# BIG DATA AND DUE PROCESS

*Brandon L. Garrett*†

INTRODUCTION ..... 207
I. BIG DATA AND ELECTRONIC DISCOVERY ..... 208
II. DIGITAL *BRADY* ..... 211
III. DIGITAL POSTCONVICTION DISCOVERY ..... 213
IV. DIGITAL *STRICKLAND* ..... 215
CONCLUSION ..... 215

## INTRODUCTION

Today, electronic footprints may follow us wherever we go. Electronic traces, left through a smartphone or other device, can be tracked to the scene of a crime, or they can place a person far from a crime scene.[1] Those traces can sometimes be tracked far more reliably than the types of trace evidence traditionally examined at crime scenes, like hairs, fibers, fingerprints, or tool marks.[2] Cases have already come to light in which individuals have cleared their names by using digital evidence, whether a surveillance video, an E-Zpass tag, a cellphone-tower signature, or an e-mail chain, and far more are certain to occur in the future. By the same token, individuals may be falsely implicated due to errors in large government or commercial databases, and evidence of innocence may linger in such archives without ever coming to light. Professors Joshua Fairfield and Erik Luna have done an important service by carefully introducing the problem of "digital innocence" and marking out areas in need of clear thinking and policy.[3]

The role that constitutional criminal-procedure rights will play with respect to litigation of such evidence remains quite uncertain. One reason is that the Due Process Clause provides such limited regulation of discovery in criminal cases, both pretrial and postconviction. In this response piece, I discuss four additional problems at the intersection of

---

† Roy L. and Rosamund Woodruff Morgan Professor of Law, University of Virginia School of Law.

1 As Ken Strutin puts it well, "[a] fact of modern life in the twenty-first century is the electronic footprint." Ken Strutin, *Databases, E-Discovery and Criminal Law*, 15 RICH. J.L. & TECH., Issue 3, at 1, 3 (2009).

2 On questions surrounding the reliability of forensic analysis of traditional trace evidence, see COMM. ON IDENTIFYING THE NEEDS OF THE FORENSIC SCIENCES CMTY., NAT'L RESEARCH COUNCIL, STRENGTHENING FORENSIC SCIENCE IN THE UNITED STATES: A PATH FORWARD 116–17 (2009), *available at* http://www.nap.edu/catalog/12589.html.

3 Joshua A.T. Fairfield & Erik Luna, *Digital Innocence*, 99 CORNELL L. REV. 981 (2014).

Big Data and due process rights: (1) the need for developed electronic discovery rules in criminal cases; (2) the need to reconsider the meaning of *Brady v. Maryland* and the due process obligations of prosecutors and government agencies in the context of government data; (3) the parallel need to reconsider standards for effective assistance of defense counsel; and (4) the need for broader and better-adapted postconviction electronic discovery and remedies.

## I
## BIG DATA AND ELECTRONIC DISCOVERY

Electronic information has become so ubiquitous that it will both inculpate and clear defendants far more often in the future. Police agencies now commonly track social media, rely on databases collecting information about crime hotspots and individuals, and monitor electronic communications.[4] One implication of Professors Fairfield and Luna's work is that far more attention must be generally paid to digital discovery in criminal cases. Indeed, improved digital discovery may help the government prove guilt far more often than it clears the innocent. However, it will do neither given the rudimentary state of electronic or digital discovery in most jurisdictions. By comparison to the criminal justice system, the civil system entered the world of e-discovery some time ago following formal amendments to the Federal Rules of Civil Procedure in 2006, and preceded by local rules and orders.[5] In contrast, as the Department of Justice's National Criminal Discovery Coordinator Andrew Goldsmith puts it, "a coherent body of case law on appropriate collection, management, and disclosure of [electronically shared information] has yet to emerge in the criminal context."[6] As data becomes increasingly relevant to criminal cases, particularly so-called "Big Data," rules capable of handling complex and Big Data discovery should be developed.

---

4 *See, e.g.*, Elizabeth Joh, *Policing by Numbers: Big Data and the Fourth Amendment*, 89 WASH. L. REV. 35, 60, 64 (2014) (discussing law enforcement's increased reliance on Big Data).

5 E-Discovery Amendments and Committee Notes, Amendments to the Federal Rules of Civil Procedure (Apr. 2006), *available at* http://www.uscourts.gov/uscourts/RulesAndPolicies/rules/EDiscovery_w_Notes.pdf; FED. R. CIV. P. 26(f) advisory committee's note.

6 Andrew D. Goldsmith, *Trends – or Lack Thereof – in Criminal E-Discovery: A Pragmatic Survey of Recent Case Law*, 59 U.S. ATT'Y BULL. 2, 2 (2011); *see also* Daniel B. Garrie & Daniel K. Gelb, *E-Discovery in Criminal Cases: A Need for Specific Rules*, 43 SUFFOLK U. L. REV. 393, 399 (2010) ("[T]he criminal justice system is devoid of procedural tools that provide criminal defendants with *automatic* access to ESI in the same fashion civil litigants enjoy pursuant to Rule 26 of the Federal Rules of Civil Procedure."). A working group has been created to begin to address this need. *See* JOINT WORKING GRP. ON ELEC. TECH. IN THE CRIMINAL JUSTICE SYS., DOJ AND ADMIN. OFFICE OF THE U.S. COURTS, RECOMMENDATIONS FOR ELECTRONICALLY STORED INFORMATION DISCOVERY PRODUCTION IN FEDERAL CRIMINAL CASES (2012), *available at* http://www.fd.org/docs/litigation-support/final-esi-protocol.pdf.

In criminal cases, however, there is no rule to which the courts can look for guidance in determining whether the production of digital evidence by the government has been in a form or format that is appropriate. The relevant discovery rules do not distinguish between paper documents and electronic records; they simply lay out discovery obligations (and in addition there are constitutional discovery obligations).[7] The "big paper" case is the exception rather than the rule in criminal cases.[8]

There have been more detailed judicial rulings in white-collar cases and corporate prosecutions, in which huge volumes of documents and digital records are more commonly reviewed and understood to be important.[9] In a Second Circuit decision in 1970, for example, the court noted (although finding that the violation did not require reversal) that: "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."[10] In one recent federal case in the District of Columbia, the court explicitly analogized to e-discovery rules under the Federal Rules of Civil Procedure regarding discovery related to large electronic databases.[11] Other cases have raised the opposite concern of a government "document dump." In cases such as the well-known *Skilling* case, federal courts have held that the government satisfies its discovery obligations by providing open-file access to the native database files, despite their volume, because the defendant could search the files just as the government could.[12]

The term "digital" applies to an incredibly wide range of types of information, ranging from Big Data in large databases to very small data. On the "small data" side, e-mails, text messages, and social-media communications between witnesses, law enforcement, and prosecutors may all raise discovery questions as well as questions of privilege.[13]

---

7 *See* 18 U.S.C. § 3500 (2012); FED. R. CRIM. P. 16. *See also* Fairfield & Luna, *supra* note 3, at 149.

8 United States v. O'Keefe, 537 F. Supp. 2d 14, 19 (D.D.C. 2008).

9 *See* Strutin, *supra* note 1, at 8.

10 United States v. Dioguardi, 428 F.2d 1033, 1038 (2d Cir. 1970). For a more in-depth discussion of the *Dioguardi* case, see Strutin, *supra* note 1, at 8.

11 *O'Keefe*, 537 F. Supp. 2d at 18–19 ("It is foolish to disregard [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."). *But see* United States v. Warshak, 631 F.3d 266, 296 (6th Cir. 2010) (rejecting analogy to Rules of Civil Procedure).

12 United States v. Skilling, 554 F.3d 529, 577 (5th Cir. 2009); *see also* United States v. W.R. Grace, 401 F. Supp. 2d 1069, 1080–81 (D. Mont. 2005) ("There is no reason to believe that the Defendants are less able to locate exculpatory materials within the evidentiary database than is the government.").

13 *See* Goldsmith, *supra* note 6, at 6–9; *see also, e.g.*, Stephanie Clifford, *Prosecutors are Reading Emails from Inmates to Lawyers*, N.Y. TIMES, July 22, 2014,

Issues of electronic metadata may increasingly arise in more routine criminal matters, including issues related to police reports that may have been paper documents in the past. For example, in a drug and weapon possession case, a district court suppressed the arrest where the government did not initially produce a photo array presented to an eyewitness who had initially identified a defendant.[14] The photo array was generated using a computerized database and provided in an electronic file.[15] The judge was concerned that the photo array eventually provided was created for the suppression hearing but not actually showed to the witness, where the government did not provide metadata to show when it was created.[16]

Of course, it should be no surprise e-discovery has lagged in criminal cases, because there is so little discovery in criminal cases to begin with. And pertinent evidence may not just be in the possession of the prosecutors; it may be social media related to witnesses or surveillance by other government agencies, or it may be cell phone or other data kept by commercial providers. Current e-discovery issues are not so different in kind from discovery issues regarding other archives of government information. For some time, for example, there have been questions concerning defense access to government DNA and fingerprint databases. In its own way, DNA evidence is often also electronic evidence, since when a search is done through the CODIS system of databases, [17] it is a search against a string of numbers entered based on DNA test results. These issues of access to government database evidence are not entirely new: in the 1980s, a New York state court held that where the government exclusively possessed vehicle identification numbers and the defendants required those numbers to try to prove the vehicles in question did not belong to the victims, it violated due process to deny the defense access.[18] The well-known U.S. Supreme Court decision in *Kyles v. Whitley* involved a license plate number as one piece of potentially exculpatory evidence.[19] Where discovery rules themselves remain so thin in criminal cases, due process rules may be important as a backstop to safeguard the fairness of criminal trials. Yet the due process regulation of discovery in criminal

---

http://www.nytimes.com/2014/07/23/nyregion/us-is-reading-inmates-email-sent-to-lawyers.html?_r=0.

14 United States v. Cross, No. 07-cr-730 (DLI), 2009 WL 3233267, at *6–8 (E.D.N.Y. Oct. 2, 2009).

15 *Id.*

16 *Id.*

17 CODIS is the Combined DNA Index System. *See* Erik Luna & Joshua A.F. Fairfield, *The Open Society and Its Digital Enemies: A Reply to Professors Bambauer and Garrett*, 99 CORNELL L. REVIEW ONLINE 216, 223 n.20 (2014).

18 People v. Evans, 534 N.Y.S.2d 640, 642 (N.Y. Sup. Ct. 1988). For an excellent discussion of the case, see Strutin, *supra* note 1, at 18–19.

19 514 U.S. 419, 428–29 (1995).

cases is not yet well adapted to Big Data or electronic discovery.

## II
## DIGITAL *BRADY*

The scope of any due process right to electronic discovery will be largely limited to what is constitutionally due under the *Brady v. Maryland* doctrine. Under *Brady v. Maryland*, prosecutors have a constitutional obligation to provide potentially exculpatory material to the defense.[20] In *Kyles v. Whitley*, the Court held that prosecutors must obtain that material from law enforcement, and the Court also emphasized how such material must be considered "collectively."[21] Professors Fairfield and Luna provide a very useful discussion regarding the question of whether the intelligence community sufficiently cooperates with law enforcement so as to be subject to *Brady* requirements, as well as a discussion of emerging caselaw concerning defense access to potentially exculpatory evidence in possession of third-party providers.[22] The more prosecutors rely on information from intelligence agencies or third-party sources of information, the stronger the defense argument that this information must be examined by prosecutors for potential discovery to the defense. Of course, it is a longstanding problem that the government's obligations under *Brady* and its progeny are not clearly defined and permit exercise of considerable judgment. Many jurisdictions have extremely narrow rules of discovery in criminal matters. Moreover, violations of the constitutional obligation, discovery rules, or ethical obligations will only arise if concealed information comes to light. That may not be a common event.

Nor will defendants always know to inquire. The "exonerating potential" of digital evidence depends very much on what it can show, and that may not be easily known, particularly after time has passed. A wide range of electronic information (and less and less information is *not* electronic in some fashion) may be potentially relevant, but not particularly probative of innocence or guilt. Moreover, the press may not learn of cases in which individuals are cleared early on in investigations by digital evidence, such as surveillance footage, for example. Exonerations occur, by definition, only after a conviction, and it may not be common for digital evidence to come to light many years later. After all, unlike evidence that can be DNA tested, which is now more routinely preserved by law enforcement as part of crime-scene evidence or in a crime-lab storage facility, digital evidence may not be routinely stored in a way that enables access for the first time years later.

---

20 Brady v. Maryland, 373 U.S. 83, 87 (1963).

21 514 U.S. at 436.

22 *See* Fairfield & Luna, *supra* note 3, at 155–60.

That may change as the technology evolves to permit better storage of this information, as Professors Fairfield and Luna describe.[23] Courts may increasingly entertain claims regarding failure to preserve or spoliation of social-media evidence and other forms of digital evidence.[24] To provide one additional example, video cameras may increasingly be worn by law enforcement, with their digital footage automatically stored offsite by the vendor (such as Taser).[25] However, due to these obstacles and limitations of the constitutional doctrine, pretrial discovery will frequently be more important than discovery occurring years later in response to claimed *Brady* violations.

Defendants do not know to ask for discovery of digital information if they do not know it exists; moreover, they must be able to understand what is available and how reliable it is. How can a defendant impeach a database? Impeachment evidence is *Brady* evidence;[26] the defense must be able to obtain access to evidence that can be used to question the credibility of a live witness. But what if it is an expert witness presenting Big Data findings, or the results of a database search, or the results of analytics on electronic surveillance? Impeaching that witness may require discovery regarding the reliability of and procedures used to produce the underlying evidence. Putting to one side the complex constitutional and privacy concerns regarding use of this information during criminal investigations,[27] errors in the collection and entry of those data themselves are an important subject, particularly where government databases may not be transparent or subject to sufficient quality control. (The scope of Confrontation Clause rights requiring that the government produce persons responsible for work on such a database will also raise interesting questions.[28])

We know that errors may occur when entering or maintaining information in any type of information system. For example, *Herring v. United States* involved an erroneous database entry concerning a warrant application.[29] In 2014, an audit of the national CODIS set of DNA

---

23 *Id.* at 120.

24 Margaret DiBianca, *Discovery and Preservation of Social Media Evidence*, BUS. LAW TODAY (Jan. 2014), *available at* http://www.americanbar.org/publications/blt/2014/01/02_dibianca.html.

25 Taser markets an Axon Flex glasses-camera that can be provided with a service automatically uploading data to its "Evidence.com" data-management resource. *See AXON Flex On-Officer Video*, TASER, http://www.taser.com/products/on-officer-video/axon-flex-on-officer-video (last visited Aug. 4, 2014).

26 Giglio v. United States, 405 U.S. 150, 153 (1972).

27 *See, e.g.*, Joh, *supra* note 4, at 60, 64.

28 For a description of a high-profile environmental prosecution in which Confrontation Clause issues related to a government database were extensively litigated, see Thomas C. Frongillo et al., *The Reinvigorated Confrontation Clause: A New Basis to Challenge the Admission of Evidence from Nontestifying Forensic Experts in White Collar Prosecutions*, 81 DEF. COUNS. J. 11, 22–24 (2014).

29 555 U.S. 135, 137 (2009).

databanks identified over 150 DNA profiles that were entered in error, based on handwriting mistakes or other oversights by lab technicians.[30] As Professor Erin Murphy has described, presumptions of regularity in such databases may not be warranted if they are maintained using shoddy procedures; however, even rudimentary discovery concerning the maintenance of government databases is often lacking.[31] And other errors may occur outside the control of law enforcement: identity theft itself raises the risk of mistaken digital identity, which data systems with inadequate controls or auditing might not detect.

Despite real concerns with exculpatory information regarding the accuracy of database evidence, there have been troubling rulings denying discovery to underlying databases or analyses.[32] Even for DNA evidence, defense access to the CODIS set of databases can be highly contested.[33] Discovery of electronic data is important—and so may be discovery of the methods that law enforcement uses to gather and store such data. The understanding of exculpatory evidence under *Brady* may need to be redefined when the database is not just the results of a database search that may inculpate or exclude but also the nature of the search terms, the reliability of the database entries, and the manner in which it is maintained. Each may be crucial information for the defense in order to effectively present a case. Hopefully, over time, courts will develop how *Brady* obligations require a meaningful inquiry into the sources and structure of digital evidence, just as a witness must be asked questions about more than just the substance of a formal statement to the police, or just as chain of custody must be documented for trace evidence.

## III
## DIGITAL POSTCONVICTION DISCOVERY

Discovery of any evidence of innocence years after the conviction, whether such evidence is digital or of some other kind, is not easy to introduce. All new facts are difficult to litigate postconviction, and the due process right to postconviction discovery has been defined by the Supreme Court as a quite limited procedural due process right to

---

30 Joseph Goldstein, *F.B.I. Audit of Database that Indexes DNA Finds Errors in Profiles*, N.Y. TIMES, Jan. 24, 2014, http://www.nytimes.com/2014/01/25/nyregion/fbi-audit-of-database-that-indexes-dna-finds-errors-in-profiles.html.

31 Erin Murphy, *Databases, Doctrine & Constitutional Criminal Procedure*, 37 FORDHAM URB. L.J. 803, 825–26 (2010).

32 *See, e.g.*, United States v. Schmidt, No. 04-cr-00103-REB, 2007 WL 1232180, at *1 (D. Colo. 2007) (denying access to a financial database on the grounds that the defendants were equally capable of exploring inconsistencies in the government's exhibits).

33 Kara Spak, *Defense in Brown's Chicken Case Gets DNA Access*, CHI. DAILY HERALD, Aug. 15, 2006, at 13. *See also* Jason Felch & Maura Dolan, *Crime Labs Finding Questionable DNA Matches*, SFGATE.COM (Aug. 3, 2008), http://www.sfgate.com/news/article/crime-labs-finding-questionable-DNA-matches-3274788.php.

nonarbitrary use of existing state postconviction discovery procedures.[34] Jurisdictions may decide to offer more expansive postconviction discovery procedures. Indeed, jurisdictions have become notably more open to development of potential new, postconviction evidence of innocence. In response to the advent of DNA testing, and over the past two decades, every state, the District of Columbia, and the federal government have passed a statute to permit newly discovered evidence of innocence motions and access to testing.[35] Whether a similar legislative change will occur in reaction to digital evidence remains to be seen. Perhaps it will depend on the degree to which digital evidence produces clear-cut evidence of innocence in sufficient numbers of cases. Moreover, discovery and postconviction remedies more generally may be waived or otherwise unavailable in the vast majority of criminal cases that are resolved through plea bargains.[36]

For the typically more serious cases in which federal habeas review is an option, federal habeas corpus, as Professors Fairfield and Luna describe, is a procedural minefield. Perhaps animated by underlying due process concerns with preserving an avenue for judicial review to those who may be factually innocent, a range of exceptions to those procedural barriers exist when an inmate provides certain types of new evidence of innocence.[37] The Supreme Court recognized in *McQuiggin v. Perkins* that the AEDPA statute of limitations does not rule out a preexisting, well-recognized miscarriage-of-justice exception to such procedural strictures.[38] In *McQuiggin*, the Court followed prior rulings creating an innocence "gateway" to other procedural restrictions (in contrast, the AEDPA's second and successive petition provisions codify a far more narrow innocence exception).[39]

The postconviction remedies available in the states may be far more important for the vast majority of prisoners. States that have generic newly discovered evidence-of-innocence statutes may be currently more receptive to such claims. States may over time add categories of digital evidence as enumerated topics for discovery or relief to their

---

34 Dist. Attorney's Office v. Osborne, 557 U.S. 52, 68–70 (2009). For a discussion of the case, see Brandon L. Garrett, *DNA and Due Process*, 78 FORDHAM L. REV. 2919 (2010).

35 For a description of the statutes in all fifty states, see *Access to Post-conviction DNA Testing*, INNOCENCE PROJECT, http://www.innocenceproject.org/Content/Access_To_PostConviction_DNA_Testing.php (last visited Aug. 4, 2014).

36 For an excellent overview, see Rebecca Stephens, *Disparities in Postconviction Remedies for Those Who Plead Guilty and Those Convicted at Trial: A Survey of State Statutes and Recommendations for Reform*, 103 J. CRIM L. & CRIMINOLOGY 309, 315–18 (2013).

37 Brandon L. Garrett, *Habeas Corpus and Due Process*, 98 CORNELL L. REV. 47, 118 (2012).

38 133 S. Ct. 1924, 1931 (2013).

39 *See, e.g.*, House v. Bell, 547 U.S. 518, 539 (2006) (holding that the innocence gateway to a procedural-bar rule does not require a showing of clear error).

postconviction statutes. Or some may adopt digital evidence—specific statutes, like Texas did by adopting a postconviction statute permitting a claim to be brought regarding scientific evidence that was not available at the time of trial or that contradicts scientific evidence relied upon by the state.[40] However, where postconviction relief may turn on judicial assessments of whether new evidence, taken along with the other evidence in the case as a whole, sufficiently affects what a reasonable fact-finder might decide, the ability to obtain relief based on digital evidence will turn on how much weight judges place on it. How judges assess the weight of various types of digital evidence may be an important topic for study in the years to come.

## IV
## DIGITAL *STRICKLAND*

Ineffective assistance of counsel claims, brought under the standard announced by the Supreme Court in *Strickland v. Washington*, are the most commonly brought postconviction claims.[41] While habeas relief of any kind is fairly rare, such claims are more successful than most.[42] As a result, perhaps more so than *Brady* claims, we may see going forward more claims that trial lawyers failed to adequately investigate the existence of digital evidence or obtain discovery from third parties and introduce digital evidence. For some types of evidence, such as the defendant's own social-media or geolocation data, that information can be readily obtained or requested by the defense. Courts will then have to rule on what the obligations of reasonably effective or diligent defense lawyers are to understand, investigate, and obtain digital evidence. Those professional standards may evolve over time, for all of the reasons Professors Fairfield and Luna describe, just as standards for adequate representation have evolved concerning subjects such as collateral consequences of conviction and representation during the sentencing phase of criminal trials.[43]

## CONCLUSION

The physical and virtual worlds now overlap. Electronic information can be generated constantly, tracking communications, a

---

40 *See* TEX. CODE CRIM. PROC. art. 11.073 (2013).

41 VICTOR E. FLANGO, NAT'L CTR. FOR STATE COURTS, HABEAS CORPUS IN STATE AND FEDERAL COURTS 45 (1994).

42 NANCY J. KING ET AL., NAT'L CTR. FOR STATE COURTS, FINAL TECHNICAL REPORT: HABEAS LITIGATION IN U.S. DISTRICT COURTS 28 (2007); *see also* FLANGO, *supra* note 40, at 46–47 (stating that ineffective assistance of counsel claims present the only avenue for a petitioner to argue new evidence or issues not raised at trial).

43 For example, the American Bar Association recently released an ethics opinion concerning using social media to research potential jurors; perhaps over time it would be considered ineffective to fail to conduct such digital investigations. ABA Comm. on Ethics & Prof'l Responsibility, Formal Op. 466 (2014).

person's location, appearance, and a wide range of other information. Professors Fairfield and Luna make an important contribution by analyzing not only how this provides powerful electronic tools to law enforcement to prove guilt as well as raises privacy concerns but also how this data can sometimes prove innocence. Yet there are powerful practical, evidentiary, statutory, regulatory, and institutional obstacles towards its discovery. As the government relies on new forms of digital evidence, it will have to disclose more potentially exculpatory evidence to the defense and more information about the reliability of the evidence upon which it is relying. Just as the meaning of the general due process right to a fair trial will evolve in the digital age, so will standards governing police and prosecutorial discovery obligations and minimally adequate defense representation. The criminal rules of discovery, both pretrial and postconviction, will inevitably adapt to our increasingly digital world.