DATABASES, E-DISCOVERY AND CRIMINAL LAW

By: Ken Strutin*

Cite as: Ken Strutin, *Databases, E-Discovery and Criminal Law*, 15 RICH. J.L. & TECH. 6, http://law.richmond.edu/jolt/v15i3/article6.pdf.

[1] The enduring value of the Constitution is the fundamental approach to human rights transcending time and technology. The modern complexity and variety of electronically stored information was unknown in the eighteenth century, but the elemental due process concepts forged then can be applied now. At some point, the accumulation of information surpassed the boundaries of living witnesses and paper records. The advent of computers and databases ushered in an entirely new order,[1] giving rise to massive libraries of factual details and powerful investigative tools. But electronically collected information sources are a double-edged sword. Their accuracy and reliability are critical issues in the hands of prosecutors and their accessibility a hard-won necessity in preparing a defense.

[2] This article examines the use of computer databases and electronic evidence from both standpoints. With limited guidance from federal and state criminal discovery rules, the courts have had to rely on constitutional principles and analogies to civil procedure when faced with database and

* Director of Legal Information Services, New York State Defenders Association. J.D., Temple University School of Law, 1984; M.L.S. St. John's University, 1994; B.A., summa cum laude, St. John's University, 1981.

[1] According to a study by the U.C. Berkeley School of Information Management and Systems, the sum of "new" information stored electronically doubled between 1999 and 2000, to five exabytes (five followed by 18 zeroes) or the equivalent of 500,000 Libraries of Congress. *See* Grant Gross, *Study Documents Data Boom: Data Storage Has Doubled During the Last Three Years*, INFOWORLD, Oct. 28, 2003, *available at* http: http://www.infoworld.com/article/03/10/28/HNstoragedoubles_1.html.

electronic document discovery requests.[2] A tension exists between the government's proprietary interest in preserving the sanctity of its databases and the right of the defense to assail the accuracy of the databases' output or to use them as investigative tools. As the gold standards of forensic science have come to be questioned,[3] so too the inviolability of government databases must be rethought.[4] And the defense's right to prepare its case and receive a fair trial makes it

[2] *See generally* Federal Judicial Center, Materials on Electronic Discovery: Civil Litigation, http://www.fjc.gov/public/home.nsf/autoframe?openform&url_l=/public/home.nsf/inavgeneral?openpage&url_r=/public/home.nsf/pages/196 (last visited Feb. 18, 2009) (providing several links, articles, presentations, and other items of interest on e-discovery); The Sedona Conference, http://www.thesedonaconference.org/content/faq (last visited Feb. 18, 2009) (stating that among the aims of this research and educational institute is the advancement of electronic document retention and production). To achieve these aims, the Sedona Conference specifically noted:

> Working Group 1 was formed in Spring of 2002 and issued a public comment version of *The Sedona Principles* addressing electronic document production in March of 2003 - a month later, the *Principles* were cited by the Federal Judicial Center's Civil Rules Advisory Committee Discovery Subcommittee as one of the reasons to focus on possible amendments to the Federal Rules of Civil Procedure in this area.

The Sedona Conference: What Have Working Groups Achieved so far in Contributing to the Advancement of Law and Policy, http://www.thesedonaconference.org/content/faq (last visited Feb. 18, 2009).

[3] *See generally* Simon Cole, *Grandfathering Evidence: Fingerprint Admissibility Rulings From Jennings to Llera Plaza and Back Again*, 41 AM. CRIM. L. REV. 1189 (2004) (arguing that forensic evidence has gained its legitimacy through legal acceptance rather than scientific validity); Adina Schwartz, *A Systemic Challenge to the Reliability and Admissibility of Firearms and Toolmark Identification*, 6 COLUM. SCI. & TECH. L. REV. 2 (2005) (arguing that scientific problems should render firearms and toolmark identification inadmissible in court); Ken Strutin, *Criminal Law Forensics: Century of Acceptance May Be Over*, N.Y. L.J., Jan. 8, 2008, at 5 ("The gold standards of forensic science are losing their luster.").

[4] Robert Garcia, *"Garbage In, Gospel Out": Criminal Discovery, Computer Reliability, and the Constitution*, 38 UCLA L. REV. 1043, 1073 (1991) ("Computerized information may be wrong, incomplete, or misleading due to mechanical failure, mistake, fraud, or bias. Ultimately, people are responsible for any errors, and there are infinite ways in which people can make mistakes, commit fraud or reflect bias. Broad discovery may be necessary to track down the reliability problems and evaluate the reliability of the computerized information.").

necessary to use database knowledge comparable to the prosecution. Much of this information is generated solely by the government or its experts. The civilian alternatives are prohibitively expensive, inadequate, or non-existent.[5] This review will highlight the problems created by disparities in resources and the role of constitutional and procedural remedies in the future development of criminal electronic discovery.

[3] The discussion is divided into several areas, beginning with an examination of the benefits of database discovery in criminal practice under Part I. Part II is an analysis of the small body of criminal electronic discovery cases involving databases and the rules that have been applied over the years. Parts III and IV analyze the constitutional foundations for defense access to government database tools under due process, compulsory process and the right to confrontation. Applications of these theories are illustrated through developments in DNA database discovery in Part V, which highlights challenges to the quality of data and the right to access DNA databanks for defense investigation. The issues that arise in challenging evidence derived from databases, particularly data relied on by experts, are discussed in Part VI. The ongoing problem of achieving defense parity with prosecution resources and the constitutional grounds for overcoming objections to disclosure or access to database information is considered in Part VII. Finally, the conclusion, Part VIII, considers the enormity of the task facing advocates as the criminal justice system, and society at large, come to terms with this next wave in the Information Revolution.

I. ELECTRONIC FOOTPRINTS

[4] A fact of modern life in the twenty-first century is the electronic footprint. Our choices and movements leave digital traces—the results of making life more convenient. These traces also impact the administration of justice in unforeseen ways.

[5] Facing a murder charge in federal court arising from the shooting death of a government witness in the Bronx, Jason Jones informed police

[5] *See, e.g.*, People v. Evans, 534 N.Y.S.2d 640, 643 (N.Y. Sup. Ct. 1988) (providing an example of why such alternatives are inadequate).

that he was innocent.[6] He claimed that at the time of the shooting he was riding the bus from his job at a manufacturing plant in Yonkers to cash his paycheck and then took the subway to visit his girlfriend.[7] It was a classic alibi defense, except for the witness, his MetroCard.[8]

[6] The card was still in his wallet when he was arrested.[9] Once his lawyer's investigator made use of it, the foundations of his innocence claim took shape.[10] The New York City Transit authority provided a report of Jones's movements on the bus and subway, miles away from the crime scene, based on the unique serial number from his MetroCard.[11] Along with a punch card from his job and his image captured on a surveillance camera when he went to cash his paycheck, the credibility of Jones's alibi defense supported reexamination of his bail status—eventually leading the prosecutors to agree to his release upon posting bond.[12]

[7] The city's database of transit records, along with the other documentation of Jones's activities that night, gave the defense an invaluable and nearly unimpeachable source of exculpatory evidence. It is only one example of the power that databases can have in the prosecution and defense of criminal cases.[13]

---

[6] *See* Benjamin Weiser, *Murder Suspect Has Witness that Doesn't Lie: A MetroCard*, N.Y. TIMES, Nov. 19, 2008, at A1.
[7] *Id.*
[8] The MetroCard is a payment system for travel on New York City buses and subways. Each card has a magnetic strip that records the amount of money or time remaining on the card. A centralized computer system stores data on where and when each card is used based on information it retrieves from buses and subway turnstiles. *Id.*
[9] *Id.*
[10] *Id.*
[11] *Id.*
[12] *See* United States v. Jones, 583 F. Supp. 2d 513, 514 (S.D.N.Y. 2008) ("The Government, after reviewing the Documentary Evidence, agreed to consent to a bail package for Jason Jones, and Magistrate Judge Katz approved the bail conditions on October 15, 2008.").
[13] *See, e.g.*, Madison Park, *E-ZPass Details Popping Up in Trials: Toll Records Leave Trail for Officers*, BALT. SUN, Aug. 31, 2007, at 1B:

> E-Z Pass [sic] was first used in New York in 1993, and today there are 9 million users who rang up more than 2 billion transactions in 2006, according to the E-ZPass Interagency Group, an Atlantic City, N.J.,

[8] In Jones's case the New York City Transit Authority complied with a defense request to supply a travel log of his movements.[14] As the decisional law shows, however, requests for access to government, and especially law enforcement databases, are often an uphill battle.

II. DATABASE DISCOVERY

[9] The constitutional underpinnings of criminal justice require the prosecution to produce reliable and material evidence of guilt beyond a reasonable doubt.[15] The accused has the rights to confrontation, cross-examination, and compulsory process.[16] Increasingly, both sides are looking toward nonhuman sources of information in preparing their cases. Databases in a raw sense are an extension of human memory and computational ability. It is only natural that they have become powerful and increasingly common witnesses in many prosecutions.

[10] Some of the largest government and private databases in the world have information directly relevant to the administration of justice. According to Business Intelligence Lowdown, Sprint, with over 53 million subscribers, "processes more than 365 million call detail records and operational measurements per day;" YouTube has more than 45 terabytes [trillion bytes] of videos; ChoicePoint harvested 250 terabytes of personal data on 250 million people; venerable AT&T has 323 terabytes of information and 1.9 trillion phone call records; and the U.S. Customs database contains "information on hundreds of thousands of people and objects entering and leaving the United States borders."[17]

> organization comprising 23 agencies in the 12 states where the system is in use.

Id.

[14] Weiser, *supra* note 6.

[15] *See In re* Winship, 397 U.S. 358, 364 (1970) ("Lest there remain any doubt about the constitutional stature of the reasonable-doubt standard, we explicitly hold that the Due Process Clause protects the accused against conviction except upon proof beyond a reasonable doubt of every fact necessary to constitute the crime with which he is charged.").

[16] U.S. CONST. amend. VI.

[17] Mini Singh, *Top 10 Largest Databases in the World*, BUS. INTELLIGENCE LOWDOWN, Feb. 15, 2007,

[11] Law enforcement databases go even further. There are forensic databanks of identifying information such as fingerprints, DNA and ballistics,[18] and more data collected by the IRS, SEC, DEA and other agencies.[19] An example of the direction in which these databanks are moving is the resource created to assist law enforcement in locating

---

http://www.businessintelligencelowdown.com/2007/02/top_10_largest_.html (last visited Feb. 17, 2009).

[18] *See, e.g.,* Robin Bowen & Jessica Schneider, *Forensic Databases: Paint, Shoe Prints, and Beyond*, 258 NAT'L INST. JUST. J., Oct. 2007, at 34, 38, *available at* http://www.ncjrs.gov/pdffiles1/nij/219603h.pdf (summarizing a study conducted by West Virginia University surveying government and private forensic databases used in law enforcement). It is important to observe their qualification of this research: "[t]he National Institute of Justice has not evaluated the utility, accuracy, or veracity of the data in these databases; no product approval or endorsement by the U.S. Department of Justice should be inferred." *Id.* at 38.

[19] *See* Garcia, *supra* note 4, at 1065.

> The government hopes to combine sophisticated information retrieval and expert systems with electronic databases, spy satellites and other technological marvels to fight drug trafficking, money laundering, tax evasion, and other crimes. The government has established a computerized financial crimes and money laundering control center that will integrate the databases of more than half a dozen federal and state agencies, including Customs, the Drug Enforcement Agency (DEA), the IRS, the Federal Reserve, and the State Department. The Counter Narcotics Center based at Central Intelligence Agency (CIA) headquarters, created in 1989, includes agents from the FBI, the DEA, the NSA, the Defense Department, the State Department, and the Coast Guard.

Id.; see also National Information Exchange Model (NIEM), http://www.niem.gov/ (last visited Feb. 17, 2009).

> NIEM, the National Information Exchange Model, is a partnership of the U.S. Department of Justice and the Department of Homeland Security. It is designed to develop, disseminate and support enterprise-wide information exchange standards and processes that can enable jurisdictions to effectively share critical information in emergency situations, as well as support the day-to-day operations of agencies throughout the nation.

Id.

cannabis cultivation by using geographic data systems and knowledge bases.[20]

[12] Computers in the 1960s had barely moved from vacuum tubes to solid-state circuitry when the first criminal prosecutions relying on this technology were brought.[21] Still, these machines were powerful enough to serve federal prosecutors at this early stage of modern computing and addressed discovery issues that remain unresolved.[22]

[13] In 1967, the defendants in *United States v. Dioguardi*[23] had been accused of fraudulently transferring and concealing property of a bankruptcy.[24] This case relied heavily on an analysis of sales figures, purchase orders, assets and inventories.[25] Government witnesses used a computer program to collect the data and compute their findings to support their theory of the case.[26] Although the U.S. attorney provided the defense with printouts of their calculations, the defense objected and asked for the actual program.[27] Despite arguments that the information constituted Jencks Act material[28] and the printouts were hearsay, the court denied the defense discovery motion.[29]

---

[20] *See, e.g., Finding the Marijuana Fields: A Computer Points the Finger*, N.Y. TIMES, Oct. 6, 1987, at A33
(discussing the early work of scientists at the United States Geological Survey and in the private sector who have developed a computer mapping program that uses data on "land ownership, distance from towns, transportation routes, water sources, natural vegetation, elevation, sunshine angle and slope of the land"). Information from this database would figure prominently in probable cause and suppression matters. *See id.*

[21] *See generally* Carol Iaciofano, *Computer Timeline*, in DIGITAL DELI 20, 26-27 (Steve Ditlea ed., 1984) (noting the prosecution of the first computer crime in 1964, and the first federal case in 1966).

[22] *See, e.g.*, United States v. Dioguardi, 428 F.2d 1033 (2d Cir. 1970).

[23] 428 F. 2d 1033 (2d Cir. 1970).

[24] *Id.* at 1034.

[25] *Id.* at 1037.

[26] *Id.*

[27] *Id.*

[28] *See* 18 U.S.C. § 3500(b) (2006):

> After a witness called by the United States has testified on direct examination, the court shall, on motion of the defendant, order the United States to produce any statement (as hereinafter defined) of the witness in the possession of the United States which relates to the

[14] On appeal, the United States Court of Appeals for the Second Circuit observed that there was a fundamental right to discovery underlying the defense request:

> We fully agree that the defendants were entitled to know what operations the computer had been instructed to perform and to have the precise instruction that had been given. It is quite incomprehensible that the prosecution should tender a witness to state the results of a computer's operations without having the program available for defense scrutiny and use on cross-examination if desired. We place the Government on the clearest possible notice of its obligation to do this and also of the great desirability of making the program and other materials needed for cross-examination of computer witnesses, such as flow-charts used in the preparation of programs, available to the defense a reasonable time before trial.[30]

[15] Nonetheless, the court affirmed the conviction.[31] Defense counsel failed to raise their[32] best grounds for relief until their reply brief on

---

> subject matter as to which the witness has testified. If the entire contents of any such statement relate to the subject matter of the testimony of the witness, the court shall order it to be delivered directly to the defendant for his examination and use.

Id.; *see also* Jencks v. United States, 353 U.S. 657, 672 (1957):

> [T]he criminal action must be dismissed when the Government, on the ground of privilege, elects not to comply with an order to produce, for the accused's inspection and for admission in evidence, relevant statements or reports in its possession of government witnesses touching the subject matter of their testimony at the trial. The burden is the Government's, not to be shifted to the trial judge, to decide whether the public prejudice of allowing the crime to go unpunished is greater than that attendant upon the possible disclosure of state secrets and other confidential information in the Government's possession.

Id. (citation omitted).
[29] *Dioguardi*, 428 F.2d at 1038.
[30] *Id.* at 1038.
[31] *Id.* at 1040.

appeal, i.e., testing the validity of the program and preparing for cross-examination of the witness.[33] In other words, they did not preserve the issue in the district court by specifying the grounds for their motion—instead they focused too much on their Jencks argument. Also, they were not prejudiced by the trial judge's decision to deny access. This was a case of punch cards versus adding machines. The calculations were simple, the data set limited and the computer's operations verifiable by tabulators or manually during the course of the trial or pending appeal. At the same time, defense counsel did not renew or clarify their motion or seek a subpoena for the information during the trial.[34]

[16] Forty years later, the data relied on in criminal prosecutions and the computing power needed to manage them can exceed a defendant's ability to realistically challenge the prosecution without adequate discovery.[35] Even when discovery is provided, the volume and nature of the response can be overwhelming and debilitating.[36] Today, computer discovery cannot be characterized as simple or limited. Data and documents are being produced in soaring and unmanageable numbers.[37] As a result, the risk of prejudice to the defense has grown proportionately.[38]

[17] Confronted with a lengthy indictment charging securities fraud, the defendants in *United State v. Ferguson*[39] filed a bill of particulars seeking specification of the false statements, false documents and fraudulent scheme at the heart of the case. [40] In accordance with Rule 16 of the Federal Rules of Criminal Procedure,[41] the prosecutors turned over 3.5

[32] Two individuals served as counsel for the defendant-appellants in this case. *Id.* at 1034.
[33] *Id.* at 1038.
[34] *Id.* at 1039.
[35] *See* George L. Paul & Jason R. Baron, *Information Inflation: Can the Legal System Adapt?*, 13 RICH. J.L. & TECH. 10, ¶¶ 4, 6 (2007).
[36] *See id.* ¶¶ 15-18 (providing an example of how discovery documents can become voluminous and unmanageable).
[37] *See id.* ¶¶ 9-10.
[38] *Id.* ¶ 23.
[39] 478 F. Supp. 2d 220 (D. Conn. 2007).
[40] *Id.* at 225.
[41] 18 U.S.C. Rule 16(a)(1)(E)-(F) (2006) (defining a defendant's right to seek access to or a copy of "books, papers, documents, data, photographs, tangible objects, buildings or places" and "results or reports of any physical or mental examination and of any

million pages of discovery "in the exact same electronically searchable format that the government is currently using."[42] When the defendants were arraigned, they received 1,350 pages of "hot documents," representing the most important information relevant to the allegations.[43]

[18] As in *Dioguardi*, prejudice was not found.[44] The government's response was sufficient to overcome the need to speculate about which materials might be relevant from millions of documents or unspecified allegations.[45] While denying the defendant's request for a bill of particulars, the court identified three important disclosure requirements: (1) a detailed accusatory instrument; (2) a full Rule 16 disclosure in an organized format, such as a searchable database; and (3) a list or identification of the "most relevant" documents.[46] These guidelines are a good starting point for measuring the responsiveness of the prosecution's discovery obligations. The next step involves search methodology.

[19] When an employee in the Department of State in Canada was indicted for allegedly accepting gifts in exchange for expediting visa applications from a business owner, STS Jewels, for his workers, a federal judge in the District of Columbia ordered the government to search its print and electronic files for responsive information.[47] The discovery order covered information about visa applications, requests for expedited interviews, and decisions.[48] The files were located in six different consulates in Canada and Mexico.[49]

[20] The scope of the search was justified by the defense's theory that STS applications were similar to other routine expedited requests granted

scientific test or experiment," among other things, that the government possesses, provided it meets the other statutory criteria).

[42] *Ferguson*, 478 F. Supp. 2d at 226.

[43] *Id.*

[44] *Id.* at 227; *see* United States v. Dioguardi, 428 F.2d 1033, 1038 (2d Cir. 1970).

[45] *See Ferguson*, 478 F. Supp. 2d at 227.

[46] *Id.* ("Given the degree of detail in the indictment and the government's provision of searchable discovery databases and a list of its key documents, the defendants have not proven that they require more particularization to adequately prepare their defenses, avoid prejudicial surprise at trial, and protect against future double jeopardy.").

[47] *See* United States v. O'Keefe, 537 F. Supp. 2d 14, 15-16, 24 (D.D.C. 2008).

[48] *Id.* at 16.

[49] *Id.*

without any incentives.[50] The defendants' request specified the methodology: "[F]or each location searched, defendants demand a comprehensive description of all of the sources that were searched (both paper and electronic), how each source was searched, and who conducted the search."[51] The search was designed to be thorough, beginning in electronic sources and extending back to archival print files.[52] It included "active servers" and "backup tapes," the parameters extended to "all email" and "stand-alone electronic documents" stored on "shared drives, personal drives and hard drives," and the search terms were "early or expedite* or appointment or early & interview or expedite* & interview."[53]

[21] The defendants objected to information produced in paper or electronically that did not identify the source or records keeper.[54] They requested that the government create an index for the hard copy documents indicating the custodian, job title, source, format (paper or electronic), and Bates number.[55] There was a gray area between print and computer files that made it impossible for the defense to make full use of the discovery or determine its completeness.[56]

[22] Without guidance from the Federal Rules of Criminal Procedure, the judge looked to Rule 34 of the Federal Rules of Civil Procedure for help.[57]

---

[50] *Id.*
[51] *Id.*
[52] *Id.*
[53] *Id.* at 17-18.
[54] *Id.* at 18.
[55] *Id.* Bates numbering, or Bates stamping, is used to place identifying numbers and/or date/time-marks on images and documents as they are scanned or processed (for example, during the discovery stage of preparations for trial). *Id.*; *see also* BLACK'S LAW DICTIONARY 161 (8th ed. 2004) (defining a Bates number as, "[t]he identifying number that is affixed to a document or to the individual pages of a document.").
[56] *See O'Keefe*, 537 F. Supp. 2d at 16-18.
[57] *See id.* at 18-19:

> In criminal cases, there is unfortunately no rule to which the courts can look for guidance in determining whether the production of documents by the government has been in a form or format that is appropriate. This may be because the "big paper" case is the exception rather than the rule in criminal cases.

In civil cases, Rule 34 has been applied over the years to carve out methods for the form and format of documents in high volume paper (and now electronic) cases.[58] It begins by requiring the producing party to turn over the records in the same manner as they were kept or categorized according to the discovery request:

> (E) *Producing the Documents or Electronically Stored Information.* Unless otherwise stipulated or ordered by the court, these procedures apply to producing documents or electronically stored information:
>
> > (i) A party must produce documents as they are kept in the usual course of business or must organize and label them to correspond to the categories in the request [59]

[23] The judge recognized that the Rule's purpose was to maintain "equality between the parties in their ability to search the documents."[60] To be usable, the files produced had to be searchable.[61] Moreover, their value as evidence depended on the defendants' ability to authenticate them.[62] Without knowing the author, custodian and source of the

---

Id.; *In re* Lees, 727 N.Y.S.2d 254, 254-57 (N.Y. App. Div. 2001) (stating defendant made an *ex parte* discovery request in rape case for access to complainant's and third party's computer for impeachment evidence granted under N.Y. Civil Practice Laws and Rules because no remedy existed under the Criminal Procedure law).

[58] *O'Keefe*, 537 F. Supp. 2d at 19:

> It is foolish to disregard them [the Federal Rules of Civil Procedure] merely because this is a criminal case, particularly where, as is the case here, it is far better to use these rules than to reinvent the wheel when the production of documents in criminal and civil cases raises the same problems.

Id.; *see* Floyd v. New York, No. 08 Civ. 1034, 2008 U.S. Dist. LEXIS 68798, at *1-2, *5-6, *14 (S.D.N.Y. Sept. 10, 2008) (stating that plaintiffs in class action suit against NYPD over an allegedly race-based stop and frisk policy sought court ordered disclosure of records in the police database under Rule 37 of the Federal Rules of Civil Procedure).

[59] FED. R. CIV. P. 34(b)(2)(E)(i).

[60] *O'Keefe*, 537 F. Supp. 2d at 19.

[61] *See id.* at 20.

[62] *Id.*

documents, electronic or paper, the defense could not meet the authentication requirements of Federal Rules of Evidence 901.[63] The magistrate judge took the step of recommending to the district court judge that all documents supplied by the government in response to the discovery request should be treated as authentic, avoiding the burdensome task of having the government certify everything under Rule 902(11).[64]

[24] The defense also challenged the thoroughness of the government's search methods in the following ways: "1) not interviewing the employees as to their use of electronic means as a form of communication regarding expedited reviews, 2) not having the employees search their own electronically stored information and 3) not indicating what software [the government] used to conduct the search or how it ascertained what search terms it would use."[65] The alleged failure of the prosecution to use forensic indexing tools, commonly relied on by law enforcement, could have hampered the completeness and accuracy of the search [66] by, for example, overlooking email stored in .pst files.[67]

---

[63] FED. R. EVID. 901 ("The requirement of authentication or identification as a condition precedent to admissibility is satisfied by evidence sufficient to support a finding that the matter in question is what its proponent claims."). The Notes of the Advisory Committee on Rules raised the problem peculiar to criminal cases, which did not have pretrial procedures for resolving this issue. "Today, such available procedures as requests to admit and pretrial conference afford the means of eliminating much of the need for authentication or identification. Also, significant inroads upon the traditional insistence on authentication and identification have been made by accepting as at least prima facie genuine items of the kind treated in Rule 902, *infra*. However, the need for suitable methods of proof still remains, since criminal cases pose their own obstacles to the use of preliminary procedures, unforeseen contingencies may arise, and cases of genuine controversy will still occur."). FED. R. EVID. 901 advisory committee's note.

[64] *O'Keefe*, 537 F. Supp. 2d at 20.

[65] *Id.* at 22 (emphasis added).

[66] *See, e.g.*, Amy Baron-Evans, *When the Government Seizes and Searches Your Client's Computer*, CHAMPION, June 2003, at 19-20, *available at* http://www.fjc.gov/public/pdf.nsf/lookup/ElecDi17.pdf/$file/ElecDi17.pdf (discussing the use of forensic software by law enforcement for searching computers).

[67] *See generally* About.com, PST (Personal Folders File), http://email.about.com/od/outlook/g/pst.htm (last visited Feb. 18, 2009) (defining .pst, which stands for Personal Storage Table, as a filename extension associated with Personal Folders files used with certain Microsoft products to store data locally). Personal Folders (.pst) files are used to store local copies of messages, calendar events, and other items within Microsoft, Microsoft Exchange Client, Windows Messaging, Microsoft Outlook, and Microsoft Outlook Express. *Id.*

[25] Lack of preservation or spoliation of evidence[68] might have been a legitimate concern, but no specific claims were made that would have borne out a due process violation.[69] Metadata[70] concerns, however, were also raised.[71] The files produced were in PDF[72] or TIFF[73] image formats, which can obscure hidden file information.[74] Only the native files contained the full metadata.[75] Rule 34 speaks to the method used by the producing party to normally store the files.[76] Since the request did not identify a particular format, the response was within the Rules:

> (ii) If a request does not specify a form for producing electronically stored information, a party must produce it in a form or forms in which it is ordinarily maintained or in a reasonably usable form or forms; and

---

[68] *See* United States v. Copeland, 321 F.3d 582, 597 (6th Cir. 2003) (defining spoliation as "the intentional destruction of evidence that is presumed to be unfavorable to the party responsible for its destruction" (citing BLACK'S LAW DICTIONARY 1437 (8th ed. 2004))); Zubulake v. UBS Warburg LLC, 220 F.R.D. 212, 216 (S.D.N.Y. 2003) (implying that the "failure to preserve property for another's use as evidence in pending or reasonably foreseeable litigation" is inherent in the definition of spoliation (quoting West v. Goodyear Tire & Rubber Co., 167 F.3d 776, 779 (2d Cir. 1999))).

[69] *O'Keefe*, 537 F. Supp. 2d at 22-23.

[70] Metadata is "information about a particular data set or document which describes how, when, and by whom the dataset or document was collected, created, accessed, or modified; its size; and how it is formatted. Some metadata, such as file dates and sizes, can easily be seen by users; other metadata can be hidden from users but are still available to the operating system or the program used to process the data set or document." Barbara J. Rothstein et al., *Managing Discovery of Electronic Information: A Pocket Guide for Judges*, FED. JUDICIAL CTR. 24-25 (2007), *available at* www.fjc.gov/public/pdf.nsf/lookup/eldscpkt.pdf/$file/eldscpkt.pdf. *See generally* SEDONA CONFERENCE, THE SEDONA GUIDELINES: BEST PRACTICE GUIDELINES & COMMENTARY FOR MANAGING INFORMATION & RECORDS IN THE ELECTRONIC AGE 28-29, 35 (2d ed. 2007) (explaining what metadata is, what it does, and how it may be useful).

[71] *O'Keefe*, 537 F. Supp. 2d at 23.

[72] Portable Document Format (PDF) is a file format created by Adobe Systems for document exchange, and it is used for representing two-dimensional documents in a manner independent of the application software, hardware, and operating system. Rothstein, *supra* note 70, at 25.

[73] Tagged Image File Format (abbreviated TIFF) is a file format for storing images, including photographs. Rothstein, *supra* note 70, at 13.

[74] *O'Keefe*, 537 F. Supp. 2d at 23.

[75] *Id.*

[76] *Id.*

> (iii) A party need not produce the same electronically stored information in more than one form.[77]

[26] The sufficiency of the government's response hinged on whether the files in an image format were "reasonably usable."[78] The magistrate judge admonished defendants to get a stipulation requiring the prosecution to preserve the files in their native format, and if the prosecution failed to agree, the magistrate judge suggested that the defendants seek a court order.[79]

[27] Lastly, the defendants criticized the search terms used to unearth the files.[80] The magistrate judge considered this issue of such complexity that he suggested a defense challenge to their sufficiency must satisfy the elements of Federal Rule of Evidence 702.[81]

[28] The use of proper search terms is probably one of the most difficult issues to litigate and solve. Searchers must have insight into the language and terms of art, as well as the factual background of the case, to even begin formulating the correct queries. Making a discovery request that captures the proper search terminology would be impossible without knowing the choice of vocabulary and syntax used by the government (or the creators of the documents or data). This may be an appropriate situation for seeking the input and assistance of a defense expert in

---

[77] FED. R. CIV. P. 34(b)(2)(E)(ii)-(iii).
[78] *O'Keefe*, 537 F. Supp. 2d at 23.
[79] *Id.* at 23.
[80] *Id.* at 23-24.
[81] *Id.* at 24; *see* FED. R. EVID. 702:

> If scientific, technical, or other specialized knowledge will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness qualified as an expert by knowledge, skill, experience, training, or education, may testify thereto in the form of an opinion or otherwise, if (1) the testimony is based upon sufficient facts or data, (2) the testimony is the product of reliable principles and methods, and (3) the witness has applied the principles and methods reliably to the facts of the case.

Id.

database searching.[82] As discussed in Part III, the defense should not have to rely on the prosecution's skill in ferreting out exculpatory or mitigating information from a government resource. No one but the defense can view evidence with an "advocate's eye."[83]

[29] In a money laundering case, an IRS agent testifying for the government prepared summaries and exhibits illustrating the contents of bank records.[84] The prosecution used a computer program to run searches laying the foundation for the spreadsheets and other exhibits they planned to use.[85] The defendants sought discovery of the financial database to assess the "accuracy, completeness, and fairness" of the exhibits and evidence.[86]

[30] Denying the motion, the district court concluded that the "source material" or "underlying data" were the actual bank records—available for examination for three years.[87] Giving the defense access to the prosecution database would reveal the search queries run by the agent, which the judge characterized as work product.[88] The court added that the defense was "equally as capable" as the agent of examining the bank records to determine if the summaries were accurate[89]—and of course, they would have an opportunity for cross-examination.[90]

---

[82] An expert in text searching (or a subject expert) can be drawn from any of several disciplines, such as information and computer science or linguistics. *See, e.g.*, Peter Tiersma & Lawrence M. Solan, *The Linguist on the Witness Stand: Forensic Linguistics in American Courts*, 78 LANGUAGE 221, 221 (2002), *available at* http://muse.jhu.edu/journals/language/v078/78.2solan.pdf (discussing the applications of linguistic expertise in civil and criminal cases and the courts' views on admissibility).

[83] *Cf.* Pennsylvania v. Ritchie, 480 U.S. 39, 60 (1987) (stating while the defendant may be denied the benefits of an "advocate's eye," partial disclosure is sufficient).

[84] United States v. Schmidt, No. 04-cr-00103-REB, 2007 U.S. Dist. LEXIS 30559, *1-2 (D. Colo. Apr. 25, 2007).

[85] *Id.* at *2.

[86] *Id.*

[87] *Id.* at *3.

[88] *Id.*

[89] *Id.* at *4. *But see* Portis v. City of Chicago, No. 02 C 3139, 2004 WL 1535854, at *1, *4-*5 (N.D. Ill. July 7, 2004) (discussing 42 U.S.C. § 1983 class action over custodial arrests for nonviolent ordinance violations, where the court granted the city's motion for disclosure of the plaintiffs database drawn from municipal arrest records: "Because the court finds that the City has a substantial need for access to the database and that the City could not obtain the substantial equivalent of the database without the undue hardship of

[31] The defense made a due process argument that the court rejected.[91] Still, in a case with voluminous records and a database created by the prosecution using undisclosed search terms, it would be extremely difficult to find the very same documents that the government relied on.[92] Because unearthing relevant, discoverable information in large databases can be problematic, partial or unguided disclosure is of little value. And, while an incomplete database may be useful,[93] it is not a substitute for full discovery.

[32] Uncontrolled searches of massive databases are like a right without a remedy. Burying the defense in data (as opposed to paper) does not serve the ends of justice and wastes resources. Full discovery must comport with due process and fulfill the constitutional mandates of compulsory

---

expending extensive, duplicative resources, the court compels production of the database."). The contents, a database of 20,000 arrest records, did not reveal mental impressions or litigation strategy and constituted fact, not opinion, work product. *Id.* at *3.

[90] *Schmidt*, 2007 U.S. Dist. LEXIS 30559, at *4; *cf.* Jules Epstein, *The Great Engine that Couldn't: Science, Mistaken Identifications, and the Limits of Cross-Examination*, 36 STETSON L. REV. 727, 729 (2007) (examining how exonerations and scientific studies have uncovered the shortcomings of cross-examination as a tool for ferreting out the truth of eyewitness identification, an issue that goes to the "integrity of the adversarial process").

[91] *Schmidt*, 2007 U.S. Dist. LEXIS 30559, at *3.

[92] *Cf.* Tessera, Inc. v. Micron Tech., Inc., No. C06-80024MISC-JW(PVT), 2006 WL 733498, at *8 (N.D. Cal. Mar. 22, 2006) ("Accordingly non-party Hynix Semiconductor America shall produce on DVD-ROMS or hard drives documents derived using *specific search terms* from databases created for the U.S. Department of Justice investigation of the DRAM industry and any related preceding litigation in which the Hynix Semiconductor companies were a party.") (emphasis added).

[93] *See* Omax Corp. v. Flow Int'l Corp., No. C04-2334L, 2007 WL 1830631, at *2 (W.D. Wash. June 22, 2007). The district court ordered disclosure of an incomplete database:

> Though Flow may very well be correct that the "Project" database is incomplete and potentially unhelpful in explaining differences between initial price quotations and final sales prices, Omax is nevertheless still entitled to the information contained in the 'Project' database, at least as it relates to initial price quotations offered to customers and potential customers. Though the data may be of limited value, it does have some value and it is relevant to Omax's damages case.

Id.

process and confrontation. Without substantial guidelines on prosecutorial disclosure and expert assistance for the defense when needed, the ends of justice are not furthered.

III. RIGHT TO PRESENT A DEFENSE AND EXCULPATORY EVIDENCE

[33] Private database services can be expensive, and much of the government's resources are not publicly accessible. Still, due process, equal protection and the right to effective assistance of counsel require the state to provide funds for expert and investigative services for those without means, independent of their ability to afford counsel.[94] Moreover, regardless of cost, an accused ought to have access to relevant and necessary resources in the exclusive possession or control of the state in furthering confrontation and compulsory process rights.

[34] In *People v. Evans*,[95] Stanley Evans faced charges of arson for allegedly setting fire to two Chevrolet vans.[96] In preparation for a hearing seeking dismissal of the charges (or in the alternative, trial), Evans asked the judge to order the New York City Police Department's Auto Crime Division to provide an expert who could examine the nonpublic VINS.[97]

---

[94] *See* Ake v. Oklahoma, 470 U.S. 68, 74-75 (1985).

> We hold that when a defendant has made a preliminary showing that his sanity at the time of the offense is likely to be a significant factor at trial, the Constitution requires that a State provide access to a psychiatrist's assistance on this issue if the defendant cannot otherwise afford one.

Id. See generally Paul C. Giannelli, *Ake v. Oklahoma: The Right to Expert Assistance in a Post-Daubert, Post-DNA World*, 89 CORNELL L. REV. 1305, 1331-38 (2004) (discussing availability of expert witnesses to indigent criminal defendants); Edward C. Monahan & James J. Clark, *Funds For Resources For Indigent Defendants Represented By Retained Counsel*, Champion, Dec. 1996, at 16, 18 ("Clients are seldom going to risk trial with retained counsel if that means they must forfeit access to funds for experts, investigation and other services despite their real indigence.").

[95] 534 N.Y.S.2d 640 (N.Y. Sup. Ct. 1988).

[96] *Id.* at 641.

[97] *Id.* The vehicle identification number (VIN) refers to:

> The identifying code for [a] SPECIFIC automobile. It is [a] car's fingerprint. It sets . . . vehicles apart from the millions of vehicles out

His goal was to dispute ownership of the vehicles and uncover irregularities in the numbers.[98] The motion, brought *ex parte*, was granted.[99]

[35] The Police Department asked the court to vacate the order.[100] Citing the state's obligation under *Ake* to provide expert services to indigent defendants and the accused's right to compulsory process, the judge concluded:

> Where the government holds a monopoly of expertise on a matter that reasonably bears on a defense in a criminal action, due process requires that a defendant be afforded access to this expertise. Such a rule places the defendant in the same position as the prosecutor because the district attorney unquestionably has the right to compel the police department auto crime experts to cooperate with the People in an appropriate case.[101]

[36] The only public source of the expertise was the NYPD's Auto Crime Division.[102] Private sources like the National Auto Theft Bureau and General Motors would not accede to Evans' request.[103] In addition, the judge observed that the ability of the defendant in this situation to hire an expert was irrelevant because "[w]hether or not he has funds to hire an expert, if the only source of expertise that may reasonably be necessary to

---

> there. Recently the VIN is reflected by 17 digit characters. It displays a car's uniqueness and manufacturer and provides a method to trace [a] car from the factory to the junk yard. [A] VIN can be used to track recalls, registrations, warranty claims, thefts and insurance coverage.

Vehicle Identification Number – VIN Numbers, What is a Vehicle Identification Number (VIN)?, http://www.vehicleidentificationnumber.com/vehicle_identification_numbers_vin_info.html (last visited Feb. 18, 2009).

[98] *See Evans*, 534 N.Y.S.2d at 641.

[99] *Id.*

[100] *Id.* at 641-42.

[101] *Id.* at 642 (internal footnote omitted).

[102] *Id.* at 641.

[103] *Id.* at 643.

his defense resides with the government, the government must give him access. This is the essence of fairness. Due process mandates no less."[104]

IV. BRADY

[37] *Evans* began with a pre-trial request for expert assistance.[105] Under *Brady v. Maryland*,[106] the prosecution may have an affirmative obligation to utilize or reveal computer-based information or face severe sanctions for nondisclosure and lack of cooperation.[107] The judge in *Evans* considered the potential problem of relying on the prosecution to conduct such investigations, and rejected the notion that the defense was "required to rest solely on the thoroughness and promptitude of the prosecutor."[108]

---

[104] *Id.*

[105] *Id.* at 641.

[106] 373 U.S. 83 (1963).

[107] *Id.* at 87; *see also* United States v. Dollar, 25 F. Supp. 2d 1320, 1322 (N.D. Ala. 1998) ("All charges against both defendants will be dismissed with prejudice because the United States . . . flagrantly, breached its unquestioned obligation to produce exculpatory and impeachment materials imposed by *Brady v. Maryland*.") (citation omitted); *cf.* Virgin Islands v. Fahie, 419 F.3d 249, 255 (3d Cir. 2005) (stating dismissal with prejudice is not always an appropriate remedy for government failure to turnover results of an ATF database search without finding exceptional circumstances: "While retrial is normally the most severe sanction available for a *Brady* violation, where a defendant can show both willful misconduct by the government, and prejudice, dismissal may be proper." (footnote omitted)).

[108] *Evans*, 543 N.Y.S.2d at 642 n.2. *Compare* United States v. Hsia, 24 F. Supp. 2d 14, 29-30 (D.D.C. 1998) ("[O]pen-file discovery does not relieve the government of its *Brady* obligations. The government cannot meet its *Brady* obligations by providing Ms. Hsia with access to 600,000 documents and then claiming that she should have been able to find the exculpatory information in the haystack. To the extent that the government knows of any documents or statements that constitute *Brady* material, it must identify that material to Ms. Hsia."), *with* United States v. Grace, 401 F. Supp. 2d 1069, 1080 (D. Mont. 2005):

> As it relates to the manner of production, *Brady* simply requires that information be produced in such a way that it will be of value to the accused. The government's production in this case complies with that requirement for at least two reasons. First, the documents have been presented in a searchable format. More importantly, over half of the documents presented -- 2,613,658 pages -- are actually Grace documents provided to the government during the Libby Superfund Clean-up litigation. There is no reason to assume that the government

The Supreme Court's holding in *Kyles v. Whitley*,[109] underscores this point. [110]

[38] Curtis Lee Kyles was sentenced to death for the murder of a 60-year-old woman in a supermarket parking lot.[111] His case rested largely on the testimony of an informant, who gave several inconsistent statements, and whose accounts raised suspicions about his involvement—all leading to serious potential challenges to eyewitness descriptions introduced at trial.[112]

[39] One element of the prosecution's theory was that Kyles drove his car to the parking lot where the murder was committed—leaving it there as he drove away in the victim's vehicle.[113] That night when the police arrived at the scene, they took down the license numbers of all the cars parked there, assuming one of the cars belonged to Kyles.[114] A computer printout of license plate numbers did not include Kyles' car, but authorities failed to disclose this fact to the defense.[115] At a minimum, disclosing this fact would have given Kyles' attorney a basis to challenge a grainy photo supposedly showing the defendant's car and contradict statements by the police informant who claimed to have picked up Kyles' vehicle later on from that location.[116]

> is better equipped through resources or knowledge to locate exculpatory documents than are the Defendants.

Id. (footnote omitted).

[109] 514 U.S. 419 (1995).

[110] *See id.* at 453 ("[T]he question is not whether the State would have had a case to go to the jury if it had disclosed the favorable evidence, but whether we can be confident that the jury's verdict would have been the same.").

[111] *Id.* at 419, 423.

[112] *See id.* at 450, 453.

[113] *Id.* at 423.

[114] *Id.*

[115] *Id.* at 428-29.

[116] *Id.* at 450.

V. DNA DATABASES AND THIRD PARTY SUSPECTS[117]

[40] The Court in *Kyles* hinted at the value of exculpatory evidence that pointed the "arrow of inculpation"[118] in another direction.[119] The revelations in that case did more to indict the informant than the defendant. Third party exculpatory information has gained importance and acceptance with the advent of DNA profiling.[120] Since the U.S. government maintains the largest DNA databank in the world as part of its law enforcement operations,[121] it makes sense that it could also be used in preparation of a defense based on an alternate suspect.

[41] There are only a handful of other countries with comparable resources, and none as extensive as the FBI database.[122] The enormity of

[117] There are a host of issues related to DNA discovery, access to post-conviction testing, and actual innocence claims that will not be considered in this article. *See generally* Glenn A. Garber & Angharad Vaughan, *Actual-Innocence Policy, Non-DNA Innocence Claims*, 239 N.Y.L.J. 4 (2008) (stating that courts should review claims of innocence in non-DNA cases); Brandon L. Garrett, *Claiming Innocence*, 92 MINN. L. REV. 1629 (2008) (arguing that appeals and post-conviction proceedings should review claims of innocence based on the "probative value of new evidence of innocence").

[118] Pennsylvania v. Ritchie, 480 U.S. 39, 46 (1987) (quoting Commonwealth v. Ritchie, 502 A.2d 148, 153 (Pa. 1985)).

[119] *See Kyles*, 514 U.S. at 450.

[120] *See* Steven Wisotsky, *Miscarriages of Justice: Their Causes and Cures*, 9 ST. THOMAS L. REV. 547, 548 (2007).

[121] "The CODIS Unit manages the Combined DNA Index System (CODIS) and the National DNA Index System (NDIS) and is responsible for developing, providing, and supporting the CODIS Program to federal, state, and local crime laboratories in the United States and selected international law enforcement crime laboratories to foster the exchange and comparison of forensic DNA evidence from violent crime investigations. The CODIS Unit also provides administrative management and support to the FBI for various advisory boards, Department of Justice (DOJ) grant programs, and legislation regarding DNA." Federal Bureau of Investigation: CODIS, http://www.fbi.gov/hq/lab/html/codis1.htm (last visited Feb. 18, 2009).

[122] The National DNA Index (NDIS) "contains over 6,539,919 offender profiles and 248,943 forensic profiles as of December 2008. Ultimately, the success of the CODIS program will be measured by the crimes it helps to solve. CODIS's primary metric, the 'Investigation Aided,' tracks the number of criminal investigations where CODIS has added value to the investigative process. As of December 2008, CODIS has produced over 80,900 hits assisting in more than 80,900 investigations." Federal Bureau of Investigation: CODIS-NDIS Statistics, http://www.fbi.gov/hq/lab/codis/clickmap.htm (last visited Feb. 18, 2009). *But see* The National DNA Database, *available at* http://www.homeoffice.gov/uk/science-research/using-science/dna-database/ (last visited

this unparalleled resource is beyond the capacity of under-resourced defendants.[123] The technology has advanced and improved over time, laying the groundwork for more post-conviction motions for testing or retesting biological evidence. This becomes all the more important as the scope of databanks changes.[124]

Feb. 10, 2009) (showing that the United Kingdom National DNA Database is second largest database with 4,983,859 profiles); 479 PARL. DEB., H.C. (6th ser.) (2008) 2344W, *available at* http://www.publications.parliament.uk/pa/cm200708/cmhansrd/cm080929/text/80929w0011.htm.

[123] *See, e.g.*, Brian Bakst, *Public Defenders Feel the Strain from Complex Courtroom Science*, DULUTH NEWS TRIB., Feb. 27, 2005:

> While the use of DNA evidence has grown rapidly in recent years, public defenders' expertise in the science has not. That's why the Board of Public Defense is seeking $1 million for a team of specially trained attorneys, ready for dispatch around Minnesota on major cases that hinge on DNA evidence or chemical tests on controlled substances like methamphetamine.

Id.

[124] Recently, the Department of Justice promulgated a rule expanding its DNA collection efforts to encompass arrestees. *See* DNA-Sample Collection and Biological Evidence Preservation in the Federal Jurisdiction, 73 Fed. Reg. 238 (Dec. 10, 2008) (to be codified at 28 C.F.R. pt. 28) ("This rule generally directs federal agencies to collect DNA samples from individuals who are arrested, facing charges, or convicted, and from non-United States persons who are detained under the authority of the United States, subject to certain limitations and exceptions."); Spencer S. Hsu, *New Rule Expands DNA Collection to All People Arrested*, WASH. POST, Dec. 12, 2008, at A2 ("The change could add as many as 1.2 million people a year to the national database, U.S. officials said."). Meanwhile, the United Kingdom has been ordered to change its retention rules to exclude DNA belonging to "unconvicted persons." *See In re* S. & Marper v. United Kingdom, App. Nos. 30562/04 & 30566/04 Eur. Ct. H.R. (2008) (stating that permanent retention of DNA from innocent persons violated Article 8 of the European Convention on Human Rights: "Everyone has the right to respect for his private . . . life . . ."); Richard Ford, *Police Are Ordered to Destroy All DNA Samples Taken from Innocent People*, TIMES (London), Dec. 5, 2008, *available at* http://www.timesonline.co.uk/tol/news/politics/article5289312.ece ("More than 1.6 million DNA and fingerprint samples of innocent people on police databases must be destroyed after a court ruled yesterday that keeping them breaches human rights.").

[42] In the 2008 term,[125] the United States Supreme Court will hear the case of William Osborne, convicted of kidnapping and assault in 1994, and sentenced to 26 years in prison.[126] He has been seeking access to genetic material for retesting in the Alaska state courts.[127] His aim is to apply modern techniques, unavailable at the time of his original trial, to the samples.[128] Although many states have enacted laws permitting post-conviction DNA testing, the Court must resolve whether there is a federal constitutional right to such testing.[129] Moreover, the questions of whether a defendant would have the right to access the database to test existing genetic material or seek a sample from a third party for testing has yet to be resolved.[130] This right would have its basis in the compulsory process clause, under the rubric of the right to present a defense.[131]

[43] In *Holmes v. South Carolina*,[132] the Supreme Court struck down a state court precedent that would have blocked evidence of third party guilt based on the strength of the prosecution's case.[133] Holmes was on trial for murder and proffered testimony of witnesses who put another suspect in the victim's neighborhood at the time of event.[134] These witnesses would have testified that this alternate suspect either confessed or admitted that Holmes was innocent.[135] However, the United States Supreme Court noted that South Carolina Supreme Court's holding in *State v. Gregory*,[136] deprived Holmes of the ability to present a complete defense:

---

[125] October Term 2008 runs from Oct. 6, 2008 through Sept. 5, 2009. 2008 Term Opinions of the Court, Supreme Court of the United States, http://www.supremecourtus.gov/opinions/08slipopinion.html (last visited Feb. 28, 2009).
[126] Brief for the Petitioners at 2, Dist. Attorney's Office for Third Judicial Dist. v. Osborne, 521 F.3 1118 (9th Cir. 2008), *cert. granted*, 129 S.Ct. 488 (U.S. Nov. 3, 2008) (No. 08-6).
[127] *Id.*
[128] *See* David Stout, *Supreme Court to Review DNA Case*, N.Y. TIMES, Nov. 3, 2008.
[129] Brief for the Petitioners, *supra* note 126, at (i).
[130] *See generally* Ken Strutin, *Third Party Culpability DNA Evidence*, N.Y. L.J., Oct. 4, 2005, at 4 (explaining the efficacy of retesting DNA evidence will depend upon a reexamination of longstanding discovery, testing and admissibility rules).
[131] U.S. CONST. amend. VI.
[132] 547 U.S. 319 (2006).
[133] *Id.* at 331.
[134] *Id.* at 323.
[135] *Id.*
[136] 16 S.E.2d 532 (1941).

> [B]y evaluating the strength of only one party's evidence, no logical conclusion can be reached regarding the strength of contrary evidence offered by the other side to rebut or cast doubt. Because the rule applied by the State Supreme Court in this case did not heed this point, the rule is "arbitrary" in the sense that it does not rationally serve the end that the *Gregory* rule and other similar third-party guilt rules were designed to further. Nor has the State identified any other legitimate end that the rule serves. It follows that the rule applied in this case by the State Supreme Court violates a criminal defendant's right to have "'a meaningful opportunity to present a complete defense.'"[137]

[44] Shortly after *Holmes* was decided, the Tennessee Court of Criminal Appeals heard the arguments of Sedley Alley,[138] a man sentenced to death for murder, kidnapping and rape, [139] who sought access to DNA testing to show that someone else was responsible.[140] The Sixth Circuit had already denied his § 1983[141] motion for testing, finding no constitutional right of

[137] *Holmes*, 547 U.S. at 331; *see Gregory*, 16 S.E.2d at 543.
[138] Alley v. State, No. W2006-01179-CCA-R3-PD, 2006 WL 1703820, *1 (Tenn. Crim. App. 2006).
[139] His appeals were ultimately unsuccessful and he was executed shortly after this decision. Melissa McNamara, *Tenn. Executes 2nd Person in 45 Years*, CBS NEWS, June 28, 2006, *available at* http://www.cbsnews.com/stories/2006/national/main1758849.shtml.
[140] *Id.*
[141] 42 U.S.C. § 1983:

> Every person who, under color of any statute, ordinance, regulation, custom, or usage, of any State or Territory or the District of Columbia, subjects, or causes to be subjected, any citizen of the United States or other person within the jurisdiction thereof to the deprivation of any rights, privileges, or immunities secured by the Constitution and laws, shall be liable to the party injured in an action at law, suit in equity, or other proper proceeding for redress, except that in any action brought against a judicial officer for an act or omission taken in such officer's judicial capacity, injunctive relief shall not be granted unless a declaratory decree was violated or declaratory relief was unavailable.

Id.

post-conviction access to DNA evidence.[142] Finally, the Governor of Tennessee granted a reprieve, allowing Alley to make a motion in state court for DNA testing.[143]

[45] Alley asked that underwear found near the victim, a stick used in the attack, and samples of genetic material from under the victim's fingernails, as well as about a dozen other items be tested.[144] He believed that "redundant results"[145] would exculpate him. And at the same time, he claimed that "DNA testing results could be entered into CODIS or a state DNA database and score a 'hit' to a convicted offender, thus not only exonerating Mr. Alley, but also identifying the actual assailant."[146] The "assailant" might have been someone in CODIS, or a new suspect.[147] As discussed in the section below on reciprocal evidence, it appears that there is a constitutional argument supporting a balance of access rights.

[46] Despite Alley's reliance on *Holmes*, the state court denied his claim as insufficient under Tennessee's Post-Conviction DNA Analysis Act.[148] It found that Act to be limited to comparing a defendant's DNA to crime related evidence.[149] The court rejected: "any implied testing of third party individuals or the need to 'run' DNA testing results through a DNA database for 'hits.' Indeed, other states have rejected requests to compare DNA profiles with state and national DNA databases as 'add[ing] yet another layer of speculation.'"[150] Rejecting the idea that the statute created a liberty interest, the court did concede: "Any interest created by enactment of the Act created a limited interest of a defendant in

[142] McNamara, *supra* note 139.
[143] *Alley*, 2006 WL 1703820, at *1.
[144] *Id.* at *3.
[145] *Id.* Redundant results are: "DNA tests results that establish the same genetic profile on a number of probative items of evidence." *Id.*
[146] *Id.*
[147] When a defendant claiming innocence seeks the genetic identity of an alternate suspect through discovery, in essence, it is no different than when a prosecutor files a John Doe DNA warrant to secure an indictment based on genetic material alone. *See* Veronica Valdivieso, *DNA Warrants: A Panacea for Old, Cold Rape Cases*, 90 GEO. L.J. 1009, 1009 (2002).
[148] *Alley*, 2006 WL 1703820, at *16.
[149] *See id.* at *5.
[150] *Id.* at *9 (citing Commonwealth v. Smith, 889 A.2d 582, 586 n.6 (Pa. Super. Ct. 2005)).

establishing his/her innocence and did not create an interest in establishing the guilt of a speculative and unknown third party."[151] The court would not accept an expansion of testing beyond confirming or negating Alley as the source of the DNA.[152]

[47] The arguments made by Alley, including one grounded on actual innocence,[153] might be redeemed depending on the Supreme Court's decision in *Osborne* this term. Already, several Circuit Courts of Appeals have recognized a federal constitutional right to post-conviction DNA testing broader than most state statutes.[154] The next step will be to justify expanding that right to encompass investigation of third party or alternate suspects.

[48] The federal and state DNA databases can serve two ends. Discovery, on the one hand, is imperative to enable defendants to successfully raise

---

[151] *Id.*

[152] *Id.* at *24.

[153] *Id.* at *10 (holding that there was no authority to consider a *Herrera* innocence claim based on evidence outside the trial record). At best the state DNA statute provided a gateway motion for potential future innocence claims. *See generally* Garrett, *supra* note 117 (discussing the case of House v. Bell, 547 U.S. 518 (2006) and subsequent claims of innocence based on DNA); Brandon L. Garrett, *Judging Innocence*, 108 COLUM. L. REV. 55 (2008) (examining the types of evidence that lead to wrongful convictions and later exonerations through DNA).

[154] *See generally* David A. Schumacher, Comment, *Post-Conviction Access to DNA Testing: The Federal Government Does Not Offer an Adequate Solution, Leaving the States to Remedy the Situation*, 57 CATH. U. L. REV. 1245, 1246-47 (2008):

> The Supreme Court has yet to rule on whether post-conviction claims are cognizable under § 1983, and the federal circuit courts of appeals are split on the matter. The Fourth, Fifth, and Sixth Circuit Courts of Appeals have all held that an inmate seeking to challenge a conviction through DNA evidence does not have a cognizable claim because a § 1983 lawsuit amounts to a direct attack on the legitimacy of the conviction. [¶] Four other circuits have gone the opposite way. The Second, Seventh, Ninth, and Eleventh Circuit Courts of Appeals, as well as district courts residing in two circuits that have yet to speak on this issue, have held that while an inmate has a cognizable claim for access to DNA testing under § 1983, the process for release must still be found in a subsequent habeas corpus lawsuit.

Id.

claims of third party responsibility and exonerate themselves. On the other hand, access is necessary to challenge the validity of database output used as prosecution evidence. There has been litigation to gain access to the FBI database to test its accuracy and the validity of the statistical conclusions underlying its matches.[155] There is also the capital prosecution case of Juan Luna, who was accused of participating in a multiple homicide at a Chicago eatery.[156]

[49] A Cook County judge granted a discovery request (subpoena) from Luna and ordered the Illinois State Police Forensic Science Center to give the defense limited access to the DNA profile database.[157] "Luna's defense team [was] hoping the DNA database information [could] help them poke holes in prosecutors' assertions that DNA matching Luna with a chicken dinner at the crime scene [had a] more than a 1 in 1 trillion chance of being someone other than Luna."[158]

[50] The prosecutors claimed that Luna's DNA matched genetic material taken from a chicken bone found at the crime scene, because Luna's DNA matched nine out of thirteen genetic loci,[159] a match whose occurrence in

---

[155] *See, e.g.*, Jennifer Friedman, *Release State DNA Profiles*, L.A. TIMES, July 27, 2008, at 2 (referring to a letter to the Editor from a Los Angeles County Public Defender pointing out the need for academics to vet the state databank to assess the accuracy of statistical profiling).

[156] *See Now, Another Kind of Waiting Begins*, CHI. DAILY HERALD, Jan. 8, 2003, at 1 (reporting on a five part series about the case before trial).

[157] Kara Spak, *Defense in Brown's Chicken Case Gets DNA Access*, CHI. DAILY HERALD, Aug. 15, 2006, at 13.

[158] *Id.*

[159] *See generally* Chris Smith, *Anatomy of a DNA Match*, S.F. MAG., Sept. 2008, http://www.sanfranmag.com/story/anatomy-dna-match:

> In 1997, FBI scientists decided on a predetermined set of 13 loci that is enough to indicate identity; most experts agree with that standard. It's generally believed that only identical twins match at 13, and that the chances of a coincidental 13-locus match—meaning it's all a terrible mistake and the defendant is innocent—is, on average, one in a trillion.

Id.; HUMAN GENOME PROJECT, DNA FORENSICS, http://www.ornl.gov/sci/techresources/Human_Genome/elsi/forensics.shtml (last visited Feb. 10, 2009):

the Hispanic population was one in 2.8 trillion.[160] Inspired by the results of an Arizona study, Luna wanted the raw data to find convicted felons who met the nine out of thirteen loci.[161]

[51] The court fashioned a compromise: the defense was not given access to the raw data, but the police would have to run a nine-loci analysis.[162] An appeal was pursued because the prosecution claimed that running the study would violate federal and state laws by using the database for an extra legal purpose.[163] The defense countered that it was in the same spirit as statutorily authorized quality assurance testing of crime laboratories.[164] The prosecutors pointed out that smaller public databases (with up to 17,000 profiles) were available for testing.[165] According to Luna's defense team, this would hardly compare with the 220,000 profiles in the state database.[166]

[52] The right to confrontation is directed at the sources of evidence the prosecutor has marshaled against the defendant—not a second tier substitute. Courts are always concerned about the authenticity and originality of evidence, and take pains to exclude hearsay and secondhand information. Thus, there is no rational basis for shielding the data in the government's computer, and relegating the defense to run studies, likely inadmissible, on private sources that are not fair representations.

> To identify individuals, forensic scientists scan 13 DNA regions, or loci, that vary from person to person and use the data to create a DNA profile of that individual (sometimes called a DNA fingerprint). There is an extremely small chance that another person has the same DNA profile for a particular set of 13 regions.

Id.

[160] *See* Brian Mackey, *Court Allows Defendant's DNA Data Request*, CHI. DAILY L. BULL., Aug. 15, 2006, at 1.

[161] *Id.*

[162] *Id.*

[163] *Id.*

[164] *Id.*

[165] *Id.*

[166] *Id.* Eventually, Luna was convicted and sentenced to life in prison. His case is currently on appeal. *See* Eric Herman, *Brown's Murderer Gets Life In Prison*, CHI. SUN TIMES, Aug. 9, 2007, at 10; Stacy St. Clair, *State Police Lauded For Saving Evidence*, CHI. DAILY HERALD, Oct. 17, 2007, at 21 ("After Luna's murder trial, jurors said the DNA evidence played a key role in their decision to convict.").

[53] The Arizona study noted above was an important basis for the defendant's application in Luna. [167] It arose from a discovery by an analyst working at the Arizona crime laboratory in 2001.[168] She found two felons who matched at nine of thirteen loci, but was disturbed by a comparison of their mug shots—one African-American, the other Caucasian.[169] Dozens of similar matches were uncovered.[170] This revelation threatened to undermine the quality of statistical matching relied on by federal and state authorities and raised the specter of higher numbers of false matches.[171]

[54] Since then, the study has spurred defense requests for "Arizona Searches" as in *Luna*.[172] For example, a San Francisco lawyer defending a rape case based on a nine-loci match was intrigued enough by the Arizona study to subpoena new results.[173] "Among about 65,000 felons, there were 122 pairs that matched at nine of 13 loci. Twenty pairs matched at 10 loci. One matched at 11 and one at 12, though both later proved to belong to relatives."[174] In a Maryland death penalty case the court ordered a quality assurance test of the state's DNA database at the defense's request.[175] "In a database of fewer than 30,000 profiles, 32 pairs matched at nine or more loci. Three of those pairs were [perfect matches,] identical at 13 out of 13 loci."[176] Finally, academics and experts have added their voices in calling for access to the DNA databanks to test the assumptions of profile rarity.[177]

---

[167] *See* Jason Felch & Maura Dolan, *Crime Labs Finding Questionable DNA Matches: FBI Tries to Keep National Database Away from Lawyers*, S.F. GATE, Aug. 3, 2008.
[168] *Id.*
[169] *Id.*
[170] *Id.*
[171] *Id.* ("At the time, [many] states looked at [only] nine or fewer loci when searching for suspects. (States now commonly attempt to compare 13 loci, though often fewer are available from old or contaminated crime scene evidence.)").
[172] *Id.*
[173] *Id.*
[174] *Id.*
[175] *Id.*
[176] *Id.*
[177] Maura Dolan & Jason Felch, *The Verdict is Out on DNA Profiles*, L.A. TIMES, July 20, 2008, *available at* http://articles.latimes.com/2008/jul/20/local/me-dna20.

> Bruce Weir, a statistician at the University of Washington who has studied the issue, said these assumptions should be tested empirically in

VI. CONFRONTING COMPUTER DATABASE EVIDENCE

[55] Databases can serve as an investigative tool for the defense, as in the *Luna* case. They can also be used to challenge database results presented by the prosecution during its case-in-chief. Here, we must consider the government's constitutional burden of proof, the defense's right to confrontation, and the limited remedies available under the codes of procedure. From a due process standpoint, it might be argued that certain kinds of database evidence, proven unreliable or inaccessible, ought to be categorically excluded.[178]

[56] One foundation of a demand by the defense for database discovery is the right to confront the witnesses against the accused.[179] Confronting database output means questioning the entire system: data collection, entry, storage, retrieval, analysis and production. Civil litigation e-discovery has shined a light in the dark corners where information can hide, such as in metadata, and on the need to determine authenticity and authorship, which can change with each incarnation of a document or data record.[180]

> the national database system. "Instead of saying we predict there will be a match, let's open it up and look," Weir said. Some experts predict that given the rapid growth of CODIS, such a search would produce one or more examples of unrelated people who are identical at all 13 loci.

Id.

[178] *See generally* Boaz Sangero & Mordechai Halpert, *Why a Conviction Should not be Based on a Single Piece of Evidence: A Proposal for Reform*, 48 JURIMETRICS J. 43 (2007) (listing types of evidence prone to such mistakes and proposing future preventative legislation); Rory K. Little, *Addressing the Evidentiary Sources of Wrongful Convictions: Categorical Exclusion of Evidence in Capital Statutes*, 37 SW. U. L. REV. (forthcoming 2009) (citing polygraph evidence as one longstanding example, and pointing out several categories of evidence proven unreliable in wrongful conviction cases, such as junk science).

[179] Although the right to confrontation has primarily been viewed as a trial right, "there might well be a confrontation violation if . . . a defendant is denied *pretrial* access to information that would make possible effective cross-examination of a crucial prosecution witness." Pennsylvania v. Ritchie, 480 U.S. 39, 61-62 (1987) (Blackmun, J., concurring) (emphasis added).

[180] Metadata in particular can be useful in clarifying the relationships among documents through pathnames and file storage architecture, version and drafting dates, and the other

[57] Law enforcement, and particularly government forensic witnesses, sometimes rely upon analysis and data garnered from institutional knowledge, and in some cases specialty databases. In a heroin smuggling case from the early 1980s, the defendant was charged with transporting the narcotic in caviar tins.[181] A chemical analyst employed by the government testified that the substance recovered was heroin.[182] The bases for his opinion were laboratory tests and computer analysis.[183] Cross-examination at trial revealed that "he [the expert] knew nothing about the computer program which caused the computer to bring forth the information it produced."[184]

[58] The defense made a confrontation clause argument: without disclosure of the technical information on how the computer worked, they could not effectively cross-examine the prosecution's witness.[185] The trial court judge rejected this argument, finding that the defense had ample information to attack the weight of this expert's opinion and the technical information would not have added to it.[186] On appeal, the defendant emphasized the importance and value of obtaining that computer information pretrial.[187] The Seventh Circuit, however, was not persuaded, and found that the testimony did not introduce "computer printouts or direct testimony of results."[188] Instead, the expert had relied on "recognized instrumental techniques involving the use of a computer."[189] In the court's eyes, the fact that the machinery involved was commercially or commonly used deflated the defense's argument.[190]

---

points on the information cycle, and this type of nuanced discovery can easily be overwritten by failure to preserve the evidence in its original format or through purposeful document scrubbing. *See generally* Douglas L. Rogers, *A Search for Balance in the Discovery of ESI Since December 1, 2006*, 14 RICH. J.L. & TECH. 8 (2008) (proposing ways in which the discovery phase may become more manageable).

[181] United States v. Bastanipour, 697 F.2d 170, 172 (7th Cir. 1982).

[182] *Id.* at 176.

[183] *Id.*

[184] *Id.*

[185] *Id.*

[186] *Id.* at 176-77.

[187] *Id.* at 177.

[188] *Id.*

[189] *Id.*

[190] *Id.* at 176-77.

[59] The direct evidence versus supporting role of computer-generated evidence test does not carry much weight today. Challenges to the reliability of computer software governing the operations of some of the most commonly used forensic technology, such as breathalyzers, have been gaining momentum and widening the doors of discovery.[191]

[60] The New Jersey case of *State v. Fortin*,[192] illustrates how far these developments have come.[193] Steven Fortin was among a group of suspects being investigated in the beating death of a woman who was killed en route to a local grocery store in Woodbridge.[194] At the time, he had been living nearby.[195] His connection to the case did not emerge until months later, when Maine State Police contacted Woodbridge law enforcement about Fortin, who was under investigation for sexually assaulting a trooper.[196]

---

[191] *See* Ken Strutin, *An Examination of Source Code Evidence*, N.Y. L.J., Nov. 13, 2007, at 5.

> Testing and analysis of source codes ought to be allowed to meet the requirements of due process. Since an accused is entitled to independently test physical and biological evidence, there is a compelling and essential need to question the proficiency of the machines that do the analyzing and measuring. This is particularly important when the evidence, whether time sensitive or consumed by examination, no longer exists.
>
> When it comes time to face the output from an analysis by a computer driven machine, a human being has the right to know whether the inner workings of that witness are reliable. And every defendant ought to be entitled to examine those inner workings with the help of an expert.
>
> These source code cases suggest the need for quality assurance and proficiency testing of computerized scientific equipment in the same vein as the protocols for forensic laboratories. Although sophisticated and impressive, computer programs should be answerable for their errors.

Id.

[192] State v. Fortin, 843 A.2d 974 (N.J. 2004).

[193] *Id.* at 999 (denying admissibility of an expert's testimony without a "reliable database" as proof of scientific reliability).

[194] *Id.* at 984-86.

[195] *Id.* at 985.

[196] *Id.* at 986.

[61] Without matching genetic material or other forensic evidence, the police did not have much to connect Fortin to the New Jersey crime, except for the similarity in the modus operandi.[197] The New Jersey prosecutors called upon the services of a retired FBI agent and "expert in violent sexual crimes," Robert R. Hazelwood, to catalog the similarities between the crimes committed against the New Jersey and Maine victims.[198] At trial he offered an opinion based on comparisons of various acts and injuries at the two crimes as to motive, modus operandi, and signs of ritual.[199] Hazelwood concluded that he had not seen the same combination of ritualistic behaviors in his work over the course of his thirty-year career.[200] He also stated that he had never seen the particular combination of modus operandi and ritualistic behaviors "in any other crime and I've never heard of it and I've never read of it."[201] Hazelwood's testimony was critical to identifying Fortin as the culprit. His analysis and comparison of the two assaults allowed the jury to infer that Fortin was responsible in the New Jersey case.[202]

[62] Before he could testify about his "uniqueness analysis," the court ordered Hazelwood to disclose the database of cases that formed the foundation for his work.[203] It was a precondition to admitting evidence of the methods of his crime comparison techniques and assessing the reliability of the information upon which he relied.[204] The prosecution argued that the witness drew on his experience in law enforcement and did not have a list of cases, only the information cited in his curriculum vitae.[205] Still, the admission of his testimony was predicated on the production of a reliable database for defense examination.[206] His resume was insufficient for that purpose, and the court would not place the burden on the defense of combing through Hazelwood's publications and citations to assemble a database from the 7,000 cases he investigated over his

[197] *Id.*
[198] *Id.* at 987.
[199] *Id.*
[200] *Id.* at 988.
[201] *Id.*
[202] *See id.* at 998-99.
[203] *Id.* at 999-1000.
[204] *Id.* at 999.
[205] *Id.*
[206] *Id.*

career.[207] The expert was in the best position to assemble that information, and without the database, there was no means for testing his conclusions at trial.[208]

[63] The investigative techniques underlying the "uniqueness analysis" had the "aura of science," and thus justified subjecting it to the more rigorous requirements for the admission of scientific evidence.[209] New Jersey's Rule of Evidence 705[210] empowered the judge to order an expert to reveal his underlying data as a condition of testifying, which the expert would have to disclose in response to cross-examination as well.[211] The purpose behind the court's original order was to ensure the reliability of the database upon which Hazelwood would offer testimony that might lead the jury to conclude Fortin was responsible.[212] The court went on to describe the contents of this database:

> Hazelwood's database should have consisted of violent sexual assault cases that he had investigated, studied, or analyzed during his professional career, and the peculiar *modus operandi* and ritualistic characteristics of those crimes. Such a database would have provided some basis for verifying the frequency of sexual assaults in which perpetrators bite the faces or breasts of their victims, or

[207] *Id.* at 1000.
[208] *Id.* ("We cannot agree with the trial court that Hazelwood's reference to his experience, training, and education was a substitute for a 'database of cases' or that the failure to provide such case information only went to the weight to be given to his opinion, rather than its admissibility.").
[209] *Id.*
[210] New Jersey Law Network, Rule 705: Disclosure of Facts or Data Underlying Expert Opinion; Hypotheses not Necessary, http://www.njlawnet.com/njevidence/705.html:

> The expert may testify in terms of opinion or inference and give reasons therefor without prior disclosure of the underlying facts or data, unless the court requires otherwise. The expert may in any event be required to disclose the underlying facts or data on cross-examination. Questions calling for the opinion of an expert witness need not be hypothetical in form unless the judge in his discretion so requires.

Id.
[211] *Fortin*, 843 A.2d at 1001.
[212] *See id.* at 998-99.

> manually strangle them, or engage in high risk attacks, to name but a few of the characteristics Hazelwood found distinctive in this case. If Hazelwood was correct about the unique combination of characteristics that the Gardner [Maine victim] and Padilla [N.J. victim] assaults had in common, the database would have strengthened and validated his conclusions. The jury also was entitled to know if there were any flaws in his analysis.[213]

[64] The appellate judges, however, were not in a position to define the size of the database, only determining it must allow an "acceptable basis for comparison."[214] The trial court would have to hold a hearing to make that assessment.[215] They concluded that it was reversible error for Hazelwood to testify without providing a reliable database to the defense beforehand.[216]

[65] In a California case where the police used a sex crimes database to establish the identity of the defendant through data correlation, the appeals court did not look kindly on the trial judge's uncritical admission of the evidence.[217] In *People v. Hernandez*, Kenneth Hernandez was charged with committing several violent sex crimes involving two different victims.[218] Crime analysis evidence from a police database called Sherlock[219] showed that these cases involving unique modus operandi had

---

[213] *Id.* at 1002.
[214] *Id.*
[215] *Id.* ("At that hearing, the trial court must determine what number of cases can be reconfigured within reason and what number of case comparisons are necessary to give the opinion validity.").
[216] *Id.*
[217] *See People v. Hernandez*, 63 Cal. Rptr. 2d 769 (Cal. Ct. App. 1997) (discussing the use of a computer system named Sherlock, which the court deemed "pseudo-scientific" testimony).
[218] *Id.* at 770.
[219] *Id.* at 771. Sherlock is

> "[A]n in-house database that was developed by crime analysis. It was defined by the sex crimes unit, variables that we capture in there. Information that is put into the sex crimes file is from a sex crimes log, which each case that is assigned to a sex crimes detective has very specific information that's put down on a sex crimes log. [¶] In turn, that log is given to us and we enter it, give it to a clerical support

not occurred before defendant moved into the searched area or since his arrest, which was central to his identification.[220]

[66] The defense opposed admission of the evidence as unscientific and lacking indicia of reliability, and because no discovery had been granted.[221] Based on the analyst's testimony, the trial judge let the evidence in.[222] On appeal, however, the court was highly dubious of the foundations for the reliability of the database:

> [T]he challenge here boils down to the basic question of whether the sources of information for the data base [sic] of Sherlock's system "were such as to indicate its trustworthiness." As noted earlier, the prosecutor argued the information in Sherlock was trustworthy because it was relied upon by the sex crimes detectives on a daily basis to do their jobs solving sex crimes. Such explanation, which the trial court apparently accepted, completely ignores the fact the business records exception has been held inapplicable to admit police reports into evidence for the sheer reason such are or might be based upon the observations of victims and witnesses who have no official duty to observe and report the relevant facts (citations omitted). The data base [sic] in Sherlock was taken from the sex crimes log prepared from the purported "relevant facts" from original police reports, whatever those may be.[223]

> person in the crime analysis unit who then enters each item into the Sherlock system, into the Sherlock sex crimes files."
>
> The entries to Sherlock were generally done within three to four days after a reported sex crimes incident.

Id.

[220] *Id.*

[221] *Id.*

[222] *Id.* at 773.

[223] *Id.* at 778-79 (citations omitted).

The Court of Appeals went on to note that putting information into a computer does not cloak it in reliability.[224] The computer did not have the power to transform hearsay from police reports into nonhearsay evidence.[225]

VII. RECIPROCAL DISCOVERY: RESTORING BALANCE

[67] A level playing field is crucial in the Information Age. Police and prosecutors have access to a widening array of surveillance tools and data from consumer and social networking technologies.[226] In a Supreme Court of Louisiana decision from the 1980s, we can observe the importance of balancing access to information resources, albeit human.[227]

[68] In *Kirk v. State*, Philip Kirk, Jr. was charged with mail fraud in federal court.[228] He, along with his attorney, brought an action in state court for declaratory and injunctive relief over a Louisiana statute that prohibited him from recording confidential conversations of adverse witnesses without their consent. [229] At the same time, law enforcement was free to do so.[230] Basically, the defense wanted to prevent the authorities

---

[224] *Id.* at 779.
[225] *Id.*
[226] *See, e.g.*, U.S. DEP'T OF JUSTICE, ELECTRONIC SURVEILLANCE MANUAL (2005), http://www.usdoj.gov/criminal/foia/docs/elec-sur-manual.pdf (explaining technologies and procedures).
[227] *See* Kirk v. State, 526 So.2d 223, 226-27 (La. 1988) (reviewing a state court ruling mooted by defendant's acquittal in a connected federal criminal action); *id*. at 227 (Watson, J., concurring) (declaring the case moot from the outset).
[228] *Id.* at 224.
[229] *Id.; see* LA. REV. STAT. ANN. § 14:322.1(A) (1990):

> It shall be unlawful for any person, intentionally and without the consent of all parties to a confidential communication, to eavesdrop upon or record such confidential communication by means of any electronic amplifying or recording device, whether such communication is carried on among such parties in the presence of one another or by means of a telegraph, telephone, or other device.

Id.
[230] LA. REV. STAT. ANN. § 14:322.1(D)(3) (1990) ("This Section shall *not* apply to the following: . . . A law enforcement agency or any of its authorized agents.") (emphasis added).

from prosecuting him as a result of getting witness statements, necessary for the defense, in violation of the law.[231]

[69] The prosecutor already possessed records of conversations between defendant and these witnesses.[232] Kirk and his lawyer claimed that the statute violated equal protection by exempting police but exposing the defense to criminal liability.[233] The case against Kirk rested on an alleged plan between defendant and his employees to defraud Photon, Inc., the corporation for which they worked.[234] Law enforcement had used these employees to record conversations with the defendant to build its case.[235] Kirk wanted his investigator to speak with these same witnesses to prepare an entrapment defense.[236]

[70] Nothing in the legislative history or case law suggested a justification for this imbalance. The court concluded:

> It is as fundamentally unfair to prohibit a criminal defendant from obtaining evidence by electronic recording of conversations when the prosecutor is free to obtain such evidence by the same method, at least in the absence of any reasonable basis for the distinction. Inasmuch as La. R.S. 14:322.1 violates a criminal defendant's constitutional right to equal protection of the law under both the federal and state constitutions, the statute cannot stand.[237]

[71] The accused should be able to use those tools relied upon uniquely by law enforcement and the prosecution in preparing a defense. Objections by the government run counter to its use of databases and the like in meeting its burden of proof.[238] The defense is not in the same position as the state when it comes to marshalling electronic resources.[239]

---

[231] *Kirk*, 526 So.2d at 224.
[232] *Id.* at 224.
[233] *Id.* at 225-26.
[234] *Id.* at 225.
[235] *Id.*
[236] *Id.*
[237] *Id.* at 227.
[238] *Cf.* United States v. Sheffer, 523 U.S. 303, 337-38 (1998) (Stevens, J., dissenting):

[72] These reciprocal discovery and disclosure obligations are firmly rooted in the right to present a defense. In *Wardius v. Oregon*,[240] the Supreme Court overturned a conviction due to an invidious state alibi evidence rule that did not allow the defense reciprocal discovery of the state's rebuttal witnesses. [241] Describing discovery as a "two-way street," Justice Marshall made this point about due process:

> The State may not insist that trials be run as a "search for truth" so far as defense witnesses are concerned, while maintaining "poker game" secrecy for its own witnesses. It is fundamentally unfair to require a defendant to divulge the details of his own case while at the same time subjecting him to the hazard of surprise concerning refutation of the very pieces of evidence which he disclosed to the State.[242]

[73] In footnote nine of its opinion, the Court anticipated the problem defendants today face in seeking discovery of government database information, while the defendant's computerized data may already be known or uncovered through investigation by the prosecution.[243]

> It is incongruous for the party that selected the [polygraph] examiner, the equipment, the testing procedures, and the questions asked of the defendant to complain about the examinee's burden of proving that the test was properly conducted. While there may well be a need for substantial collateral proceedings when the party objecting to admissibility has a basis for questioning some aspect of the examination, it seems quite obvious that the Government is in no position to challenge the competence of the procedures that it has developed and relied upon in hundreds of thousands of cases.

Id.; Rock v. Arkansas, 483 U.S. 44, 55 (1987) ("Just as a State may not apply an arbitrary rule of competence to exclude a material defense witness from taking the stand, it also may not apply a rule of evidence that permits a witness to take the stand, but arbitrarily excludes material portions of his testimony.").

[239] *See generally* U.S. DEP'T OF JUSTICE, INDIGENT DEFENSE AND TECHNOLOGY: A PROGRESS REPORT (1999), http://www.ncjrs.gov/pdffiles1/bja/179003.pdf (studying the "disparities in resources and technological expertise" in public defense offices).

[240] 412 U.S. 470 (1973).

[241] *Id.* at 472.

[242] *Id.* at 475-76.

[243] *See id.* at 476 n.9.

Specifically, the Court noted: "Indeed, the State's inherent information-gathering advantages suggest that if there is to be any imbalance in discovery rights, it should work in the defendant's favor."[244]

[74] The Court has stressed that the Constitution will trump a state evidence rule that denies a defendant the right to present his case or challenge the evidence. In *Chambers v. Mississippi*,[245] a hearsay rule that prevented introduction of exculpatory evidence of third party guilt violated due process;[246] and a rule barring a co-participant's testimony in *Washington v. Texas*,[247] which would have allowed the prosecution to present that evidence, ran afoul of the compulsory process clause.[248]

---

[244] *Id.*

[245] 410 U.S. 284, 302 (1973):

> Although perhaps no rule of evidence has been more respected or more frequently applied in jury trials than that applicable to the exclusion of hearsay, exceptions tailored to allow the introduction of evidence which in fact is likely to be trustworthy have long existed. The testimony rejected by the trial court here bore persuasive assurances of trustworthiness and thus was well within the basic rationale of the exception for declarations against interest. That testimony also was critical to Chambers' defense. In these circumstances, where constitutional rights directly affecting the ascertainment of guilt are implicated, the hearsay rule may not be applied mechanistically to defeat the ends of justice.

Id.

[246] In defense of a murder indictment, Leon Chambers wanted to call a man who had confessed the killing as well as the witnesses who heard his statement. The state's voucher rule prevented him from impeaching his own witness, and the testimony of the other witnesses to the admissions was hearsay. *Id.* at 289-90. The Supreme Court did not allow the defendant to be deprived of an opportunity to present his case due to an overly restrictive state rule of evidence. *Id.* at 302.

[247] 388 U.S. 14, 19 (1967):

> The right to offer the testimony of witnesses, and to compel their attendance, if necessary, is in plain terms the right to present a defense, the right to present the defendant's version of the facts as well as the prosecution's to the jury so it may decide where the truth lies. Just as an accused has the right to confront the prosecution's witnesses for the purpose of challenging their testimony, he has the right to present his own witnesses to establish a defense. This right is a fundamental element of due process of law.

[75] Both cases illustrate the constitutional imperatives behind a defendant's right to marshal evidence in his favor, albeit outside the restrictions of inequitable state evidentiary rules. Restrictions on accessing government databases due to privilege and privacy arguments cannot reasonably overcome due process and compulsory process mandates. The contents of a database, like an alternate suspect's confession to witnesses or the admissions of a convicted co-defendant, can be relevant to innocence and cast doubt on the strength of the prosecution's case. The collective knowledge embodied in government resources stand behind police and forensic witnesses, and indirectly serves as testimony against the accused. Basic fairness demands that these databases also be called into service for the defense.

VIII. CONCLUSION

[76] At one time, when it was possible for a human being to master the entire sum of knowledge in a field, such a person became an expert, a living database. It is no longer realistic for any individual to match the speed, size and sheer power of computer-based information. Law enforcement and forensic experts rely on these resources to conduct investigations, make comparisons, identify suspects and prepare cases for court. Their findings are inextricably bound to the information contained in these knowledge banks. As a matter of fairness, a defendant should be entitled to examine that same information to test its accuracy and reliability. In addition, defendants should be permitted access to the same tools to conduct their own investigations and prepare their cases.

Id.

[248] Jackie Washington wanted to call his co-defendant in the crime, who had already pled guilty and had been sentenced to fifty years in prison, to exculpate him. The Texas rule at the time would not allow it. His attempt to introduce exculpatory evidence was kept out by a rule whose foundations were unsupportable. *See id.* at 16-17. Compulsory process was a firmly established right and entitled Washington to produce exonerating evidence in his defense. *See id.* at 23.

[77] The complexity of the law[249] is mirrored by the staggering size, growth and depth of computer-generated data.[250] In the Information Age, it is inevitable that digitally-based output will lionize the evidence assembled by law enforcement in the prosecution of crime. As a result, the defense will labor under the heavy burdens of challenging presumptions of reliability and the aura of infallibility surrounding electronic data. Routine access to forensic databases and government expertise, or comparable resources, remains beyond the pale for most if not all defendants, regardless of their financial standing. While our justice system recognizes the strategic information advantage possessed by the prosecution, it has yet to adjust the playing field. Ultimately, the foundational principles of the Constitution and the lessons drawn from the civil side of the legal system will be called upon to offer guidance in the continued development of criminal e-discovery.

---

[249] *See generally* Paul Rosenzweig, *The Over-Criminalization of Social and Economic Conduct*, THE HERITAGE FOUNDATION, Apr. 7, 2003, http://www.heritage.org/Research/LegalIssues/upload/40268_1.pdf:

> Estimates of the current size of the body of federal criminal law vary. It has been reported that the Congressional Research Service cannot even count the current number of federal crimes. The American Bar Association reported in 1998 that there were in excess of 3,300 separate criminal offenses. More than 40 percent of these laws have been enacted in just the past 30 years, as part of the growth of the regulatory state. And these laws are scattered in over 50 titles of the United States Code, encompassing roughly 27,000 pages. Worse yet, the statutory code sections often incorporate, by reference, the provisions and sanctions of administrative regulations promulgated by various regulatory agencies under congressional authorization. Estimates of how many such regulations exist are even less well settled, but the ABA thinks there are "[n]early 10,000."

Id. (footnotes omitted).

[250] SCHOOL OF INFORMATION MANAGEMENT AND SYSTEMS AT THE UNIVERSITY OF CALIFORNIA AT BERKELEY, HOW MUCH INFORMATION? (2003), http://www2.sims.berkeley.edu/research/projects/how-much-info-2003/printable_report.pdf ("In 1997, the largest database was Knight Ridder's DIALOG, a text database, with 7 terabytes of storage, according to SearchDatabase.com. As of 2002, the world's largest database is at the Stanford Linear Accelerator Center which stores 500 terabytes of experiment data.").