a brief account of a Supreme Court case from this term. In *NASA v. Nelson*, the Supreme Court granted certiorari on a case that might have permitted it to revisit its contested right of information privacy, which it first articulated in *Whalen v. Roe*, a decision from 1977.[215] This earlier opinion might have been used to bolster the Fourth Amendment privacy right but instead has largely receded from case law. In an 8-0 decision, the *Nelson* Court decided that it would neither praise nor bury *Whalen*.[216] Its decision was to bracket the question of the continuing validity of the right of information privacy; it stated its explicit assumption that "the Government's challenged inquiries implicate a privacy interest of constitutional significance."[217] It could do so because the governmental contractors in the case would lose regardless of whether such an interest existed.[218] In separate concurrences in this result, both Justice Scalia and Justice Thomas expressed their view that the Constitution lacked any right to informational privacy.[219] Given the approach in *Nelson*, the Supreme Court is not likely to develop its constitutional standards for informational privacy or apply the Fourth Amendment to those new technologies that involve information collection and processing.

This Article began by suggesting that the law in different countries sometimes will "see" different things when considering the same or similar phenomenon. Such a situation exists for the regulation of data mining in Germany and the United States. These distinctly different approaches point to one reason for the difficulties in reaching agreement on international data sharing accords.[220] The

---

Theory of the Fourth Amendment, 125 HARV. L. REV. (forthcoming 2011). For his earlier work, see Orin S. Kerr, *The Case for the Third Party Doctrine*, 107 MICH. L. REV. 561 (2009). For a skeptical response, see Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747 (2005).

215. NASA v. Nelson, 131 S. Ct. 746 (2011); Whalen v. Roe, 429 U.S. 589, 600 (1977).

216. *Nelson*, 131 S. Ct. at 746-57.

217. *Id.* at 756-57.

218. *Id.*

219. *Id.* at 764 (Scalia, J., concurring).

220. *See, e.g.*, Francesca Bignami, *supra* note 57, at 609 (explaining the illegality under

E.U.-U.S. negotiations on the transfer of aircraft passenger data is an example of such complex, multi-year negotiations.[221] Although such agreements have been reached, the different starting points for the two countries demonstrate the great obstacles that the necessary negotiations must surmount.

CONCLUSION

The legal systems in Germany and the United States respond in different ways to the use of data mining by the government for law enforcement and national security purposes. The German Federal Constitutional Court has set strict limits on the conditions for use of "data screening," the German term for this practice. Its focus has been on regulating the use of this technique in a "preventive" fashion, that is, before a crime has occurred. Among the limits that it identified in the Basic Law, the German constitution, the Constitutional Court has found data screening to be constitutional only if justified by the existence of a "concrete danger" for the security of the country, an individual state, or the life of a citizen.

In contrast, the U.S. Supreme Court has developed a Fourth Amendment jurisprudence that effectively forecloses the possibility of meaningful constitutional protections from governmental data mining. This result follows from long-established precedents, developed in the era before widespread use of computers. The Supreme Court appears unlikely to revisit its critical decisions, and at the statutory level, moreover, the law of criminal procedure in the United States simply does not consider data mining a "search." This Article concluded that these quite different approaches point to one underlying reason for the difficulty sometimes present in negotiating international data sharing accords.

E.U. law of data mining of databases in a fashion similar to that carried out by the NSA in the United States).

221. For a 2007 opinion of the Article 29 Working Party that sets out the background of this issue, see Article 29 Data Protection Working Party, *Opinion 5/2007 on the follow-up agreement between the European Union and the United States of America on the processing and transfer of passenger name record (PNR) data by air carriers to the United States Department of Homeland Security concluded in July 2007* (Aug. 17, 2007), *available at* http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2007/wp138_en.pdf.