

U.C.L.A. Law Review

Big Data Prosecution and *Brady*

Andrew Guthrie Ferguson

ABSTRACT

Prosecutors are joining the big data revolution, adopting “intelligence-driven” strategies to target crime patterns. Structured and unstructured datasets are collecting information to track offenders, places, and groups, allowing prosecutors to link crimes by time, location, associations, or other connections. But as powerful as these new forms of centralized data systems might be for investigators, there remains a critical open issue: the systems were not designed to identify the exculpatory and impeaching material prosecutors are required to disclose under *Brady v. Maryland*. This Article examines the design flaw at the core of the intelligence-driven prosecution model—a flaw that creates a due process problem that threatens to undermine this innovation. The Article also explores how big data prosecution necessitates a new theory of *Brady* and suggests a way to engineer a theoretical and technological solution to current *Brady* practice consistent with due process principles.

AUTHOR

Visiting Professor of Law, American University Washington College of Law; Professor of Law, UDC David A. Clarke School of Law. Thank you to Jeff Bellin, Barry Friedman, David O’Keefe, and Barry Scheck for helpful comments on earlier drafts.

TABLE OF CONTENTS

INTRODUCTION.....	182
I. BIG DATA PROSECUTION	185
A. Intelligence-Driven Prosecution: Structured Big Data	187
1. The Strategy of Intelligence-Driven Prosecution.....	189
2. The Technology of Intelligence-Driven Prosecution	193
a. Data About Active Cases	194
b. Data About Uncharged Crimes.....	196
c. Data About Places of Criminal Activity.....	199
d. Data About Priority Offenders.....	200
e. Data About Criminal Networks	206



f. Data About Probationers/Parolees	207
3. Centralized Big Data Prosecution	208
B. Big Data Surveillance: Unstructured Big Data.....	209
1. Unstructured Video Surveillance	210
2. Unstructured Sensor Data	213
3. Structuring Unstructured Data.....	215
II. THE DESIGN PROBLEM: HOW THE <i>BRADY</i> DOCTRINE FITS BIG DATA	
PROSECUTION SYSTEMS.....	217
A. <i>Brady</i> Basics.....	218
B. The Content of Required <i>Brady</i> Disclosures	219
1. Eyewitnesses.....	220
a. Eyewitnesses and <i>Brady</i>	220
b. Eyewitness Information in Intelligence-Driven Prosecution Systems.....	221
2. Motive/Bias	224
a. <i>Brady</i> and Motive-Bias Evidence.....	224
b. Motive/Bias in Intelligence-Driven Systems	226
3. Capacity	228
a. Capacity and <i>Brady</i>	228
b. Capacity in Structured Big Data Systems	229
4. Credibility.....	230
a. Credibility and <i>Brady</i>	230
b. Credibility Markers in Intelligence-Driven Systems.....	232
5. Exculpatory Facts.....	234
a. Exculpatory Facts and <i>Brady</i>	235
b. Exculpatory Facts in Intelligence-Driven Systems.....	236
C. <i>Brady</i> 's Structural Weaknesses	238
D. The Duty of Disclosure	241
III. REENGINEERING INTELLIGENCE-DRIVEN <i>BRADY</i>	243
A. Theory: Networked <i>Brady</i>	244
1. Relational Understanding.....	244
2. Quantitative Understanding.....	245
3. Qualitative Understanding.....	246
4. Proactive Understanding	246
B. Technology: Incorporating Networked <i>Brady</i> by Design	247
1. Flags—Inputting <i>Brady</i>	248
a. Reliability Flags: Credibility	249
b. Associational Flags: Links	251
c. Category Flags: Patterns.....	251
2. Intelligence-Driven Checks: Filling <i>Brady</i> 's Gaps.....	253
3. A <i>Brady</i> Button	254
CONCLUSION	255

INTRODUCTION

Prosecutor offices are going digital.¹ Paper files are being uploaded to the cloud. Big data systems hold vast streams of investigative clues, useful for prosecuting completed crimes and monitoring crime patterns across a city.² Attempts to create seamless law enforcement information-sharing capabilities and proactive prosecutions necessitate new forms of information collection and storage.³ An “intelligence-driven prosecution” model is being promoted nationally as the future of prosecution.⁴

This change in prosecution involves both a shift in technology and strategy. New digital technologies link disparate sources of information into a centralized investigative system.⁵ These big data prosecution tools facilitate evidence collection and information sharing, offering the ability to identify suspects by time, place, associations, or other connections.⁶ Adding to these types of formalized, structured databases are growing sources of raw, unstructured big data from digital surveillance technologies like video cameras, police body cameras, and

-
1. See Andrew Guthrie Ferguson, *Predictive Prosecution*, 51 WAKE FOREST L. REV. 705, 716 (2016).
 2. See, e.g., JENNIFER A. TALLON ET AL., CTR. FOR COURT INNOVATION, THE INTELLIGENCE-DRIVEN PROSECUTION MODEL: A CASE STUDY IN THE NEW YORK COUNTY DISTRICT ATTORNEY'S OFFICE 5 (2016) https://www.courtinnovation.org/sites/default/files/documents/IDPM_Research_Report_FINAL.PDF [<https://perma.cc/25LC-JXST>] (evaluating the Manhattan District Attorney's Intelligence-Driven Prosecution model,).
 3. See MANHATTAN DISTRICT ATT'Y'S OFFICE, MODELS FOR INNOVATION: THE MANHATTAN DISTRICT ATTORNEY'S OFFICE 2010–2018, at 19 (2018) [hereinafter MODELS FOR INNOVATION], <https://www.manhattanda.org/wp-content/uploads/2018/03/Models-For-Innovation-Report-1.pdf> [<https://perma.cc/W7FK-YUF5>] (“Using a method called intelligence-driven prosecution (IDP), [the Crime Strategies Unit] leverages crime data and deep community ties to develop a clear understanding of both the nature of criminal activity and the individuals committing these offenses.” (footnote omitted)).
 4. See Chip Brown, *Cyrus Vance Jr.'s 'Moneyball' Approach to Crime*, N.Y. TIMES MAG. (Dec. 3, 2014), <https://www.nytimes.com/2014/12/07/magazine/cyrus-vance-jrs-moneyball-approach-to-crime.html> [<https://perma.cc/5DER-F6VJ>].
 5. See Conor Skelding, *Cy Vance on '21st Century Crime-Fighting'*, POLITICO (June 10, 2014, 11:45 AM), <https://www.politico.com/states/new-york/city-hall/story/2014/06/cy-vance-on-21st-century-crime-fighting-013554> [<https://perma.cc/UWR7-NPYG>] (“Like CompStat, the Crime Strategies Unit identifies the crime-drivers and crime hotspots. . . . But that's just the beginning. C.S.U. collects, connects, and analyzes that, and other data, from seemingly unrelated cases. It makes sense of the enormous data that comes into our office and creates actionable intelligence.” (quoting Manhattan District Attorney Cyrus Vance)).
 6. *Id.*; see also Heather Mac Donald, Opinion, *First Came Data-Driven Policing. Now Comes Data-Driven Prosecutions.*, L.A. TIMES (Aug. 8, 2014, 8:24 PM), <https://www.latimes.com/opinion/op-ed/la-oe-mac-donald-prosecutor-data-20140810-story.html> [<https://perma.cc/YD4W-PEBK>].

automated license plate readers (ALPRs).⁷ Prosecutors now sit on a wealth of valuable investigative insights—all searchable and potentially relevant for intelligence gathering and criminal prosecution.

But as helpful as these new forms of data collection might be to reorganize prosecution priorities, there remains a critical open question: how can these centralized big data systems be engineered to identify exculpatory and impeaching material that prosecutors are required to disclose under *Brady v. Maryland*?⁸ The question remains unanswered and presents a due process problem that threatens to undermine the constitutional fidelity of intelligence-driven prosecution systems.⁹

This Article explores the *Brady* problem in big data prosecution.¹⁰ While prosecutors' offices, like the rest of the professional world, are beginning to embrace a data-driven future, these systems have not been engineered to identify exculpatory or impeaching evidence for the defense. And—to put it starkly—the resulting design gap threatens the legitimacy of the criminal justice system because it risks creating systemic and structural due process violations. Without the ability to flag or find evidence required to be turned over to the defense, the big data systems—and, thus, the prosecutors—will constructively possess relevant *Brady* material without the ability to provide this information to the defense.¹¹

This *Brady* problem arises from a fundamental shift in prosecution theory. In an effort to adopt data-driven or intelligence-driven prosecution strategies, prosecutors' offices are reorienting themselves to be proactive intelligence-gathering entities.¹² This shift involves data collection and providing a way to

7. See Sarah Brayne, *The Criminal Law and Law Enforcement Implications of Big Data*, 14 ANN. REV. L. & SOC. SCI. 293, 299–301 (2018); Kristine Hamann, *Police Body-Worn Cameras: What Prosecutors Need to Know*, PROSECUTOR J. NAT'L DISTRICT ATT'YS ASS'N, Sept. 2017, at 22.

8. *Brady v. Maryland*, 373 U.S. 83, 87 (1963) (“We now hold that the suppression by the prosecution of evidence favorable to an accused upon request violates due process where the evidence is material either to guilt or to punishment, irrespective of the good faith or bad faith of the prosecution.”).

9. See Miriam H. Baer, *Timing Brady*, 115 COLUM. L. REV. 1, 4 (2015) (“Derived from the due process clauses of the Fifth and Fourteenth Amendments, *Brady* and its progeny require prosecutors to disclose material, exculpatory evidence in time for use at trial or sentencing.”).

10. See Brandon L. Garrett, *Big Data and Due Process*, 99 CORNELL L. REV. ONLINE 207, 211–13 (2014) (discussing the concept of due process rights to digital discovery under *Brady* in the context of a response essay to Joshua A.T. Fairfield & Erik Luna, *Digital Innocence*, 99 CORNELL L. REV. 981 (2014)).

11. See *infra* Part II.

12. See generally David Alan Sklansky, *The Nature and Function of Prosecutorial Power*, 106 J. CRIM. L. & CRIMINOLOGY 473, 510–20 (2016) (discussing prosecutorial reform); cf. KRISTINE HAMANN & LAURA GREENBERG-CHAO, PROSECUTORS' CTR. FOR EXCELLENCE, *THE PROSECUTOR'S EVOLVING ROLE: SEEKING JUSTICE THROUGH COMMUNITY PARTNERSHIPS AND INNOVATION 1* (2016), <https://pceinc.org/wp-content/uploads/2019/11/20170108-The-Prosecutors-Evolving->

share that information across jurisdictions.¹³ In addition, through a host of technologically enhanced information gathering strategies, prosecutors are proactively targeting places and people thought to be responsible for criminal acts and attempting, preemptively, to incapacitate them through aggressive prosecution strategies.¹⁴ Prosecutors are no longer merely reactive, thinking of cases as simply responses to discrete factual scenarios, but rather are viewing them more often as predictable patterns connected by geography, group association, and across time.¹⁵ The goal has been to widen the aperture of prosecution to understand how individual criminal actors influence crime patterns across geographic locations, groups, and in relation to others in the community.

Yet, while an intelligence-driven theory has expanded the focus for how prosecutors see cases, it has not expanded the focus for how prosecutors see *Brady* material. This is so even though the same contextual relationships of known crime areas, rival gangs, and reciprocal violent incidents across time should also increase the availability of potentially impeaching or exculpatory evidence.¹⁶ This Article argues that by looking at the *Brady* doctrine through the lens of intelligence-driven prosecution, a new and much stronger theory of *Brady* can emerge.

Part I of this Article explores the growth of new big data prosecution systems. The main idea behind intelligence-driven prosecution is that data can identify the particular places and specific people who are driving up crime rates, allowing for targeted interventions to remove those problem actors from those communities.¹⁷ The operational information for this strategy is located in ever-growing structured big data systems.¹⁸ In addition, a related type of design problem arises from unstructured datasets, such as those now being created by the daily footage from police body cameras or other sensor tracking surveillance technologies.¹⁹ Vast collections of data are held by law enforcement and third parties to be used by

Role-Seeking-Justice-Through-Community-Partnerships-and-Innovation-Prosecutors-Center-for-Excellence-1.pdf [https://perma.cc/L8GP-LW4E] (“Traditionally, a prosecutor’s role was a limited and relatively passive one—to evaluate and prosecute arrests made by the police.”).

13. See Fairfield & Luna, *supra* note 10, at 1032–43 (discussing the problem of providing exculpatory evidence in the context of mass surveillance technologies).

14. See *infra* Part I.

15. See David O’Keefe, *Head of the Manhattan District Attorney’s Crime Strategies Unit*, CTR. FOR CT. INNOVATION (Sept. 2013), <https://www.courtinnovation.org/publications/david-okeefe-head-manhattan-district-attorneys-crime-strategies-unit> [https://perma.cc/GY2R-FEX9] [hereinafter O’Keefe Interview] (“It used to be we only went where the cases took us. Now, we can build cases around specific crime problems that communities are grappling with.”).

16. See *infra* Part I.

17. See *infra* notes 105–110.

18. See *infra* Part II.

19. See *infra* Subpart I.B.

prosecutors.²⁰ But that same government-controlled dataset may also contain exculpatory information without any efficient way to locate the information prosecutors have a duty to disclose.²¹

Part II of the Article examines the complexity of applying the *Brady* doctrine to big data prosecution systems. The simple constitutional principle that prosecutors must turn over exculpatory or impeaching evidence has never been simple in practice.²² This Part explores what the commands of *Brady* might mean when thinking about an expanding digital system of interconnected evidence.

Part III then offers a framework to reengineer the *Brady* puzzle being created by big data prosecution systems. This Part offers a practical redesign of how *Brady* material can be identified in big data systems, focusing on input flags and social network analysis that incorporate *Brady* by design. Such a technical redesign builds off an alternative theoretical understanding of the *Brady* doctrine—an understanding that looks at *Brady* as more relational, incorporating a broader range of variables across larger groups, wider time horizons, and within a contextual understanding of crime patterns. As will be demonstrated, the move away from a reactive, case-based approach to prosecution toward a more networked, intelligence-driven approach also necessitates a move toward a more proactive, networked understanding of the *Brady* doctrine.

I. BIG DATA PROSECUTION

Prosecutors have always been in the information business. A myriad of information sources from police officers, witnesses, experts, and colleagues enters the prosecution office every day. The traditional visualization of that data overload can be seen in the piles of paper, transcripts, sticky notes, reports, motions, briefs, cases, medical records, and handwritten comments that build up in prosecutors' offices and end up in file cabinets (real and virtual). But, those prosecution-created or collected documents only account for a portion of the information supporting

20. Ferguson, *supra* note 1, at 720.

21. See *infra* Subpart I.B.1.

22. See Bennett L. Gershman, *Litigating Brady v. Maryland: Games Prosecutors Play*, 57 CASE W. RES. L. REV. 531, 534 (2007) (“*Brady* is enforced by the judiciary through widely inconsistent approaches as to what constitutes *Brady* evidence, the specific types of information required to be disclosed, when it must be disclosed, and the sanctions for noncompliance. In addition, given the various enforcement protocols of different prosecutors’ offices, and even of individual prosecutors in the same office, it is virtually impossible to identify clear and consistent norms of compliance by prosecutors as to what evidence is required to be disclosed, when it must be disclosed, and permissible reasons for noncompliance.” (footnotes omitted)).

the prosecution team.²³ In addition, police departments have their own files, as do probation and parole officers, experts, and quasi-law enforcement agencies, and all of it exists in an organized but fragmented context.

Prosecutors, like other professionals, have come to understand that efficiencies and insights can be gained by centralizing and sharing that information.²⁴ In fact, in offices inspired by “intelligence-driven prosecution” strategies, this push to share data has led to a revolution in how local prosecutions organize their efforts.²⁵ This Part explores the rise of intelligence-driven prosecution as an example of a data-centered prosecution strategy. While focused on the leading intelligence-driven prosecution office in the country, the Manhattan District Attorney’s Office (Manhattan DA), the analysis holds lessons for other big data prosecution systems developing in other jurisdictions.²⁶

This Part first explores the structured data collection systems used in intelligence-driven systems, and then shows how those same data points will soon be at issue in larger unstructured data collection systems (like police body camera videos or sensor data). While the search capabilities for these unstructured policing systems do not quite exist (yet), the technology does, and these capabilities will soon create constitutional questions for prosecutors.²⁷

23. Hilary Oran, Note, *Does Brady Have Byte? Adapting Constitutional Disclosure for the Digital Age*, 50 COLUM. J.L. & SOC. PROBS. 97, 99 (2016) (discussing the problems of massive electronic discovery cases and *Brady*).

24. See TALLON ET AL., *supra* note 2, at 1 (“Intelligence-driven prosecution represents a novel prosecutorial strategy rooted in the rigorous collection of background information about the people, places, and problems driving crime in specific neighborhoods. Through improved information gathering on the role of criminal suspects within local criminal enterprises, the prosecutor’s office intends to facilitate more informed prosecutorial decision-making.”); see also Neil M. Richards, *The Dangers of Surveillance*, 126 HARV. L. REV. 1934, 1939 (2013) (“Big Data is notable not just because of the amount of personal information that can be processed, but because of the ways data in one area can be linked to other areas and analyzed to produce new inferences and findings.”).

25. See MODELS FOR INNOVATION, *supra* note 3, at 19; N.Y. COUNTY DISTRICT ATT’Y, INTELLIGENCE-DRIVEN PROSECUTION: AN IMPLEMENTATION GUIDE 4 (2015) [hereinafter IMPLEMENTATION GUIDE], <https://pceinc.org/wp-content/uploads/2015/06/Reducing-Crime-Intelligence-Driven-Prosecution-An-Implementation-Guide.pdf> [<https://perma.cc/UFT2-K5AH>] (“To appropriately target priority offenders for aggressive prosecution, a prosecutor’s office should develop an internal structure to gather, organize and make accessible intelligence regarding criminals and their activities.”).

26. See Ferguson, *supra* note 1, at 708 (noting the existence of predictive law enforcement programs beyond New York City in “Los Angeles, . . . Chicago, Philadelphia, Miami, Seattle, Kansas City, and Memphis, and smaller cities like Reading, Pennsylvania and Alhambra, California.” (footnote omitted)).

27. See *infra* Part II.

A. Intelligence-Driven Prosecution: Structured Big Data

Intelligence-driven prosecution developed in Manhattan under the leadership of District Attorney Cyrus Vance Jr.²⁸ In 2010, the Manhattan DA's office established the first Crime Strategies Unit (CSU) to develop an "Intelligence-Driven Prosecution Model."²⁹ Due to the large number of cases processed every year in Manhattan (more than 100,000), the larger number of people in the criminal justice system, and the hundreds of Assistant District Attorneys who worked the cases, the original idea was to try to break out of a reactive prosecution model to proactively understand crime patterns and prioritize resources in higher risk areas and with higher risk individuals.³⁰

By identifying risky people, the theory was that prosecutors could get smarter about who should be targeted, reducing overall arrests while nevertheless incapacitating the crime-drivers in an area.³¹ A combination of human intelligence (gang detectives and community members) and surveillance technologies (social network analysis and other digital tracking) all quantified into charts, maps, and predictive analytics now allows prosecutors to proactively target the criminal threats identified.³² In addition, D.A. Vance promised to develop "a

28. See Brown, *supra* note 4.

29. TALLON ET AL., *supra* note 2, at 5; Jason Kreag, *Prosecutorial Analysis*, 94 WASH. U. L. REV. 771, 788 (2017) ("The changes instituted by Manhattan District Attorney Cy Vance exemplify how policy changes can happen quickly on the prosecution side. When Vance took office in 2010, he prioritized incorporating analytics into prosecutorial decisions. Vance created the Crime Strategies Unit to develop 'intelligence-driven prosecution' techniques." (footnotes omitted)).

30. See HAMANN & GREENBERG-CHAO, *supra* note 12, at 26 ("Traditionally, case-focused prosecution has been relatively self-contained, in that prosecutors are primarily reactive to an arrest and focus on the investigation of that particular case. In contrast, crimes strategies units (CSUs) across the country have significantly broadened the prosecutor's traditional focus to include analyzing community concerns about crime, identifying crime trends and the people who are the crime-drivers and coordinating with other prosecutors and law enforcement partners."); TALLON ET AL., *supra* note 2, at 5 ("[The Manhattan District Attorney's Office (Manhattan DA)] created [the Intelligence-Driven Prosecution Model (IDPM)] to solve the inherent difficulties of informed decision-making in a large prosecutorial office. Specifically, [Manhattan DA] employs more than 500 ADAs and handles more than 100,000 cases each year, making it one of the largest prosecutor's offices in the country.").

31. See David O'Keefe, *Innovations in Prosecution and Research: Intelligence-Driven Prosecution*, TRANSLATIONAL CRIMINOLOGY, Spring 2013, at 6, <http://cebcp.org/wp-content/TCmagazine/TC4-Spring2013> [<https://perma.cc/79ES-G7R5>]; IMPLEMENTATION GUIDE, *supra* note 25, at 4 ("An Intelligence-driven Prosecution model requires prosecutors to (i) understand the crime issues facing their communities, from violent crimes to quality-of-life issues, and (ii) identify which defendants disproportionately drive those crimes.").

32. Mac Donald, *supra* note 6 ("The unit has compiled a database of Manhattan's most significant criminal players—now numbering about 9,000—whose arrest anywhere in the city immediately triggers an alert to one of the Crime Strategies Unit attorneys. The attorney will then contact the local prosecutor who has been assigned the case—whether in Manhattan or another borough—

seamless web” of information sharing capabilities between the Manhattan DA and the New York Police Department (NYPD).³³ All of the collected police data would be shared to give line prosecutors a better understanding of the defendants appearing before them in court in almost real time.

This “Moneyball” approach to crimefighting drew national media attention and academic support.³⁴ In no small part due to the Manhattan DA’s influence among prosecutors’ offices generally, intelligence-led prosecution has become a national phenomenon, changing prosecution tactics in California,³⁵ Delaware,³⁶

to make sure the defendant is prosecuted to the full extent of the law rather than slipping through the cracks.”).

33. See James C. McKinley Jr., *In Unusual Collaboration, Police and Prosecutors Team Up to Reduce Crime*, N.Y. TIMES (June 4, 2014), <https://www.nytimes.com/2014/06/05/nyregion/in-unusually-close-partnership-police-dept-and-district-attorney-team-up-to-reduce-crime.html> [https://perma.cc/5L3J-5VDU] (“As part of a template for relations between the two agencies, the district attorney’s office will provide the police with more than \$20 million from drug forfeiture cases to pay for new technology. That money will go for security cameras, fiber-optic information systems and hand-held tablets that will feed police officers data about suspects, Mr. Bratton said. The Police Department, in turn, will provide the district attorney’s Crime Strategies Unit access to more of the data it collects not only on reported crimes but also on suspects, Mr. Bratton said. He called the new approach ‘extreme collaboration’ and illustrated it by clasping his hands together.”); see also IMPLEMENTATION GUIDE, *supra* note 25, at 17 (“The automated arrest alerts are emailed to registered users. NYPD officers who have an interest in a particular target or group or subgroup can be subscribed to the alerts by providing a verifiable email address. For example, NYPD Gang Unit officers may subscribe to arrest alerts of gang members. And, precinct commanders and Field Intelligence Officers can subscribe to targets identified in the Arrest Alert System as priorities for a precinct.”).
34. See Brown, *supra* note 4; *infra* notes 38, 40; see also Press Release, Manhattan Dist. Attorney’s Office, Manhattan DA’s Office, John Jay College of Criminal Justice, and Institute for Innovation in Prosecution Host Symposium on Intelligence-Driven Prosecution (June 3, 2016), <https://www.manhattanda.org/manhattan-das-office-john-jay-college-criminal-justice-and-institute-innovation-prose> [https://perma.cc/79Z3-ZRY2].
35. See *SF District Attorney Takes Crime Reduction into Neighborhoods*, S.F. EXAMINER (Jan. 18, 2015), <https://www.sfexaminer.com/news/sf-district-attorney-takes-crime-reduction-into-neighborhoods> [https://perma.cc/RL2Q-PKA2].
36. See Press Release, Del. Dep’t Justice, Biden: New Crime Strategies Unit Will Prevent Crime on Local Level (May 19, 2014), <https://news.delaware.gov/2014/05/19/biden-new-crime-strategies-unit-will-prevent-crime-on-local-level-expand-on-past-success-of-attorney-generals-program-that-shuts-down-crime-infested-properties> [https://perma.cc/KH3T-NRG5].

Louisiana,³⁷ Missouri,³⁸ Illinois,³⁹ and potentially many more jurisdictions.⁴⁰ Annual national symposia have been hosted by the Manhattan DA in conjunction with John Jay College of Criminal Justice to promote the model.⁴¹ National grants have funded pilot programs, and the “intelligence-driven” idea is growing in popularity as it offers a mixture of smart-on-crime policies, new technology, and a claim to “innovation” when many are looking for fresh solutions to an oft-criticized criminal justice system.

1. The Strategy of Intelligence-Driven Prosecution

The strategy behind intelligence-driven prosecution is pretty straightforward: prosecutors focus on intelligence gathering in order to prioritize resources and proactively target human crime drivers in a community.⁴² The idea is to gather better information and use technology to develop better connections so prosecutors can more aggressively respond to identified crime patterns and problems.⁴³

-
37. See U.S. Attorney’s Office Middle Dist. of La., *New Baton Rouge Crime Strategies Unit Announced*, U.S. DEP’T JUST. (Sept. 23, 2015), <https://www.justice.gov/usao-mdla/new-baton-rouge-crime-strategies-unit-announced> [<https://perma.cc/L5YL-954C>].
 38. See St. Louis Post-Dispatch, *St. Louis, Mo., Crime Strategies Unit Uses ‘Moneyball’ Crime Fighting*, GOV’T TECH. (June 29, 2015), <http://www.govtech.com/public-safety/St-Louis-Mo-Crime-Strategies-Unit-Uses-Moneyball-Crime-Fighting.html> [<https://perma.cc/3U2W-EM26>].
 39. See *Crime Strategies Taskforce*, COOK COUNTY STATE’S ATT’Y, <https://www.cookcountystatesattorney.org/crime-strategies-taskforce> [<https://perma.cc/9AMR-FPE2>] (last visited Oct. 21, 2019).
 40. See Emily Lane, *Baton Rouge Law Enforcement Adopting NYC’s ‘Moneyball’ Approach to Crime*, TIMES-PICAYUNE (Sept. 3, 2015, 3:09 PM), https://web.archive.org/web/20150904002725/http://www.nola.com/news/baton-rouge/index.ssf/2015/09/baton_rouge_moneyball_crime_hi.html [<https://perma.cc/2EGW-UGXY>].
 41. *IIP & Manhattan DA’s Office Host Symposium on Intelligence-Driven Prosecution*, JOHN JAY C. CRIM. JUST. (June 3, 2016), <https://www.jjay.cuny.edu/news/iip-manhattan-da-s-office-host-symposium-intelligence-driven-prosecution> [<https://perma.cc/C9UR-YKWG>]; Press Release, *supra* note 34.
 42. IMPLEMENTATION GUIDE, *supra* note 25, at 2 (“A key element of CSU’s mandate is to make more effective use of the vast amounts of information gleaned from the thousands of cases prosecuted each year by the Office. Previously, the information acquired through our investigations and prosecutions of street-crime cases was not centrally organized, or analyzed. CSU is finding innovative ways to make this information available throughout the Office, when and where it is needed.”); TALLON ET AL., *supra* note 2, at 13 (“CSU Area ADAs also requested each precinct commander identify 25 priority offenders. These priority offenders included individuals identified as crime drivers in each of the precincts, primarily drivers of violent crime and, to a lesser extent, quality-of-life issues. By prosecuting and incarcerating these individuals, [the Manhattan DA] believed it could improve community safety and quality of life.”).
 43. John Eligon, *Top Prosecutor Creates a Unit on Crime Trends*, N.Y. TIMES (May 24, 2010), <https://www.nytimes.com/2010/05/25/nyregion/25vance.html> [<https://perma.cc/S7TT->

In Manhattan, for example, the CSU sought to gain a granular understanding of localized crime patterns.⁴⁴ First, the entirety of Manhattan was divided into five geographic zones with a small team of prosecutors assigned to each area.⁴⁵ Then the CSU focused on figuring out crime at the precinct level. The lead CSU prosecutor began an intelligence gathering process which involved mapping crime patterns, tracking demographics, and identifying hot spots within each of the twenty-two police precincts.⁴⁶ Human intelligence about gangs or crews, community concerns, and local factors were cataloged in a violence timeline.⁴⁷ The result was to identify a historic pattern of violent acts or repetitive criminality all tied to geography. Each of the twenty-two precincts then generated a list of twenty-five primary targets (“priority offenders”), human beings who were thought to be most responsible for the criminal activity in the precinct.⁴⁸ These people were then targeted for incapacitation through aggressive prosecution tactics.⁴⁹ The theory was that by removing the crime drivers, overall crime levels would drop. The strategy—part data-driven and part human intelligence-driven—resulted in detailed digital maps of crimes, computer dossiers of suspects, and a

UBQQ] (“The Crime Strategies Unit will rely on a computer database developed by the district attorney’s office to allow prosecutors to draw parallels among cases, unearth crime patterns in particular areas and make more informed decisions on how to handle defendants . . .”); *The Right Choices*, *ECONOMIST* (June 20, 2015), <https://www.economist.com/briefing/2015/06/19/the-right-choices> [https://perma.cc/N99G-PHR9] (“Cy Vance, Manhattan’s district attorney, is a fan of what he calls intelligence-driven prosecution. Under his tutelage, a Crime Strategies Unit collects information on the most persistent criminals, which can inform prosecutors even if it does not form part of the case. ‘If I know someone who is involved in shootings or violence, even if he is arrested for shoplifting, I want to charge it as aggressively as possible,’ says Mr. Vance.”).

44. See O’Keefe Interview, *supra* note 15 (“Working with our partners in the precincts, we also identified hot spots and the names of the people committing the most crimes in each area.”).

45. TALLON ET AL., *supra* note 2, at 8 fig.1.1, 12.

46. *Id.* at 13–14.

47. IMPLEMENTATION GUIDE, *supra* note 25, at 23 (“CSU creates and maintains violence timelines in areas where there are patterns of violence or a history of ongoing violence. These timelines can list violence geographically, setting forth the violence in a specific precinct, neighborhood, or housing development. [Violence timelines] can also be based on the gangs or groups committing the violence. These timelines include information about the event: date, time, location, and a brief synopsis of the event, as well as the details regarding the individuals involved or believed to be involved, including suspects, defendants, victims, and witnesses. The facts provided about the individuals include name, NYSID, DOB (including age at the time of incident) and gang affiliation, if known.”).

48. Brown, *supra* note 4 (“They asked police commanders to submit a list of each precinct’s 25 worst offenders—so-called crime drivers, whose ‘incapacitation by the criminal-justice system would have a positive impact on the community’s safety.’ Seeded with these initial cases, the C.S.U. built a searchable database that now includes more than 9,000 chronic offenders, virtually all of whom have criminal records.”).

49. *Id.*

better understanding of the links between the places, people, and patterns of criminal activity in localized areas.⁵⁰

In addition to geographic and human targeting, the Manhattan DA also organized thirty-three Bureau-Based Projects (BBPs) which focused on particular crimes (for example, narcotics, grand larceny) or particular gangs in the city.⁵¹ These BBP teams involved a small group of prosecutors to specialize in the particular types of crime or groups at issue.⁵² Again, like the precinct level studies, intelligence about types of crime allowed a targeting of individuals engaged in repetitive acts of particular criminal activity.

In San Francisco, District Attorney George Gascón adopted a similar intelligence-driven approach to prosecution.⁵³ With the assistance of a Federal Bureau of Justice Assistance (BJA) grant, the San Francisco DA's office partially reorganized into a CSU model.⁵⁴ While not as expansive a program as Manhattan's, the goal of studying crime patterns to target higher risk areas and individuals became the focus. As DA Gascón explained:

Traditionally, prosecutors have approached crime one case at a time. However, this approach doesn't make sense when we know that crime is not driven by a series of isolated incidents, but rather tends to concentrate across individuals and locations. In San Francisco, just 5 percent of offenders are responsible for 25 percent of crime. Less than one percent of street segments have driven a huge increase in burglaries from automobiles, making it one of the largest crime problems in San Francisco. Nearly 60 percent of homicides occur in known gun violence hot spots. After learning of the success of District Attorney Cyrus Vance's Crime Strategies Unit (CSU) in New York, I established a CSU in 2014 to take advantage of innovations in data science and

50. See IMPLEMENTATION GUIDE, *supra* note 25, at 2 ("Gathering information about criminal activity and identifying those who disproportionately drive crime is of limited use, unless we are alerted to a priority target's arrest and are prepared to respond appropriately. The challenge faced by prosecutors' offices, especially urban ones, is being informed at the earliest stage of a prosecution as to the importance of a particular defendant in wider criminal activity. In some cases, the priority of a defendant will be clear based on the number of arrests and convictions appearing on the rap sheet. However, key information frequently is not apparent in a defendant's prior criminal history but consists of knowledge that a defendant is, for example, the leader of a violent gang, a suspect in a shooting, or the main supplier of narcotics in a public housing development.").

51. See TALLON ET AL., *supra* note 2, at 16 ("DA Vance created thirty-three Bureau-Based Project Teams to investigate and prosecute specific crime areas (i.e. crime types, gangs, hot[s]pots, or 'projects') across the city.").

52. *Id.*

53. See CRAIG D. UCHIDA ET AL., A GUIDE FOR IMPLEMENTING A CRIME STRATEGIES UNIT: THE SAN FRANCISCO EXPERIENCE 3–6 (2017).

54. *Id.*

technology that now make it possible for prosecutors to be more strategic in determining what is driving crime, and to direct the resources of the San Francisco District Attorney's Office (SFDA) to those most responsible.⁵⁵

These techniques of targeted prosecution usually involve violent crime. In one of the most heavily promoted examples of intelligence-driven prosecution, the Manhattan DA's office brought a conspiracy case against 103 defendants in two separate neighborhoods.⁵⁶ These prosecutions involved extensive surveillance of social media, communications, and intelligence collection.⁵⁷ After months of investigating particular public housing complexes, police arrested dozens of individuals thought to be associated with violent criminal activity in one large takedown.⁵⁸ Over six years, 377 gang members have been indicted through these New York CSU investigatory methods.

While primarily focused on serious crime, the intelligence-driven method has also targeted quality of life crimes like transit fare evasion, pickpocketing, and counterfeit ticket sales.⁵⁹ Such targeting often identifies individuals who repeatedly break the law in minor ways and thus traditionally are not held to account, thereby minimizing the magnitude of their long-term criminality. In a Center for Court Innovation case study on the Manhattan Intelligence-Driven Prosecution model, prosecutors justified why and how the intelligence driven strategy was used to prosecute a subway fare evader:

Transit Recidivist: This case concerns a defendant who tampered with MetroCard machines in the subway (Criminal Tampering in the First Degree). CSU received a transit recidivist arrest alert and notified ECAB [Early Case Assessment Bureau]. Because CSU identified this defendant as a problem for nearly five years, prosecutors charged the case as a felony; without CSU's intervention, prosecutors would have

55. *Id.*

56. See Victoria Cavaliere, *More Than 100 Indicted in Harlem in Largest-Ever NYC Gang Bust*, REUTERS (June 4, 2014), <https://www.reuters.com/article/us-usa-crime-gangs/more-than-100-indicted-in-harlem-in-largest-ever-nyc-gang-bust-idUSKBN0EF1DQ20140604> [<https://perma.cc/2H8C-Q2UK>].

57. *Id.*; see also J. David Goodman, *Dozens of Gang Suspects Held in Raids in Manhattan*, N.Y. TIMES (June 4, 2014), <https://www.nytimes.com/2014/06/05/nyregion/dozens-of-suspected-gang-members-arrested-in-raid-of-2-harlem-housing-projects.html> [<https://perma.cc/2K32-BEVN>].

58. *Id.*

59. See TALLON ET AL., *supra* note 2, at 7, 13 ("While individuals on the [Arrest Alert System] are most often repeat offenders with serious and violent criminal history, priority offenders may also be quality-of-life recidivists."); IMPLEMENTATION GUIDE, *supra* note 25, at 21 ("Some of the issues addressed by BBPs in Manhattan included night club violence, pick-pockets, counterfeit ticket sellers and street scammers who prey on tourists.").

normally reduced the charge to a misdemeanor. The more aggressive charging may have contributed to a \$15,000 bail request (the judge ultimately set bail at \$5,000) and the defendant's eventual plea to a misdemeanor with a lengthy six-month jail sentence."⁶⁰

In addition to capturing a longer-term picture of criminal activity, intelligence-driven prosecution also supports broader sharing of information among more actors within the criminal justice system.⁶¹ In the Center for Court Innovation case study report, investigators interviewed one Crime Strategies Unit prosecutor who explained how the information sharing worked across jurisdictions:

A CSU ADA provided an example illustrating how efficient intelligence gathering can influence cases across the five boroughs. The ADA, following initial meetings with law enforcement and community contacts, identified two brothers as priority offenders associated with grand larcenies, robberies, and narcotics. Soon after Hurricane Sandy, CSU received an arrest alert indicating that the brothers had been arrested for trespassing in a business on Staten Island. The case was weak, however, because prosecutors could not prove why the brothers were in the store (possibly seeking shelter from the hurricane) or on Staten Island in the first place. At the time of the trespassing arrest, one of the brothers had an open case in special narcotics and CSU knew that his Facebook page was listed under his street narcotics name, information otherwise unavailable to an attorney unfamiliar with the offender. Prior to the hurricane, the offender posted on his Facebook page that, "I am going to Staten Island to get rich tonight." Within a matter of days, CSU coordinated with Staten Island DAs, who used the Facebook post to support a burglary case against the offender.⁶²

This broader strategic focus allowed prosecutors to see links between individuals and groups and more easily share relevant information about defendants, witnesses, and victims around the city. It was made possible by technological advancements discussed next.

2. The Technology of Intelligence-Driven Prosecution

Intelligence-driven prosecution has begun utilizing new data-driven technologies to assist with the need to collect and sort information about communities, crimes, and alleged criminals. The basic idea is to upload the

60. TALLON ET AL., *supra* note 2, at 31.

61. *See id.* at 19, 32.

62. *Id.* at 30.

disparate pieces of collected knowledge about criminal patterns into a single, centralized dataset that can be searched, mapped, and linked together to assist prosecutors in visualizing threats and investigating crimes.⁶³

Because there is no single accepted model of intelligence-driven prosecution at this early stage of development, this Subpart examines some of the possible technologies at a level of abstraction. While based on actual technologies and examples detailed in the Manhattan DA Crime Strategies Unit training materials,⁶⁴ the goal here is to show the general types of information that could be collected, incorporated, and shared throughout any prosecution system, and the wide variety of personal data that might exist at any one time in a big data prosecution system.

In simplified form, this Subpart looks at big data technologies that allow prosecutors to collect, sort, and link data about: (a) active cases; (b) uncharged crimes; (c) priority offenders; (d) places of criminal activity; (e) networks of criminal activity; and (f) individuals on probation or parole. In total, the information gathering systems attempt to capture the “who,” “what,” “where,” and “how” of criminal acts and patterns in a particular geographic area.

a. Data About Active Cases

Any prosecution-oriented data system must naturally focus on collecting information about criminal cases for prosecution. For decades in traditional systems, prosecutors kept handwritten casefiles with notes, documents, police forms, motions, and everything else associated with a case.⁶⁵ This physical casefile remains the standard default which accompanies the lawyer as she travels to court, the grand jury, the office, or wherever the information is needed. Reduced to physical form, the contents include paper, photographs, and some information about digital evidence that might be available.

63. See UCHIDA ET AL., *supra* note 53, at 4 (“Traditionally, DA’s offices have access to critical data sources but few engage in any attempts to examine the data beyond looking at it case by case. In this instance, CSU analysts have been hired to make use of the vast amounts of information available from different data sources. They employ analytic tools to assist prosecutors with investigations and prosecution. They use software that enables them to map crime, to link criminal offenders to associates, and to extract data for more complex analyses.”).

64. These training materials were posted as part of a 2018 Intelligence-Driven Prosecution Symposium held at John Jay College (copy on file with the author). The training was hosted by the Manhattan DA’s Office as part of a semiregular national training program. Many other prosecutors from other jurisdictions were in attendance learning about the technology available to develop intelligence-driven prosecution. *Id.*

65. See Mac Donald, *supra* note 6 (“Vital information about offender networks gleaned in the course of preparing a case for trial remains on a prosecutor’s legal pad without getting conveyed back to the police or to other prosecutors.”).

Like everything else in a digital world, this paper-based storage method has been replaced by digital equivalents. Information that once lived on the back of a casefile (and nowhere else) now lives on a computer server or in a connected cloud.⁶⁶ Case management systems are the unexciting backbone of this type of centralized system. They are neither very new nor very technologically sophisticated but do manage to centralize information about cases.

As an example, the Manhattan District Attorney's Office uses the "DANY Case Management" system to track active and closed cases in their system.⁶⁷ Like all data management systems, because information is inputted into structured fields, the different fields (name, sentence, charges, court hearings, case numbers, etc.) can be searched.⁶⁸ For prosecution offices, this data allows a supervisor to find all of the cases a particular ADA had as their responsibility or the status of each case.⁶⁹ In addition, upcoming court dates and other important details can be centralized for more efficient institutional organization. Information about defendants is collected, including information about the time and location of an arrest, what precinct and officers were involved, the type of charges, the witnesses (police and civilian), gang affiliations, 911 calls, and the basic facts of a case.⁷⁰

To be clear, establishing a data management system to replace paper files is not a big data innovation. Such a digital transition has been done more or less successfully by many traditional prosecution offices that have not subscribed to a belief in intelligence-driven prosecution. But the digitization of information does provide a centralized dataset about cases. If you imagine every criminal case over a period of five years as the recorded details of suspect names, witness names, times, locations, officer names, and crimes charged you can see that while the management of the data for individual cases might not reveal much that is new, the aggregated information will offer a source for revelatory datamining. The ability to see patterns within the data (types of crimes, rates of crimes, locations, gangs, etc.) are now observable by searching in the dataset.⁷¹ Further, this information can be mapped to visualize crime patterns and actors in the criminal justice system.

66. See IMPLEMENTATION GUIDE, *supra* note 25, at 2 ("Rather than information lost amid thousands of legal pads in the offices of hundreds of Assistant District Attorneys (ADAs), CSU gathers this information and converts it into useable criminal intelligence in the form of data maps, searchable databases, and meaningful arrest alerts.").

67. See *id.* at 39.

68. See *id.*

69. See *id.*

70. See *id.*

71. See Ferguson, *supra* note 1, at 720–21 ("Intelligence-driven prosecution is not just about being smarter, but developing actionable intelligence about crime patterns in an area. Finally, all of this information about past criminal activities is memorialized in a searchable dataset for future action.").

Two representative examples show how the ability to search the dataset of active criminal cases offers new ways to visualize patterns in the data. Prosecutors have long known that certain locations generate a disproportionate amount of crime.⁷² Prosecutors might even become familiar with a particular housing complex or building, developing a sense of a problem areas and problem people.⁷³ But, now with a quick search, prosecutors could pull up all of the cases to come from that address with all of the associated witnesses and factual circumstances. Prosecutors could identify an area and identify all the “usual” suspects in proximity.⁷⁴ A modern history of that particular problem area could be revealed and mapped. Or, if prosecutors learn that a police officer witness is compromised in some way, they now will be able to search the digital files to find and flag all of the cases the officer has been listed as a witness. Both types of information gathering were possible in the predigital era, but a central database makes it that much easier to visualize and map.

b. Data About Uncharged Crimes

Case management is a backward-looking process, seeking to organize information in a helpful way to facilitate the prosecution of identifiable suspects. It requires a filed case, a charged suspect, and a completed crime to be prosecuted in court. Many local prosecutors’ offices limit themselves to prosecuting the cases brought to them.⁷⁵ Lots of crimes, however, occur without a suspect or a case filed against someone. Intelligence-driven prosecution also focuses on understanding

72. See, e.g., Douglas F. Gansler, *Implementing Community Prosecution in Montgomery County, Maryland*, PROSECUTOR, July/Aug. 2000, at 30, 30–31.

73. See Eric Holder, *Community Prosecution*, PROSECUTOR, June 2000, at 31, 32 (discussing the importance of prosecutors knowing their community, the individuals involved in criminal activity, and seeing that crime is geographically based and sometimes connected).

74. Geolocation is one of the features of the Palantir Gotham technology. Geolocation simply means identifying a geographic location by its coordinates and collecting the information within those coordinates. See *Platform Features*, PALANTIR GOTHAM, <https://www.palantir.com/palantir-gotham/platform-features> [https://perma.cc/R3J2-S8EJ] (last visited Jan. 10, 2020).

75. See IMPLEMENTATION GUIDE, *supra* note 25, at 28 (“Prosecutors’ offices tend to gather and organize information around arrests. Generally, only when an arrest has been made, and a prosecution commences, do we document details such as the incident location, the crime victim(s), witnesses, the defendant(s) and, possibly, the connection between the incident and other crimes. Unfortunately, many opportunities for solving crimes and building cases are missed by waiting until an arrest occurs before documenting and organizing criminal intelligence. For example, uncooperative shooting victims or suspects in violent crimes frequently are arrested on unrelated matters. Unless a prosecutor’s office has a method in place for gathering and organizing information about violent crime, for example, opportunities to leverage an arrest for cooperation or to incapacitate a violent offender may be missed.”).

those open or uncharged crimes, looking to understand and perhaps prevent future crimes by seeing patterns in uncharged (but very real) criminal activity.⁷⁶

The Manhattan DA's Office has developed a "Crime Prevention System" (CPS) that charts out the patterns of crime, charged and uncharged, in particular areas. This digital collection system is an attempt to categorize and understand every criminal event in an area, whether or not there is a formal prosecution. With the CPS, prosecutors can use the database to search for particular people, gangs, investigations, or incidents even without an active case.⁷⁷

Assume, for example, a serious crime occurs without an obvious initial suspect. The CPS database will record the type of crime in a checkbox system (homicide, shots fired, stabbing, home invasion, robbery, burglary-commercial, police involved, etc.).⁷⁸ In addition to the crime, the incident details will include the location, victim's name, age, address, and geocoordinates.⁷⁹ An incident description will be included based on initial investigation.⁸⁰ In training materials, the Manhattan DA included a sample incident description for intelligence sharing around a shooting:

[Jefferson Houses Intel Requirements:] (19 [year old]) was shot once in the left groin area by an unknown male in front of 2227 Second Avenue (Jefferson Houses). . . . The perpetrator fled the location in an unknown direction. No ballistics recovered. [C.F.] . . . (ABM ["All Bout Money" gang]) witnessed the incident.⁸¹

76. See MODELS FOR INNOVATION, *supra* note 3, at 28 (discussing the crime prevention system (CPS) as a model focused on charged and uncharged criminal activity); IMPLEMENTATION GUIDE, *supra* note 25, at 28 ("To enable the capture and organization of crime-related information, regardless of whether an arrest has been made, the Manhattan DA's Office created CPS (Crime Prevention System), a repository of criminal intelligence that permits the documenting of relationships amongst the data collected.").

77. See TALLON ET AL., *supra* note 2, at 28 ("Crime Prevention System (CPS) is a CSU-maintained repository of criminal intelligence. CSU organizes CPS around persons, gangs, BBPs, and incidents, which allows prosecutors to discover relationships in the data. Individual of interest may have a file even if they have not been arrested. For example, CSU staff may add a file to CPS documenting a violent incident, including the date, start date, end date, precinct, address, relative location, geocoding fields for mapping, and incident description, even if the incident did not result in an arrest. CSU can also describe incidents as homicides, shootings, shots fired, stabbings, sexual assaults, drug-related incidents, gang-related incidents or domestic violence incidents. CSU staff can identify victims, suspects, witnesses, or defendants, and document the type of weapon used in the crime.").

78. See *id.*; see also IMPLEMENTATION GUIDE, *supra* note 25, at 29.

79. See IMPLEMENTATION GUIDE, *supra* note 25, at 29.

80. See *id.*

81. KERRY CHICON, N.Y. COUNTY DISTRICT ATT'Y'S OFF., INTELLIGENCE-DRIVEN PROSECUTION: PROMOTING COLLABORATION (2010), <http://www.icjia.state.il.us/assets/sites/reduceviolentcrime/Peoria%20Conference.pdf> [https://perma.cc/ZA37-A8RD] (full names have been changed to initials to preserve privacy).

Names, ages, relationships, gangs, and motives can be included in the system.⁸² Because the goal is to understand the context of the crime, other details are included in the CPS database. For example, flags about whether the case is domestic violence related, drug related, gang related, or club related are included.

For additional context, information about the affiliated relationships between witnesses, defendants, or victims are memorialized.⁸³ Intelligence gathering is conducted through sharing notes electronically that otherwise might not have been linked.⁸⁴ These intelligence notes might look like the following:

At about 1:00 am, Aubrie Smith (16 y/o, Whoadey [gang]) was beaten and hit in the head with a baseball bat by a group including Cooper (18 y/o, AIO ["Air It Out" gang]), who swung the bat, and Cooper's sister Gabriella (15 y/o), who joined in the beating and urged her brother to beat Smith with the bat. On 12/11/12, Smith died from his injuries. ADA . . . [assigned].⁸⁵

The system might flag gang associations or loyalty to a particular housing complex, building, or neighborhood.⁸⁶ Information about the dates when someone was a gang member could be included as well as affiliated incidents.⁸⁷ In a CPS system, these incidents might include prior shootings of individuals, prior crimes, or other motives for retaliatory violence.⁸⁸ Linked to the CPS is data about the suspects and witnesses to the crime. Personal information including name, date of birth, nicknames, and a Wiki page about other police-obtained

82. *See id.*

83. *See* Mac Donald, *supra* note 6 (discussing how the Crime Strategies Unit "has compiled a database of Manhattan's most significant criminal players" and other persons of interest such as elusive or uncooperative witnesses, based on daily communication with local police).

84. *See* IMPLEMENTATION GUIDE, *supra* note 25, at 29 ("Once entered into CP[S], incidents are linked to a 'Person' entry; the persons are identified as victim, suspect, witness or defendant. Both incidents and persons can be linked to Gangs or to a BBP. In this way, CPS creates a record of people and incidents and their connections to each other and to violent gangs. With one click, CPS can retrieve all violent incidents, and the persons involved in those incidents, which are connected to any one of the fifty-plus active gangs in Manhattan.").

85. *Id.* at 45 (names have been changed or redacted to preserve privacy).

86. *Id.*

87. *Id.* at 46.

88. *Id.*

information also can be found.⁸⁹ These Wiki pages grow every time an individual is contacted by police.⁹⁰

Standing alone, an individual CPS incident report is little different than a traditional incident report taken by an investigating officer. But, as with the digital case management system, the aggregation of these incidents reveals new patterns. Because prosecutors can search these digital files for names, nicknames, gang associations, or rivalries over time, new clues can emerge from the aggregated data. For example, if Gabriella (the sister described above) became the victim of an assault in the same neighborhood, even without witnesses to the assault, police might have a clue about a possible retaliatory motive. Or if there were an uptick in “Whoadey” assaults, police might be able to trace it back to a pattern of violence starting with this memorialized murder. Knowing which gang or family member might have a motive to engage in violence (and against whom) allows for both more effective deterrent solutions and faster police investigation.

Over time, the collection of CPS incident reports paints a picture of crime patterns in an area.⁹¹ Gangs, individuals, and feuds are mapped in overlapping patterns. Even without arrests or suspects, law enforcement can obtain a better understanding of the crimes occurring in an area. This might be helpful in solving future crimes or redirecting law enforcement resources to anticipate future conflicts.

c. Data About Places of Criminal Activity

Related to the focus on crime patterns is a focus on the places in which crimes occur. Prosecutors have long spent time trying to understand the neighborhoods in which they work.⁹² Big data systems allow locational data to be visualized in new

89. TALLON ET AL., *supra* note 2, at 28 (“Wikis are a CSU-written and interlinked set of web pages designed to store and organize unstructured intelligence on defendants. . . . Wikis allow users to not only search individuals, but locations, crimes, contact information, and more. Through a comprehensive search engine on a variety of topics, prosecutors can highlight patterns, connections, and relationships that may have otherwise remained hidden under a vast amount of data.”).

90. *Id.* (noting that “[p]rosecutors may request access to these pages from CSU, which controls the levels of access and permissions for each user. Each ‘page’ represents a person of interest; these individuals could be priority offenders or criminal associates. Information on a Wiki page may include the defendant’s association with gangs, feuds, victims, and eyewitnesses to the defendant’s criminal activity.”).

91. See CHICON, *supra* note 81.

92. See *id.* In fact, entire prosecution strategies have been developed to focus on community-oriented prosecution. See generally Bruce A. Green & Alafair S. Burke, *The Community Prosecutor: Questions of Professional Discretion*, 47 WAKE FOREST L. REV. 285 (2012).

ways. Crime statistics can now be collected and displayed on digital maps,⁹³ as can areas of successful crime eradication. These developments are not new,⁹⁴ but in combination with other technologies they offer a better geographical sense of crime patterns.

More cutting edge, real-time awareness of gang geography can be mapped, with explanatory information such as, “There are members of the East Coast Bloods and Latin Kings in this area, but no organized youth crew recognized by law enforcement.”⁹⁵ Technologies like SharePoint allow cities, gangs, public housing, and even active gang rivalries to be organized by type.⁹⁶ ARCGIS mapping technology allows prosecutors to see shots fired incidents even when there is no reported crime or arrest,⁹⁷ and more sophisticated mapping technologies provided by companies like Palantir can show all gun arrests for a particular time and place (over time).⁹⁸ The utility of such technology is that prosecutors can visualize both past crimes and possible suspects for small geographic areas.⁹⁹

d. Data About Priority Offenders

The centerpiece of intelligence-driven prosecution involves identifying the people thought to be driving criminal activity in an area.¹⁰⁰ As discussed, the stated

93. See IMPLEMENTATION GUIDE, *supra* note 25, at 24 (“CSU creates maps which visually display a pattern or history of violence in an area. . . . For example, maps may be used to show the violence in a particular year or timeframe. This may indicate the escalating violence or show the decrease in violence following a successful investigation and law enforcement strategy in the area.”).

94. See generally Andrew Guthrie Ferguson, *Crime Mapping and the Fourth Amendment: Redrawing “High Crime-Areas”*, 63 HASTINGS L.J. 179, 184–90 (2011) (discussing the history of crime mapping).

95. CHICON, *supra* note 81.

96. See IMPLEMENTATION GUIDE, *supra* note 25, at 27 (“SharePoint is a web application framework and platform developed by Microsoft. It serves as a secure place to store, organize, share, and access information. All that is required is a web browser, such as Internet Explorer, Chrome, or Safari. CSU’s SharePoint site is the online portal to the majority of intelligence CSU gathers and distributes throughout the Office. Any employee of the Manhattan DA’s Office can access the SharePoint site by navigating to an internal URL.”).

97. See *id.* at 24.

98. *Id.* at 63 (displaying Palantir Gun Arrests in East Harlem from April 1, 2014–April 15, 2015).

99. See HAMANN & GREENBERG-CHAO, *supra* note 12, at 26 (“[E]ach of Manhattan’s CSU prosecutors oversees a geographic area in the city to become experts on the particular impact of specific crimes and criminals on a community, and to create meaningful partnerships with police, other law enforcement groups, local community groups, and individuals.”).

100. See *id.* at 26 (“In Manhattan’s ground-breaking Crime Strategies Unit, created in 2010, a small team of senior prosecutors employ statistics and technology to ‘gather and deploy intelligence on Manhattan’s crime patterns and serious offenders,’ thus amassing a wealth of information available to the rest of the office to inform about ‘the importance of a particular defendant in wider criminal activity’ so as to make sure that those criminals do not ‘slip through the

goal is to incapacitate these “priority offenders” under the theory that if the bad apples are removed from society, overall crime will decrease.¹⁰¹ The technology to implement this target-based approach involves four interrelated systems—top 25 target lists, arrest alerts, Wikis, and photo-imaging mugshots—which all work together to inform prosecutors about the individuals most at risk to be involved in crime in the particular precincts.

In Manhattan, CSU prosecutors identify approximately 20–25 priority offenders in every precinct.¹⁰² These targets are usually men who have a history of criminal involvement, including felony convictions.¹⁰³ In some cases, these men will be known to be involved in shootings or robberies, even if they have not been caught doing those particular crimes. In other circumstances, individuals will be known because of prior police contacts or investigation,¹⁰⁴ or information from detectives or community activists might be the underlying cause for being placed on the target list.¹⁰⁵ Making the list as a “target” can result in prosecutors asking for stricter pretrial release conditions, less leniency in plea bargaining, or a harsher final sentence.¹⁰⁶

cracks.” (quoting Heather Mac Donald, *Prosecution Gets Smart*, CITY J., Summer 2014, <https://www.city-journal.org/html/prosecution-gets-smart-13663.html> [<https://perma.cc/4YBB-AF7R>])).

101. *C.f.* TALLON ET AL., *supra* note 2, at iv (“At the beginning of the project, CSU area assistant district attorneys (ADAs) collaborated with local police commanders and Field Intelligence Officers (FIOs) to identify at least 25 priority offenders in each precinct. ADAs then entered offender names into the Arrest Alert System (AAS) . . . and can continuously expand the list of priority offenders and/or record relevant intelligence.”); O’Keefe Interview, *supra* note 15 (“The question became, what can we do to incapacitate these people?”).
102. *See* IMPLEMENTATION GUIDE, *supra* note 25, at 8 (“[W]e asked each precinct to identify their worst 25 criminals and provide an explanation as to why each target was so identified. After reviewing the information in support of the precincts’ determinations, we termed these individuals ‘Priority Targets’—people whose incapacitation . . . would have a positive impact on the community’s safety and/or quality of life. These targets were then entered into the Arrest Alert System to ensure an appropriate response when targets are arrested.”).
103. Telephone Interview with David O’Keefe & Kerry Chicon, Crime Strategies Unit, Manhattan Dist. Attorney’s Office (Mar. 30, 2016) (David O’Keefe, one of the senior leaders of the Manhattan District Attorney’s Crime Strategy Unit, stated that priority offenders usually had five or more felonies before being designated a priority target.).
104. *See* IMPLEMENTATION GUIDE, *supra* note 25, at 7–8 (“The NYPD’s knowledge of specific individuals disproportionately responsible for committing crimes was invaluable. To capture this insight, we met with each precinct’s Field Intelligence Officer (FIO) who briefed us on crime within his or her precinct. We also identified and met with detectives and patrol officers within each precinct who were most familiar with high-crime areas or entrenched crime issues. These officers have detailed knowledge of the nature of the criminal activity based upon their daily interactions with the community and were able to identify particular individuals as priority targets.”).
105. *See id.*
106. *See id.* at 3 (“[T]he information gathered by CSU and disseminated through the Arrest Alert System allows us to assess and recommend appropriate sentences for defendants, i.e., identify

In addition, priority offenders become the subject of the arrest alert system.¹⁰⁷ The Manhattan DA Arrest Alert system compiles a host of important and not so important data points, as well as a good amount of opinion and even rumor, to be used by the prosecution in court.¹⁰⁸ For example, the alert system will include name, NYSID, aliases, gang affiliation, as well as other information about past criminal habits (including labels like bike thieves, car boosters, former juvenile robbery intervention program member, etc.).¹⁰⁹ Shared notes allow police officers and prosecutors to provide more detail about individuals subject to an arrest alert. For example, two sample digital notes in the system read:

“This defendant has committed multiple violent crimes in the confines of the 5th Pct, including Robbery/Grand Larceny/Assault/CPCS, and he is a known recidivist shoplifter on Canal Street.”¹¹⁰

“This defendant is known to be arrested for AC [alcohol] violations for drinking in public. However he is very violent and has multiple crimes against police officers, particularly in and around the 5th Pct.”¹¹¹

Relationships are identified and nicknames clarified. Details about whether the target is an arrest priority, requests for follow up information, and open

those for whom incarceration is an imperative from a community-safety standpoint and those for whom alternatives to incarceration will not negatively impact overall community safety.”); TALLON ET AL., *supra* note 2, at vii (“Arrest Alert cases arraigned on a felony were more likely to receive a prison sentence (reaching statistical significance in one of the two comparison samples). In addition, among those sentenced to jail or prison, Arrest Alert defendants received jail or prison sentences averaging more than 100 days longer than sentences for defendants in either of the two comparison groups.”); McKinley, *supra* note 33 (“The office’s strategy has been to pursue people believed to be drivers of crime, using whatever felony charge prosecutors can prove and seeking the maximum penalty.”); O’Keefe Interview, *supra* note 15 (“This system has all sorts of useful applications. It can help shape the plea offers made to the court.”).

107. TALLON ET AL., *supra* note 2, at 23 (“The enhanced communication and intelligence flow between CSU and prosecuting ADAs means that bail requests, charging decisions, and disposition and sentencing recommendations more accurately reflect a priority offender’s true criminal involvement. In other words, ADAs obtain stronger evidence to support their sentencing recommendations through comprehensive intelligence gathering and organization.”).

108. See IMPLEMENTATION GUIDE, *supra* note 25, at 7 (detailing how the system works); O’Keefe Interview, *supra* note 15 (“The Arrest Alert system has started to revolutionize the way cases are handled; I call it the ‘central nervous system’ for intelligence-driven prosecution. . . . If a prosecutor has a case they’re working on, they can add names of persons of interest to the list and they will get an alert in the form of an email if that person is arrested anywhere in New York City.”).

109. IMPLEMENTATION GUIDE, *supra* note 25, at 53.

110. CHICON, *supra* note 81, at 9.

111. *Id.*

investigatory questions are included in the database. As a few examples from a training dataset, here are some of the details attached to particular targets:

“AIO. Brother of Monday Cooper. Known as D-Sour.”¹¹²

“AKA “Jiggy Josh” Notify Lt. Brown if arrested.”¹¹³

“Possible AIO. Is he the person in the group photo of 8 people posing as if they had guns?”¹¹⁴

“23rd precinct Person of Interest—notify Lt. Brown if arrested.”¹¹⁵

“This Defendant was flagged by PBMN [Patrol Bureau of Manhattan North] crime analysis as an electronic device recidivist on either parole or probation (23rd pct., Robbery). . . . NYPD has him on a list as AIO for unknown reasons.”¹¹⁶

Finally, other information about possible cooperation with police, allegiances, and possible biases are all included in the central data system:

“AIO Debriefing opportunity. Was a fugitive for 3 months on (case #) before getting a 60 day probation split. Bail jump never indicted. AKA Staxx.”¹¹⁷

“AIO. Said to be Dell Scott’s best friend.”¹¹⁸

The information which exists in this ever expanding database is also shared among prosecutors who need the information in court.¹¹⁹ The innovation of the arrest alert system is to be able to provide line prosecutors information necessary for bail determinations at the earliest stage of the criminal justice process,¹²⁰ including prewritten bail applications asking for higher bail for targeted individuals.¹²¹ Sample arrest alert emails read something like:

112. IMPLEMENTATION GUIDE, *supra* note 25, at 42.

113. *Id.*

114. *Id.*

115. *Id.*

116. *Id.*

117. *Id.*

118. *Id.*

119. See O’Keefe Interview, *supra* note 15 (“Before arrest alerts, prosecutors would likely have no idea if the person they were prosecuting had been arrested again while the case was active, particularly if the arrest happened outside of Manhattan. The arrest alert system has allowed us to break out of a reactive approach to prosecution to one that is focused on coordination and proactive measures.”).

120. See Kreag, *supra* note 29, at 788 (“The backbone of this [CSU] unit is an automated database system—the Arrest Alert System—that notifies prosecutors when a ‘priority defendant’ has a new police encounter.” (footnote omitted)).

121. See TALLON ET AL., *supra* note 2, at vi (“Arrest Alert cases were modestly but significantly more likely to have bail set, and averaged significantly higher bail amounts than comparison cases.”); *id.* at 21 (“CSU Area ADA may also offer the attorney in [the Early Case Assessment Bureau (ECAB)] a prepared bail application with all of the relevant intelligence entered.”); McKinley,

“Note: AKA: “Dev”. Primary Target. Defendant is an uncooperative victim of a stabbing that occurred on 11/18/10 at 2:30pm in front of 1875 3rd Avenue in the Washington Houses in the 23rd pct.¹²²

“Note: Possible witness to shooting on October 31, 2011 at 419 East 93rd Street.”¹²³

Again, this fragmented information can be shared across jurisdictions and be useful in providing context of a suspect arrested in another case.¹²⁴ The theory behind this intelligence sharing is that, many times, priority offenders are arrested on minor crimes but present a major threat to the community. One such explanatory email from the arrest alert system read:

Here are the facts of his *open 265 case*. AO observes D with others walking down street and they appear intoxicated and D in possession of something that looked like a flashlight. AO heard the zap of a taser and approached D as D used the taser on the person he was with. D saw cops and ran across the bridge to the Bronx. Bag on bridge is recovered with a taser, a box for a taser, and a charger for a taser.

When D was 15yo in 2011 he *was arrested with a gun after a robbery*—He robbed victims of their cell phones at gunpoint. D was captured on video holding the gun and placing it where it was later recovered. He got YO and probation.

He has been *uncooperative in his 2 shootings*. We also believe him to be (2 shootings and one miss: shots fired).¹²⁵

Such information about a particular suspect’s past criminal involvement, knowledge about shootings in the area, and some criminal exposure beyond the instant charge may result in a more restrictive bail determination. In addition, places can be flagged for an “arrest alert” to make sure prosecutors know about

supra note 33 (“Bail application letters detailing the defendant’s history of other crimes have been prepared in advance, and at the arraignment, the prosecutor regularly pushes for higher bail and sometimes brings a more serious charge, if it can be justified by the evidence.”).

122. CHICON, *supra* note 81.

123. *Id.*

124. See TALLON ET AL., *supra* note 2, at iv (“The Arrest Alert System includes information on each priority offender of interest. Updated numerous times since 2010, the system enables Manhattan DA to record intelligence that is not available on a defendant’s rap sheet (for example, criminal associations, gang involvement, or other activities), and ensures that intelligence on priority offenders is effectively stored for future use.”); McKinley, *supra* note 33 (“The unit assembled what amounts to a list of prioritized targets for prosecution in each precinct. When people on the list are arrested, even for minor crimes, prosecutors receive an electronic alert.”).

125. CHICON, *supra* note 81.

crimes occurring in particular locations.¹²⁶ As will be discussed in Part II, however, all of the information would be potential impeaching evidence if the defendant ever turned up as a government witness.¹²⁷

This type of personal information about past criminal involvement, friendships, rivalries, and the like is not limited to the arrest alert system, but also gets uploaded onto a Wiki system.¹²⁸ Wiki systems are based on the Wikipedia approach to information sharing whereby individuals crowdsource information in the hope that the collective effort will provide a more accurate description of a subject.¹²⁹ In the criminal context, this means that individuals who make the priority offender list also have Wiki pages created so law enforcement can upload details about their suspicions about them. All this information, including debriefing notes from detectives and photographs, is uploaded to the system.¹³⁰ If a prosecutor wants to find out more information about a defendant or a witness, she need only search the system.

Less technologically sophisticated targeting mechanisms also exist in Manhattan and in other cities. The early version of a shared Wiki was an open access Excel spreadsheet that tracked names, nicknames, gangs, individuals' roles in gangs, information about who identified an individual as part of a gang (ADA, NYPD, PSA, Arrest Alert), and individuals' social media profiles.¹³¹ A similar Excel spreadsheet was also used to track curfew violators, memorializing the name, date, time, and description of each violation.¹³² These old-fashioned tracking systems can be used in conjunction with the more advanced data systems.

126. IMPLEMENTATION GUIDE, *supra* note 25, at 20 ("An ADA investigating a shooting at a particular location could, for example, create an alert to be notified of the arrest of any person at that address or nearby locations. Alternatively, an ADA focusing on a particular housing development could create an alert that would notify subscribers when anyone is arrested at any of the addresses of that development or when a resident of that development is arrested elsewhere.").

127. *See infra* Part II.

128. *See supra* note 92 (describing Wikis).

129. IMPLEMENTATION GUIDE, *supra* note 25, at 65.

130. *Id.* at 9 ("Debriefings, the interview for intelligence purposes of a person recently arrested or a charged defendant, can be an invaluable investigative tool... Defendants are advised beforehand that the proffer or debriefing is being done with no promise or benefit to the defendant. The proffer is a tool for CSU to gather more intelligence on a geographic area, gang, or a pattern of ongoing violence or unsolved crimes."); Brown, *supra* note 4 ("Every morning, I talk to my five A.D.A.s, who are experts in their areas. We decide whom we should try to pull out for a debriefing. . . . We pull people arrested on low-level misdemeanor charges, maybe two or three a week. We read them their Miranda rights. About 80 percent of them will talk." (statement of CSU Chief Kerry Chicon)).

131. IMPLEMENTATION GUIDE, *supra* note 25, at 40.

132. *Id.* at 41–42.

e. Data About Criminal Networks

Understanding networks of crime is a key part to intelligence-driven prosecution.¹³³ In addition to compiling information on cases, crimes, places, and people, prosecutors also want to understand the associational relationships and linkages among these data points.

Technology allows prosecutors to see these social network connections. Private companies, for example, offer prosecutors new capabilities to search for people and connections.¹³⁴ And as Elizabeth Joh explains, such law enforcement social network analysis can be a very powerful investigative tool:

Social networks refer to a set of personal connections among a group of people. The basic unit of analysis in social network analysis consists of the link between two people. The ties (relationships) between nodes (people) can take many forms: drug transactions, phone calls, or physical contacts between victims and offenders. Based on mathematical modeling, social network analysis maps a particular group of relationships. Most importantly, the approach identifies the relative importance or centrality of nodes (individuals): “their importance to the criminal system, role, level of activity, control over the flow of information, and relationships.”¹³⁵

In the policing context, investigators can search the dataset for arrests, properties, charges, and arresting officers, and they can flag related events, entities, and documents. Investigators can use filters to search phone calls, emails, photos, police assignments, Facebook activity, Facebook Communications, and other communications.¹³⁶ Ultimately, all of these searchable data points and connections allow prosecutors to link people by common phone numbers, addresses, shared flights, or shared friendships.¹³⁷ For example, X1 Social Media Monitoring technology allows prosecutors to search YouTube, Twitter, Instagram, Tumblr, and Facebook looking for tags, or metadata, with the ability to

133. See UCHIDA ET AL., *supra* note 53, at 11.

134. See TALLON ET AL., *supra* note 2, at 28 (discussing the use of Palantir, a “technology suite for data analysis” to “connect data and information across all pertinent databases” and “also enable[] prosecutors to make connections between data derived from phone calls and Facebook”).

135. Elizabeth E. Joh, *The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing*, 10 HARV. L. & POL’Y REV. 15, 25 (2016) (quoting Jennifer A. Johnson et al., *Social Network Analysis: A Systematic Approach for Investigating*, FBI L. ENFORCEMENT BULL. (Mar. 5, 2013) (<http://leb.fbi.gov/2013/march/social-network-analysis-a-systematic-approach-for-investigating>) [<http://perma.cc/47QG-ZNYC>]).

136. IMPLEMENTATION GUIDE, *supra* note 25, at 50–56.

137. *Id.*

map the discovered connections.¹³⁸ I2 is a company that allows prosecutors to conduct link analysis between phone numbers.¹³⁹ And prosecutors use their own DANY InPho system to track calls among inmates from New York City jails.¹⁴⁰ The NYC DOC inmate call report allows searches by name, number, date, frequency of calls to particular numbers, duration, and even a call summary of the substance (because all the calls are recorded).¹⁴¹

Other technologies allow police to search and sort by biometric clues. Photo Imaging Mugshot System (PIMS) is used in Manhattan to identify suspects from a larger collection of arrest mugshots.¹⁴² Prosecutors can conduct side by side comparison, create charts of suspects, link together images as neighborhoods or gangs, arrange by data and attempt facial recognition matches.¹⁴³ All of these different digital investigative tools provide a better picture of the complex relationships between different actors in the criminal justice system and are now available to prosecutors with access to the system.

f. Data About Probationers/Parolees

Traditionally, prosecutors focused on issues arising from pretrial, trial, sentencing, and appeal matters, being less involved with defendants who came back into the system (unless they got rearrested). A defendant on probation or parole normally remained outside of a prosecutor's field of vision unless they reoffended or became a witness. New technology is changing this focus, widening the net of interest and allowing prosecutors to track defendants as they return home.¹⁴⁴

Prosecutors are now notified when a particular "flagged" individual is returning home from his sentence.¹⁴⁵ In partnership with the parole commission,

138. *Id.* at 41–43.

139. *Id.*

140. *Id.* at 52–53.

141. *Id.*

142. *Id.* at 22 ("Photo sheets are helpful for learning nicknames, criminal associations, social media addresses, and to learn details about specific violence involving those in the photo sheets.").

143. *Id.* at 51–56. *But see* Clare Garvie, *Garbage In, Garbage Out: Face Recognition on Flawed Data*, GEO. CTR. ON PRIVACY & TECH. (May 16, 2019), <https://www.flawedfacedata.com> [<https://perma.cc/5UBX-THL9>].

144. TALLON ET AL., *supra* note 2, at 6 ("Although the IDPM focuses heavily on improved information flow *within* the prosecutor's office, the model also focuses on enhanced information sharing and interagency coordination with *external* stakeholders, including law enforcement and representatives of local community-based agencies." (emphasis original)).

145. MODELS FOR INNOVATION, *supra* note 3, at 19 ("CSU and CPU also make recommendations to Parole regarding specialized conditions and provide reentry services for individuals returning to their communities after a period of incarceration.").

prosecutors might even suggest release conditions. One such example was used in a training document:

Proposed Geographic Restrictions: Mr. Reed released to parole supervision. . . . We believe successful re-entry would be best aided if he were to be excluded from the area between Adam Clayton Jr. Boulevard (7th Avenue) and Fredrick Douglass Boulevard (8th Avenue), between West 146th and West 152th Streets in the 32nd Precinct.

Reasons for Exclusion Area: Mr. Reed has been identified as a member of “From Da Zoo” (FDZ), a gang based in the 32nd Precinct primarily located in the area between Adam Clayton Jr. Boulevard (7th Avenue) and Fredrick Douglass Boulevard (8th Avenue), between West 146th and West 152 Streets.¹⁴⁶

The goal, of course, is to use the data prosecutors have about problem places to avoid preventable conflict between rival groups. The proposed restrictions are largely adopted by parole officers responsible for the monitoring.¹⁴⁷

3. Centralized Big Data Prosecution

All of these data streams fuel the development of a more centralized intelligence-driven prosecution system. Recognizing the valuable information that exists, the Manhattan CSU decided to create a separate technological system to allow prosecutors from all over the area to query the CSU database.¹⁴⁸ The DANY311 Request for Assistance allows prosecutors to search for all matter of collected criminal information.¹⁴⁹

So, for example, an interested prosecutor can ask for background information, debriefing information, investigation, search warrants, case status, photo sheets, witness location, social media information, place data, contact

146. CHICON, *supra* note 81 (quoted language from slide 24) (names have been changed in the example to protect privacy).

147. TALLON ET AL., *supra* note 2, at 32 (“CSU received an arrest alert that an identified gang member, who was on parole, had been arrested for a misdemeanor shoplifting offense. CSU staff successfully requested that the State Division of Parole set conditions barring the defendant from the gang area and from associating with members of his gang. While the new arrest was outside the gang area, it triggered an arrest alert, which prompted CSU to examine the co-defendant’s background. CSU informed Parole that the co-defendant was on a list of individuals who the original defendant was barred from associating; Parole subsequently filed a parole violation.”).

148. *See id.* at v (“DANY established a wide range of technology-based tools enabling ADAs throughout the office to monitor arrests, request additional information from CSU, and/or share intelligence about priority offenders.”).

149. *Id.* at 24.

information, gang details, video, crime data, inmate data, or other details.¹⁵⁰ The result is a centralized digital system in the possession and control of the prosecution. All the information—fragmented and raw, inculpatory and exculpatory—exists in searchable centralized systems. It is new, powerful, unwieldy, and—despite the risks of data overload and fragmentation—clearly valuable to prosecutors seeking to gain a competitive edge in reducing crime.¹⁵¹

B. Big Data Surveillance: Unstructured Big Data

Intelligence-driven prosecution functionally acts to organize information in prosecution-focused datasets. But prosecutors do not work in isolation. In addition to police investigation notes and forensic evidence, prosecutors are also able to access newly developing law enforcement surveillance technologies.¹⁵² As a result, an almost overwhelming amount of unstructured data from fixed police surveillance cameras, police body cameras, and a host of other sensor devices can be used for investigation.¹⁵³ The term “unstructured” here refers to the fact that the information is not in a formal, searchable database and not organized in a predefined manner.¹⁵⁴ While unstructured, this information is nevertheless in the

150. See *id.* at 22 (“For example, a CSU Area ADA may be interested in debriefing an individual who was arrested and linked to an active gang. Even if some of the information the defendant provides is not immediately useful for prosecuting a priority offender, ADAs can still enter this intelligence into files on SharePoint or Wiki Pages and re-access the information at a later time. Maintaining up-to-date intelligence is a vital step in tracing and identifying evolving criminal patterns and associations.”).

151. IMPLEMENTATION GUIDE, *supra* note 25, at 29 (“The regular processing of cases within a prosecutor’s office frequently generates information about a defendant’s background that usually is not organized for later access and analysis but which may assist in solving crimes or simply provide a fuller understanding of the person being prosecuted. Layer on that the significant amount of criminal intelligence generated, for example, through debriefings, through an IDP model, and it becomes necessary to have the ability to organize and make available for later use that unstructured data.”).

152. See generally Andrew Guthrie Ferguson, *Big Data and Predictive Reasonable Suspicion*, 163 U. PA. L. REV. 327 (2015); Elizabeth E. Joh, *Policing by Numbers: Big Data and the Fourth Amendment*, 89 WASH. L. REV. 35 (2014).

153. JOHN S. HOLLYWOOD ET AL., PRIORITY CRIM. JUST. NEEDS INITIATIVE, USING VIDEO ANALYTICS AND SENSOR FUSION IN LAW ENFORCEMENT 4 (2018), https://www.rand.org/content/dam/rand/pubs/research_reports/RR2600/RR2619/RAND_RR2619.pdf [<https://perma.cc/69ZE-8XYC>] (“The proliferation of internet-enabled digital video cameras and sensor devices (also known as the Internet of Things), combined with the ongoing fielding of conventional cameras, provides public safety agencies with huge technological opportunities.”).

154. There are other definitions of unstructured data, which can include things like the text in police narratives. Because the data are searchable (even if not in structured form), they present a slightly easier dataset from which to find information. Video surveillance footage is currently even less structured and thus harder to search. JAY STANLEY, ACLU, THE DAWN OF ROBOT SURVEILLANCE: AI, VIDEO ANALYTICS, AND PRIVACY 29 (2019),

possession of law enforcement, is being used in criminal investigations, and potentially contains *Brady* material.

For *Brady* purposes, all of this information is functionally still the responsibility of prosecutors as leaders of the prosecution team, but because it resides in a police-dominated environment it is addressed separately. This Subpart briefly describes the potential for *Brady* information in these data systems, focusing on video surveillance and sensor surveillance.

1. Unstructured Video Surveillance

Surveillance cameras have been in use in New York since 1968¹⁵⁵ and are widely deployed in most major cities. For the most part, cameras shoot in fixed frame view with footage only retrieved or reviewed if an incident occurs. Use of surveillance footage in criminal prosecutions has become routine.¹⁵⁶ Like a traditional casefile, a traditional video surveillance clip provides a limited, targeted subset of information useful for a prosecution. Today, prosecutors have access to the location of surveillance cameras through a detailed Surveillance Camera Interactive Map (SCIM).¹⁵⁷ This map allows prosecutors to know where to look for video evidence of crime, which can be very useful for identifying suspects.¹⁵⁸

New networked digital video surveillance systems add complexity to the traditional process because they simultaneously record entire areas of a city. In lower Manhattan, over 9000 linked video cameras feed real-time footage of the city directly to a central command center.¹⁵⁹ Part of the Domain Awareness Center,

https://www.aclu.org/sites/default/files/field_document/061119-robot_surveillance.pdf [https://perma.cc/X2AR-E3H4].

155. Jonathon Keats, *In Praise of Ugly and Conspicuous Security Cameras*, WIRED (Oct. 22, 2019), <https://www.wired.com/story/in-praise-of-ugly-conspicuous-security-cameras> [https://perma.cc/26ZX-3HZT].

156. See HOLLYWOOD ET AL., *supra* note 153, at 4; *Police Unlock AI's Potential to Monitor, Surveil and Solve Crimes*, WALL STREET J. VIDEO (May 30, 2019, 5:30 AM), <https://www.wsj.com/video/police-unlock-ai-potential-to-monitor-surveil-and-solve-crimes/819D5F78-22BC-4A41-9517-AE31BE3C5E7E.html> [https://perma.cc/8MA6-ZG3Y].

157. See McKinley, *supra* note 33 (“Prosecutors will have access, for instance, to the network of security cameras on city streets the department uses to solve crimes, as well as the mountains of data collected on police reports, while detectives will receive the granular intelligence about criminal conspiracies gathered by prosecutors as they prepare for trial.”).

158. IMPLEMENTATION GUIDE, *supra* note 25, at 24–25 (Explaining that CSU and Technology Analysts can access S.C.I.M. on their computers, and “soon, every ADA in the office will be able to access S.C.I.M using their desktop computer and a program called Palantir, a technologies suite for data analysis”).

159. See Brayne, *supra* note 7, at 300–01 (“In the largest Domain Awareness System, the NYPD partnered with Microsoft to collect information from closed-circuit surveillance cameras, ALPRs, radiation sensors, and other sensors to match with police databases.”); Chris Francescani, *NYPD Expands Surveillance Net to Fight Crime as Well as Terrorism*, REUTERS

the NYPD, in partnership with Microsoft, has developed a smart camera network that can watch as a person goes from block to block.¹⁶⁰ The system also automatically records all of the license plates that drive into the area, automatically flags suspicious behavior, and can search for items, objects, colors, or text across the system.¹⁶¹ Chicago, Illinois, has deployed over 30,000 cameras in higher crime areas linked back to localized command centers specifically created to respond quickly to criminal activity.¹⁶² ShotSpotter has recently announced a pilot project to link video-capable drones to their system of acoustic sensors.¹⁶³ Other drone makers are in talks with camera companies for aerial scans, which could offer similar capabilities of object identification or facial recognition matches in large groups.¹⁶⁴ In Hartford, Connecticut, several hundred cameras link back to a central system run through BriefCam technology that can digitally search for objects, colors, cars, or other items of interest using artificial intelligence.¹⁶⁵ In other cities across America, police and privately owned or commercially owned cameras are being linked together into citywide surveillance networks.¹⁶⁶

(June 21, 2013, 8:24 AM), <https://www.reuters.com/article/usa-ny-surveillance/nypd-expands-surveillance-net-to-fight-crime-as-well-as-terrorism-idUSL2N0EV0D220130621>

[<https://perma.cc/F793-HXRS>]; Robert Lee Hotz, *As World Crowds In, Cities Become Digital Laboratories*, WALL ST. J. (Dec. 11, 2015, 11:10 AM), <https://www.wsj.com/articles/as-world-crowds-in-cities-become-digital-laboratories-1449850244> [<https://perma.cc/QSW8-S77N>].

160. Brayne, *supra* note 7, at 300–01.

161. Kelsey Finch & Omer Tene, *Welcome to the Metropticon: Protecting Privacy in A Hyperconnected Town*, 41 FORDHAM URB. L.J. 1581, 1601 (2014) (“Face and object detectors are already widely deployed throughout urban landscapes, both as safety measures (the police in lower Manhattan can track cars and people moving south of Canal Street and even detect unattended packages) and as energy conservation tools (motion sensors on smart streetlights can save an additional twenty to thirty percent on energy by dimming lights during hours of low activity, as well as tracking noise and pollution levels.)” (footnotes omitted)).

162. Timothy Williams, *Can 30,000 Cameras Help Solve Chicago’s Crime Problem?*, N.Y. TIMES (May 26, 2018), <https://www.nytimes.com/2018/05/26/us/chicago-police-surveillance.html> [<https://perma.cc/YC4Q-CZP7>].

163. Sidney Fussell, *Kentucky Is Turning to Drones to Fix Its Unsolved-Murder Crisis*, ATLANTIC (Nov. 6, 2018), <https://www.theatlantic.com/technology/archive/2018/11/police-drone-shotspotter-kentucky-gun-911-ai/574723> [<https://perma.cc/KQ86-UZVY>].

164. See Chaim Gartenberg, *DJI is Partnering with Axon to Sell Video-Capable Drones Directly to Cops*, VERGE (June 5, 2018, 2:13 PM), <https://www.theverge.com/2018/6/5/17429908/dji-axon-air-taser-drones-police-officers-program-sale> [<https://perma.cc/7Y2M-TTN2>].

165. Eoin Higgins, *Pre-Crime Policing Is Closer Than You Think, and It’s Freaking People Out*, VICE NEWS (June 12, 2018, 12:47 PM), https://www.vice.com/en_us/article/7xmmvy/why-does-hartford-have-so-many-cameras-precime [<https://perma.cc/9LUY-VQMJ>]; see also Milestone Systems, *Hartford Crime Center Expands City Surveillance*, YOUTUBE (Dec. 12, 2017), <https://www.youtube.com/watch?v=OLGxTITe6dE>.

166. See Ann Pierret, *Flint Police Using Surveillance Camera Network to Help Fight Crime, Deploy Officers*, ABC 12 WJRT (Nov. 3, 2017), <https://www.abc12.com/content/news/Flint-police-using-surveillance-camera-network-to-help-deploy-officers-454973523.html> [<https://perma.cc/5NN3-TSA3>]; Rick Rojas, *In Newark, Police Cameras, and the Internet, Watch*

On the ground, police officers and police cars have been equipped with police body cameras that record day-to-day interactions with citizens.¹⁶⁷ The rapidly expanding use of body cameras is a direct response to technological advancements and political pressures for greater police accountability.¹⁶⁸ The result has been a proliferation of video footage from thousands of police cameras.

Expanded use of police body cameras has created a need for greater storage capacity for this footage and better technological tools to make practical use of the footage.¹⁶⁹ If police and prosecutors cannot access the relevant part of a video in a timely and cost-effective manner, then the benefit of the video becomes greatly reduced.¹⁷⁰ As a result, leading police body camera makers and other surveillance companies have begun investing in AI shortcuts to allow for quick searching through video.¹⁷¹ For example, Axon, the leading police body-worn camera company in the United States, has been internally testing AI technology—Dextro—to search footage for criminal cases.¹⁷²

Dextro is a video analysis tool “trained” to recognize objects when scanning camera footage. Started in 2014 as advertising technology for

You, N.Y. TIMES (June 9, 2018), <https://www.nytimes.com/2018/06/09/nyregion/newark-surveillance-cameras-police.html> [<https://perma.cc/8QDS-PR5U>]; Aviva Shen, *New Orleans Eyes Bars and Restaurants as New Focus of Surveillance*, CITYLAB (Feb. 9, 2018), <https://www.citylab.com/life/2018/02/new-orleans-eyes-bars-and-restaurants-as-new-focus-of-surveillance/552836> [<https://perma.cc/ULW4-S7CM>].

167. See Mary D. Fan, *Justice Visualized: Courts and the Body Camera Revolution*, 50 U.C. DAVIS L. REV. 897, 932 (2017); Mary D. Fan, *Privacy, Public Disclosure, Police Body Cameras: Policy Splits*, 68 ALA. L. REV. 395, 426 (2016).

168. *But see Developments in the Law: Policing*, 128 HARV. L. REV. 1706, 1805–14 (2015) (discussing how police body cameras were viewed as a technological response to a call for greater police accountability); Adam A. Marshall & Katie Townsend, Opinion, *A Tool to Gain the Public’s Trust*, WASH. POST (May 15, 2015), https://www.washingtonpost.com/opinions/a-tool-to-gain-the-publics-trust/2015/05/15/f7f9ad14-f4f8-11e4-84a6-6d7c67c50db0_story.html [<https://perma.cc/F3BE-PTF8>] (detailing how police body cameras were conceived as a way to gain the public’s trust after a series of high profile policing shooting of unarmed black men).

169. See *In the Police Body Camera Business, the Real Money’s on the Back End*, MARKETPLACE (Apr. 18, 2017), <https://www.marketplace.org/2017/04/18/business/police-body-camera-business-real-moneys-on-back-end> [<https://perma.cc/687Z-BDQD>].

170. See Alex Pasternack, *Police Body Cameras Will Do More Than Just Record You*, FAST COMPANY (Mar. 3, 2017), <https://www.fastcompany.com/3061935/police-body-cameras-livestreaming-face-recognition-and-ai> [<https://perma.cc/CBA3-TXVX>]; Patrick Tucker, *Facial Recognition Coming to Police Body Cameras*, DEF. ONE (July 17, 2017), <http://www.defenseone.com/technology/2017/07/facial-recognition-coming-police-body-cameras/139472> [<https://perma.cc/V57S-JC9E>] (“At least one Motorola competitor—Axon, formerly Taser—which also makes body cameras for cops, is also looking to integrate on-camera artificial intelligence into future products.” (citation omitted)).

171. See, e.g., Sidney Fussell, *The New Tech That Could Turn Police Body Cams Into Nightmare Surveillance Tools*, GIZMODO (Mar. 9, 2017, 10:09 AM), <https://gizmodo.com/new-ai-could-turn-police-body-cams-into-nightmare-surve-1792224538> [<https://perma.cc/W36W-6WJZ>].

172. *Id.*

tagging livestreaming videos, Dextro scans and pinpoints objects in footage that users are looking for, for example, a book, a Nike shoe, lines of text, or a gun. Dextro can also pick up motion information, like handshakes or a punch. Once Dextro has identified the objects or movements, it creates a timeline for when they appear in the footage, providing timestamps and frequency data. Presumably, an officer could take four hours of boring footage, run it through Dextro, and then automatically redact everything but the moments in which the desired object or motion appears. Officers can then search entire databases for videos based on these key moments like “officer foot chase” or “traffic stop.”¹⁷³

In addition, Axon has the capacity to upload all of the data for police and prosecution use in a centralized data center called Evidence.com.¹⁷⁴ So, as with the expansion of fixed surveillance camera footage, the quantity and quality of police-worn body camera footage in the prosecution’s hands has been matched with an effort to centralize this information.

2. Unstructured Sensor Data

Video is just one type of newly developing big data surveillance technology. Police are also utilizing automated license plate readers to track cars,¹⁷⁵ audio

173. *Id.*

174. Drew Harwell, *Facial Recognition May Be Coming to a Police Body Camera Near You*, WASH. POST (Apr. 26, 2018, 8:30 AM), <https://www.washingtonpost.com/news/the-switch/wp/2018/04/26/facial-recognition-may-be-coming-to-a-police-body-camera-near-you/> [<https://perma.cc/49PQ-5HWK>] (“Taser International...advertises itself as ‘the largest custodian of public safety data in the U.S.,’ saying more than 20 petabytes—or 20 million gigabytes—of police photos, body-camera video and other criminal-investigation documents have been uploaded to its cloud-storage service, Evidence.com.”). *But see* POLICING PROJECT, FIRST REPORT OF THE AXON AI & POLICING TECHNOLOGY ETHICS BOARD (2019) https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/5d9df18e9b1895351ceea85f/1570632083376/Axon_Ethics_Report_vfinal-English.pdf [<https://perma.cc/B2WS-JPJV>]; Madeline Purdue, *Axon Body-Camera Supplier Will Not Use Facial Recognition in its Products—For Now*, USA TODAY (July 1, 2019, 2:17 PM), <https://www.usatoday.com/story/tech/2019/07/01/axon-rejects-facial-recognition-software-body-cameras-now/1601789001> [<https://perma.cc/JNK2-JCNP>].

175. Brayne, *supra* note 7, at 299 (“One of the most pervasive dragnet surveillance tools is the Automatic License Plate Reader (ALPR). ALPRs can be static (for example, at an intersection) or mobile (for example, mounted on police cars). They take two pictures of every vehicle that passes through their line of vision—one of the car and one of the license plate—and record the time, date, and GPS location. Law enforcement can supplement their own ALPR data with privately collected readings, such as those gathered by repossession agents. ALPR data can provide a map of the distribution of vehicles throughout the city and, in some cases, may enable police to track individuals’ routine travel patterns or infer where they live or work based on where their car is repeatedly parked.”).

sensors to detect gunshots,¹⁷⁶ and cell site towers to identify cell phones.¹⁷⁷ Future technologies involving robots and autonomous vehicles may not be far behind.¹⁷⁸ All of these technologies collect sensor data in large databases and offer powerful investigative tools because they reveal digital patterns of people, places, and crimes that can be of value to both the prosecution and the defense.¹⁷⁹

These types of digital technologies can be searched for particular points of interest. For example, one can map all the times a particular license plate was flagged across a city, revealing intimate patterns of travel and activity.¹⁸⁰ Police can also track a phone to a specific location or identify groups of associates through social media locations.¹⁸¹ Because of the way the data systems are engineered (to be identified and identifiable by location or person), these types of data trails can be very helpful to investigators trying to build a case.¹⁸²

The full impact of the rise of big data policing is beyond the scope of this Article,¹⁸³ but some of these data trails may ultimately end up in large intelligence-driven prosecution systems.¹⁸⁴ The trend toward increased aggregation signals a strong likelihood that whatever information ends up in police hands for investigation will end up in the prosecution's centralized digital files, as well. For purposes of this Article, it is thus important to think about how these data driven systems are structured as they enter into big data prosecution systems.

176. Cara Buckley, *High-Tech 'Ears' Listen for Shots*, N.Y. TIMES (Nov. 20, 2009), <http://www.nytimes.com/2009/11/22/nyregion/22shot.html> [https://perma.cc/2FJX-KCXG].

177. *E.g.*, *Carpenter v. United States*, 138 S. Ct. 2206, 2212 (2018) (determining that warrantless acquisition of seven days of cell site locational data violated the Fourth Amendment).

178. See Elizabeth E. Joh, *Policing Police Robots*, 64 UCLA L. REV. DISCOURSE 516, 519, 534 (2016).

179. Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. 547, 560–61 (2017).

180. See, e.g., Cyrus Farivar, *Your Car, Tracked: The Rapid Rise of License Plate Readers*, ARS TECHNICA (Sept. 28, 2012, 1:30 AM), <http://arstechnica.com/tech-policy/2012/09/your-car-tracked-the-rapid-rise-of-license-plate-readers/2> [https://perma.cc/BM3T-8XXZ]; Eric Roper, *Police Cameras Quietly Capture License Plates, Collect Data*, STAR TRIB. (Aug. 16, 2012, 9:46 PM), www.startribune.com/local/minneapolis/165680946.html [https://perma.cc/CW23-TG4Z].

181. C. Justin Brown & Kasha M. Leese, *StingRay Devices Usher in a New Fourth Amendment Battleground*, CHAMPION, June 2015, at 12, 13–14; Matt Cagle, *Facebook, Instagram, and Twitter Provided Data Access for a Surveillance Product Marketed to Target Activists of Color*, ACLU N. CAL. (Oct. 11, 2016), <https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target> [https://perma.cc/5YMN-LJB4].

182. See Jennifer Valentino-DeVries et al., *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018), <https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html> [https://perma.cc/LV56-YBJX].

183. For more on this topic, see generally ANDREW GUTHRIE FERGUSON, *THE RISE OF BIG DATA POLICING: SURVEILLANCE, RACE, AND THE FUTURE OF LAW ENFORCEMENT* (2017).

184. See McKinley, *supra* note 33.

3. Structuring Unstructured Data

To be used by prosecutors, data must be searchable because otherwise there is no way to identify relevant material. Of the various surveillance technologies in use, some are structured to be searchable and some are not. Structured data sets are more easily used by prosecutors for investigation and more obviously the type of data that should be turned over if it is exculpatory or impeaching. For example, a suspect's ALPR license plate hit at the scene of the crime is inculpatory and helpful to the prosecution.¹⁸⁵ A suspect's ALPR license plate hit across town is exculpatory and should be turned over as potential *Brady* material.¹⁸⁶ But a prosecutor can only search for the information if the data is organized by license plate number, time, and location in a structured way.

This search capability was not always true for raw surveillance video. Once upon a time, prosecutors would have to watch, or fast-forward through, the entire video to get to the part relevant to a case.¹⁸⁷ The data (visual images) were not structured in searchable form by object or person. With new digital technology and artificial intelligence, however, the unstructured data can be structured into identifiable and thus searchable forms.¹⁸⁸ Cars, faces, colors, clothes, movements, speeds, and almost everything else can be broken down into digital features identifiable and thus searchable for efficient use.¹⁸⁹

One of the most significant innovations in recent years is how unstructured data systems are becoming structured through artificial intelligence and pattern matching algorithms.¹⁹⁰ As a gross simplification, picture a single camera feed of a busy urban intersection. Digital video cameras would capture different types of

185. A suspect's car being placed at the scene of the crime would be relevant evidence tending toward guilt if there were a question of linking the defendant to the crime scene.

186. A suspect's car being placed not near the scene of the crime would tend to undermine the government's case linking the suspect to the area of the crime.

187. As someone who practiced criminal law in the age of VHS tapes, the author can confirm the process was very slow.

188. HOLLYWOOD ET AL., *supra* note 153, at 4–6.

189. Jake Laperruque, *Preventing an Air Panopticon: A Proposal for Reasonable Legal Restrictions on Aerial Surveillance*, 51 U. RICH. L. REV. 705, 717 (2017) ("For example, the tracking technology, BriefCam, allows law enforcement to overlay hours of video and then isolate individuals based on certain factors so monitors can view all applicable targets with hours of time reduced to minutes. This can be used to isolate all individuals or cars that are a particular color, or traveling on a specific route. With such technologies, police could 'reverse-engineer' location tracking, picking a route they want to monitor, then use BriefCam to immediately isolate and identify everyone who used it over the course of several hours." (footnotes omitted)).

190. For a primer on video analytics, see HOLLYWOOD ET AL., *supra* note 153, at 4.

cars and people walking by and doing different things.¹⁹¹ In the background, buildings, roads, streets, and signs would be visible. If you took a freeze frame of the digitized image you could isolate each part of the photograph. Each section of each image can be broken down to digital features, looking at edges, corners, curves, and shapes, down to the pixel. Each object can be identified as a unique object.¹⁹² Two things are happening with digitization. First, each object and the background can be given a digital signature. Second, with the advent of artificial intelligence, objects with a digital signature can be compared to other objects and identified as such.¹⁹³ So, all blue cars can be identified as blue (and not some other color), or all blue Subaru Outbacks can be identified as a distinct type of car (different make, model), or all people wearing Washington Nationals' baseball hats can be isolated based on pattern recognition of the Nationals' logo. The work behind the scenes is made possible by artificial intelligence whereby computer models and machine learning systems can learn to recognize similar images as being the same thing.¹⁹⁴ Datasets teaching the model to distinguish between the Nationals' curly "W" and other sports teams with the same letter takes a lot of data, but it is relatively simple to accomplish as a technical matter. AI pattern matching systems, in other words, are now enabling the structuring of previously unstructured data collections, like those of police video surveillance footage.¹⁹⁵

The value for law enforcement intelligence is evident. Criminal actors can be observed, tracked, and identified. Clues can be mined from the data streams. Patterns of crime can be visualized. And all of this centralized big data policing can end up in the hands of the prosecution, including somewhere like the Manhattan District Attorney's Office. But what about all the other information that is less helpful to the prosecution? What about exculpatory information or inconsistencies that arise from video footage that undercut the prosecution's case? Without a system designed to flag and identify exculpatory information, not just

191. See, e.g., Milestone Systems, *supra* note 165; *Police Unlock AI's Potential to Monitor, Surveil and Solve Crimes*, *supra* note 156.

192. See Milestone Systems, *supra* note 165; *Police Unlock AI's Potential to Monitor, Surveil and Solve Crimes*, *supra* note 156.

193. See Laperruque, *supra* note 189; see also HOLLYWOOD ET AL., *supra* note 153, at 4–6.

194. See Andrew D. Selbst, *Disparate Impact in Big Data Policing*, 52 GA. L. REV. 109, 134 (2017) ("The ultimate goal of data mining is pattern-matching and generalization."); Harry Surden, *Machine Learning and Law*, 89 WASH. L. REV. 87, 91 (2014) (describing the power of machine learning).

195. Seth W. Stoughton, *Police Body-Worn Cameras*, 96 N.C. L. REV. 1363, 1396 (2018) ("Body-worn camera video can be used to facilitate machine learning, in which massive amounts of data can be fed through a software algorithm so that 'computer systems learn about an underlying process and its patterns by creating a useful mathematical approximation of how the process works.'" (quoting Michael L. Rich, *Machine Learning, Automated Suspicion Algorithms, and the Fourth Amendment*, 164 U. PA. L. REV. 871, 875 (2016))).

inculpatory information, the government will effectively *possess* such information without the ability to *find* it. This is the *Brady* problem discussed next in Part II.

II. THE DESIGN PROBLEM: HOW THE *BRADY* DOCTRINE FITS BIG DATA PROSECUTION SYSTEMS

The amount of data being handled by prosecutors' offices is vast and expanding daily.¹⁹⁶ Yet, while the volume and variety of information may have changed,¹⁹⁷ the law has not. The same constitutional requirement of due process remains.¹⁹⁸

This Part looks at how the *Brady* doctrine fits these big data, intelligence-led systems.¹⁹⁹ Within a review of the legal doctrine itself, the Part looks at how the various interconnected pieces of investigative big data might be considered *Brady* material in different types of cases. The *Brady* problem in intelligence-driven systems combines both theory and technology. Because there has not been a focus on *Brady* in the design, the systems will not flag the material as relevant. Even though centralized and technically available, the design choices blind prosecutors to potential exculpatory or impeaching evidence.

196. See e.g., Garrett, *supra* note 10, at 213; Ion Meyn, *Discovery and Darkness: The Information Deficit in Criminal Disputes*, 79 BROOK. L. REV. 1091, 1092 (2014); Oran, *supra* note 23, at 122 (discussing *Brady* in the context of electronic discovery with large datasets of documents); Jenia I. Turner, *Managing Digital Discovery in Criminal Cases*, 109 J. CRIM. L. & CRIMINOLOGY 237, 258 (2019).

197. VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, *BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK* 11 (2013); O'Reilly Media, *Volume, Velocity, Variety: What You Need to Know About Big Data*, FORBES (Jan. 19, 2012, 9:46 AM), <https://www.forbes.com/sites/oreillymedia/2012/01/19/volume-velocity-variety-what-you-need-to-know-about-big-data/2/#219a250470a1> [<https://perma.cc/JD55-Q5U5>].

198. See Garrett, *supra* note 10, at 216 ("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.").

199. One of the most comprehensive catalogs of the law surrounding *Brady* has been compiled by the Public Defender Service (PDS) for the District of Columbia. See SPECIAL LITIGATION DIVISION, D.C. PUBLIC DEFENDER SERV., *BRADY V. MARYLAND OUTLINE* (2013), [https://www.pdsdc.org/docs/default-source/default-document-library/brady-outline-final-\(2013\).pdf?sfvrsn=b77794d0_0](https://www.pdsdc.org/docs/default-source/default-document-library/brady-outline-final-(2013).pdf?sfvrsn=b77794d0_0) [<https://perma.cc/4JX5-KG3V>]. This Part was heavily influenced by their excellent canvassing of case law. As a lawyer at PDS during the early years of the creation of this document, I know the hard work put in by many attorneys in the Special Litigation Division.

A. *Brady* Basics

The U.S. Supreme Court has recognized that criminal trials under our constitutional system must comport with due process.²⁰⁰ One component of that due process requirement involves prosecutors turning over exculpatory or impeaching evidence to the defense to be used in trial. In 1963, in *Brady v. Maryland*, the Court articulated that “the suppression by the prosecution of evidence favorable to an accused . . . violates due process where the evidence is material either to guilt or to punishment, irrespective of the good faith or bad faith of the prosecution.”²⁰¹

The logic underlying this due process requirement arises from the belief that government disclosure prevents misconduct, preserves fairness, and ensures public confidence in criminal justice.²⁰² As the Court stated in *United States v. Bagley*, “By requiring the prosecutor to assist the defense in making its case, the *Brady* rule represents a limited departure from a pure adversary model.”²⁰³ And, as the Court emphasized in *Brady* itself, “Society wins not only when the guilty are convicted but when criminal trials are fair; our system of the administration of justice suffers when any accused is treated unfairly.”²⁰⁴

In a series of cases, the Supreme Court has extended *Brady*’s exculpatory definition to include impeachment evidence (including information about witness bias, pecuniary interest, or inconsistencies)²⁰⁵ but restricted *Brady*’s

200. See, e.g., *Kyles v. Whitley*, 514 U.S. 419, 441–45 (1995); *United States v. Bagley*, 473 U.S. 667, 676 (1985); *Giglio v. United States*, 405 U.S. 150, 154 (1972); *Brady v. Maryland*, 373 U.S. 83, 87 (1963); see also Laurie L. Levenson, *Discovery From the Trenches: The Future of Brady*, 60 UCLA L. REV. DISCOURSE 74, 81–84 (2013); Daniel S. Medwed, *Brady’s Bunch of Flaws*, 67 WASH. & LEE L. REV. 1533, 1535 (2010).

201. *Brady*, 373 U.S. at 87. But see Cynthia E. Jones, *Here Comes the Judge: A Model for Judicial Oversight and Regulation of the Brady Disclosure Duty*, 46 HOFSTRA L. REV. 87, 88 (2017) (“[I]n over fifty years since the Supreme Court’s landmark 1963 decision, very little regulation or enforcement of the Brady disclosure duty has occurred.”); Cynthia E. Jones, *A Reason to Doubt: The Suppression of Evidence and the Inference of Innocence*, 100 J. CRIM. L. & CRIMINOLOGY 415, 428–31 (2010) (discussing intentional *Brady* violations by prosecutors).

202. See Mark D. Villaverde, Note, *Structuring the Prosecutor’s Duty to Search the Intelligence Community for Brady Material*, 88 CORNELL L. REV. 1471, 1487 (2003) (discussing the policies underlying *Brady* disclosure).

203. *Bagley*, 473 U.S. at 675 n.6; see also Thea Johnson, *What You Should Have Known Can Hurt You: Knowledge, Access, and Brady in the Balance*, 28 GEO. J. LEGAL ETHICS 1, 5–9 (2015) (discussing the adversarial balance).

204. *Brady*, 373 U.S. at 87.

205. See *Bagley*, 473 U.S. at 676 (“Impeachment evidence . . . as well as exculpatory evidence, falls within the *Brady* rule.”).

remedial force by emphasizing the materiality requirement.²⁰⁶ Beyond trial evidence, *Brady* material can be relevant to sentencing mitigation²⁰⁷ and suppression hearings.²⁰⁸ In addition, the Court has put an affirmative duty on prosecutors to seek *Brady* material available in their larger networks of investigative resources and agents. While many commentators have criticized *Brady* in application, the principles still apply and can be seen in criminal cases every day.²⁰⁹

This Article examines how *Brady* evidence might surface in big data prosecution systems like those discussed in Part I. Rethinking *Brady* disclosure and duties in a big data context will show the scope of the challenge ahead.

B. The Content of Required *Brady* Disclosures

The *Brady* doctrine requires the prosecution to reveal evidence “favorable” to the defense.²¹⁰ But the scope of what might be considered favorable has been challenging to define, since criminal prosecutions can vary greatly in subject matter and scale.²¹¹ For example, favorable evidence might come in the form of evidence that impeaches witnesses, exposes bias or corruption, or reveals evidentiary weaknesses. This Subpart examines *Brady* under five separate (but overlapping) categories: (1) eyewitnesses, (2) motives or biases, (3) capacity, (4) credibility, and (5) exculpatory facts. The goal here is to flag what has been considered *Brady* material as a framework to identify “favorable” material in big data prosecution systems. While this overview is necessarily incomplete, it offers examples of how to visualize the *Brady* problem in big data systems.

206. See *Weary v. Cain*, 136 S. Ct. 1002, 1006 (2016) (“Evidence qualifies as material when there is ‘any reasonable likelihood’ it could have ‘affected the judgment of the jury.’” (quoting *Giglio v. United States*, 405 U.S. 150, 154 (1972))).

207. See *Cone v. Bell*, 556 U.S. 449, 470 (2009) (“The documents suppressed by the State . . . [e]ach strengthen[] the inference that [the defendant] was impaired by his use of drugs around the time his crimes were committed.”).

208. See *Biles v. United States*, 101 A.3d 1012, 1020 (D.C. Cir. 2014) (“[S]uppression of material information can violate due process under *Brady* if it affects the success of a defendant’s pretrial suppression motion.”); *United States v. Gamez-Orduño*, 235 F.3d 453, 461–62 (9th Cir. 2000) (finding that *Brady* was violated in the pretrial context by suppression of evidence that helped demonstrate standing for Fourth Amendment search).

209. See Oran, *supra* note 23, at 111 (“The application of *Brady* and its progeny reveals two major concerns with the doctrine: (1) the discretion and subjectivity involved in a prosecutor’s disclosure decision and (2) the prosecutor’s difficulty in predicting what the court will later classify as material evidence.”); see also *infra* Subpart II.D.

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

211. See *Leka v. Portuondo*, 257 F.3d 89, 101–02 (2d Cir. 2001) (favorable material includes that which, through its “full exploration and exploitation . . . would have had a material bearing on defense preparation” (quoting *Grant v. Alldredge*, 498 F.2d 376, 382 (2d Cir. 1974))).

1. Eyewitnesses

Many criminal prosecutions involve human witnesses who are required to recount past facts, provide descriptions, conduct identifications, and describe events. Being human, inaccuracies and inconsistencies abound in the process of telling law enforcement facts about the case.²¹² But these statements are also critical to criminal prosecutions, sometimes being the only evidence linking a suspect to an offense.

a. Eyewitnesses and *Brady*

Eyewitness statements create many potential *Brady* problems. For example, eyewitnesses to a crime might not accurately identify a suspect, creating impeaching evidence for possible cross-examination. Identifications can be mistaken, so descriptive notes (height, weight, hair color, etc.) in an investigative file might not match the suspect. *Kyles v. Whitley* was a Supreme Court case in which several eyewitnesses provided inconsistent descriptions to investigating officers that did not match the defendant.²¹³ The Court stated, “the evolution over time of a given eyewitness’s description can be fatal to its reliability.”²¹⁴

Sometimes witnesses fail to identify the suspect when presented with a photo array, lineup, or other eyewitness identification procedure.²¹⁵ This failure to identify a suspect in an early proceeding can constitute *Brady* material (impeaching the certainty of a later identification).²¹⁶ Other times, witnesses may

212. See Memorandum from David W. Ogden, Deputy Att’y Gen., U.S. Dep’t of Justice, to Dep’t Prosecutors, Guidance for Prosecutors Regarding Criminal Discovery (Jan. 4, 2010) [hereinafter DAG Guidance Memo], <https://www.justice.gov/archives/dag/memorandum-department-prosecutors> [<https://perma.cc/2AD9-DP6E>] (requiring prosecutors to review disclosures of “[p]rior inconsistent statements” and “[s]tatements or reports reflecting witness statement variations”).

213. *Kyles v. Whitley*, 514 U.S. 419, 441–45 (1995) (determining that *Brady* principles were violated when the prosecution failed to disclose inconsistent eyewitness descriptions of suspect).

214. *Id.* at 444.

215. See *Mackabee v. United States*, 29 A.3d 952, 962–63 (D.C. Cir. 2011) (concluding that a witness’s failure to identify defendant in a photo array coupled with his statement that the shooter “sort of look[ed] like” the photos of two other people in the array was *Brady* information, yet the Court found that the evidence was not material because it was produced in time to use at trial).

216. See, e.g., *United States v. Jernigan*, 492 F.3d 1050, 1054 (9th Cir. 2007) (“In a case that turned *entirely* on eyewitness identifications, the presence of a second robber in the same area fitting the very same physical description was bound to ‘substantially reduce[] or destroy[]’ the ‘value’ of the eyewitness testimony.” (quoting *Kyles*, 514 U.S. at 441)); *Slutzker v. Johnson*, 393 F.3d 373, 387–88 (3d Cir. 2004) (finding that a witness statement that did not initially identify defendant was *Brady* information); see also *id.* at 386 (“One of the disputed reports was of a *third* interview with Mrs. DeMann, in which she not only ‘failed to identify’ Slutzker, but in fact

identify a different person, not the charged defendant, as the perpetrator.²¹⁷ These statements, which could be human mistakes or could be evidence that the police have accused the wrong person, must be revealed under the theory that the information impeaches the witnesses' trial identification and must go before the factfinder before that factfinder decides on the credibility and reliability of the witness.

Inconsistencies may also involve witnesses recounting different narratives of the crime or giving inconsistent statements. The sequence of events, timing, and observations offered by eyewitnesses can vary due to a host of influences. These different accounts can be considered *Brady* material if they undercut the planned trial testimony of prosecution witnesses.²¹⁸

b. Eyewitness Information in Intelligence-Driven Prosecution Systems

The open question is how to identify potential inconsistent or inaccurate eyewitness statements in big data systems. Uploaded into a cloud through an arrest alert system, or memorialized in a Wiki page, these details about what happened, who was involved, and motive can be potential *Brady* material. Yet, unless identified as such, the information will not be connected to the appropriate case.

Take a simple identification of a suspect in a stabbing case. Using a digital case management system, prosecutors might obtain a description from Witness 1—"White male, 5'11," brown hair, glasses, in mid 40s, kitchen knife"—and a description from Witness 2—"White male, 6'1" blond/brown hair, about 30 years old with a butcher knife." A prosecutor using a big data system, like a traditional system, should easily be able to see this inconsistency through the ordinary course of preparation for trial. There are differences in height, hair color, glasses, and the type of knife that would be within a single digital file or easily searchable by case.

positively stated that the man she saw was *not* Slutzker, and was significantly shorter than Slutzker.").

217. See, e.g., *Jamison v. Collins*, 291 F.3d 380, 389 (6th Cir. 2002) ("The suppression of a positive identification of different suspects by an eyewitness to the crime certainly disadvantaged Jamison in conducting his defense."); *White v. Helling*, 194 F.3d 937, 944–46 (8th Cir. 1999) (holding that *Brady* was violated when the state failed to disclose that a witness had initially identified another person in a robbery and failed to disclose notes revealing a suggestive series of questioning by police); *Clemmons v. Delo*, 124 F.3d 944, 950–52 (8th Cir. 1997) (holding that the *Brady* rule was violated when the state withheld communication showing that the witness had observed a different person commit the stabbing).

218. *Brady* was itself a case involving one inconsistent story about the person who killed the decedent. See *Brady v. State*, 174 A.2d 167, 168 (Md. 1961), *aff'd*, 373 U.S. 83 (1963).

But what if, in a separate debriefing in a different case a month later, Witness 3 talked about the same suspect, describing that suspect as “White/Hispanic, 5’8” young-looking with blond hair with a knife, ‘clearly defending himself.’” Debriefings routinely touch on all sorts of cases beyond the instant arrest and can take place weeks or months later. The inconsistent information would be in a Wiki but not connected to the trial case. How would the lead prosecutor know the details of this inconsistent eyewitness statement about a different case? How would she know any other information about the case exists in the system?

Or, what if Witness 1 were arrested himself (which happens routinely with debriefing witnesses) and, contradicting his earlier statement, tells officers that he did not get a good look at the suspect or did not really see the event? The statement would be available in the case in which he is a defendant, but it would not necessarily be linked to the case in which he is a witness.

Eyewitness inconsistencies need not be verbal. What if, in a separate digital file, detectives had observed the charged suspect at a different location during the time of the alleged crime or digital video footage caught the suspect somewhere else at the moment of the crime, giving him an alibi?²¹⁹ Geocoordinates that exculpate might exist, but how would the prosecutor know to find this information?²²⁰ How would she find those exculpatory bits of information? Unless flagged in the system as potentially relevant to another case, the information will not be linked to that case.

In addition to eyewitness identification, narrative stories about how or why an event occurred will be memorialized in the larger data system, but in separate and unconnected files. In a traditional investigation, any inconsistencies in details will be observable in the casefile. So, for example, if the detective speaks to Witness 1, Witness 2, and Witness 3, each of their narratives will hopefully be accessible to the prosecutor for potential inconsistencies in the same digital record. But if different law enforcement agents (detectives and prosecutors, for example) are pursuing other cases and within the debriefing sessions learn information about

219. See, e.g., Keith L. Alexander, *Authorities Said Video Showed a Man Committed Murder. He Spent 13 Days in Jail Before His Defense Team Proved He Didn't*, WASH. POST (Nov. 22, 2019), https://www.washingtonpost.com/local/public-safety/authorities-said-video-showed-a-man-committed-murder-he-spent-13-days-in-jail-before-his-defense-team-proved-it-didnt/2019/11/21/1fa7f36a-07b0-11ea-924a-28d87132c7ec_story.html [https://perma.cc/PNV2-KBEW] (providing an example of how digital evidence can play an exculpatory role in criminal cases).

220. See Kashmir Hill, *Imagine Being on Trial With Exonerating Evidence Trapped on Your Phone*, N.Y. TIMES (Nov. 22, 2019), <https://www.nytimes.com/2019/11/22/business/law-enforcement-public-defender-technology-gap.html> [https://perma.cc/3DAF-UXF2] (describing the problem of how defense counsel does not have the same access as prosecutors to digital evidence even when it might prove innocence).

our stabbing story, then how will that information be flagged for the stabbing prosecution? Unless flagged, how will the prosecuting attorney know that eyewitnesses in her case are talking to detectives in another case (with information uploaded in the centralized system)? Unless flagged, how would the information about self-defense ever make it back to the prosecutor preparing her case? Again, the inconsistency will exist in the shared system, but unless there is a way to flag all witnesses' statements, the information might not come to light.

As investigations can take months or longer and as opportunities to debrief suspects happen at unscheduled times, the need for a flagging system by person, case, incident, and other links grows in importance. Many witnesses become victims or defendants, and, over the years, the interrelated cases and relationships can get quite complicated (and yet still relevant). The challenge remains whether a search system can be built to flag and link such information.

Eyewitness identifications also show up in digital videos. Police body camera surveillance footage captures witness statements from incidents. The statements of Witness 1 might be both written down and stored in raw video footage. In some cases, the eyewitness statement will be easy to link to a particular investigation. Footage will be limited by time and place and officers will know to link it to an active case. For example, all videos recorded in connection with the immediate investigation of a stabbing will be linked to that case, usually by a common case number. But, many times, officers continue speaking with witnesses well after the initial investigation is over. On patrol the next day or week, officers might interact with individuals looking for insights into the crime. It is those identifications (or denials of knowledge) which are not easily connected to the original incident or linked by a case number. Unless designed to connect that video to a case, it will exist in the prosecution's possession yet remain unobtainable in the ordinary course of practice. These types of inconsistencies also arise out of factual statements of events.

While inconsistent identifications memorialized from interrogations are common to traditional prosecution, as well, the difference with big data systems is that the information is more available to prosecutors in a shared, searchable central database. While the same disconnect has long existed with physical police notes, now the evidence actually sits in the digital files and thus in the actual possession of the prosecutor.

Fixed surveillance videos might also impeach the narrative of eyewitnesses. In some cases, the recovered video footage could provide a different picture than what human eyewitnesses remember. This information would likely be impeaching *Brady* material, but it is not necessarily linked to a particular case. Fortunately, the (future) ability of digital video surveillance to be coded by time,

location, and event might make locating this information easier. The cataloging of video surveillance locations may also make obtaining evidence a bit easier.²²¹ For example, assume the stabbing takes place outside 127 West 127th Street in New York. With a quick search of the SCIM system, prosecutors could learn that there are six cameras recording inside and outside the building. Obviously, if prosecutors obtained the video surveillance data and observed an inconsistent version of events that counters a witness's narrative story, this would constitute *Brady* material. More interestingly, whether observed or not, because the video was fed to a central police command center and stored there, this information is in the possession of the government and would be a *Brady* violation if not disclosed.²²²

2. Motive/Bias

A witness can make honest mistakes, but they can also lie or try to deceive the factfinder. Understanding the motivation, animus, bias, or favor of a witness toward a party in a case is crucial to being able to evaluate the truthfulness of his or her testimony.

a. *Brady* and Motive-Bias Evidence

Information that prosecutors have in their files about these motivations that can impeach government witnesses is potential *Brady* evidence.²²³ After all, a deal for a lenient sentence, promised financial benefits, legal immunity, or other rewards can all potentially influence a witness's testimony by providing incentives to support the government's case.²²⁴ For example, the Supreme Court held in *Banks v. Dretke* that payments to a testifying witness must be disclosed because

221. See *supra* notes 163–164 and accompanying text (describing the SCIM video locations).

222. This analysis assumes connected video feeds. The question of whether exculpatory material that exists but is not reviewed by the government or in the government's possession may present a harder question for a *Brady* violation.

223. See also *United States v. Abel*, 469 U.S. 45, 52 (1984) (defining bias as “the relationship between a party and a witness which might lead the witness to slant, unconsciously or otherwise, his testimony in favor of or against a party.”).

224. See DAG Guidance Memo, *supra* note 212 (requiring disclosure of benefits to any testifying witness including but not limited to: “[d]ropped or reduced charges, [i]mmunity, [e]xpectations of . . . reduce[d] . . . sentence[s], [a]ssistance in . . . [other] criminal proceeding[s], [c]onsiderations regarding forfeiture of assets, [s]tays of deportation or other immigration status considerations, S-Visas, [m]onetary benefits, [n]on-prosecution agreements, [l]etters to other law enforcement officials (. . . [including] parole boards), setting forth the extent of a witness's assistance or making substantive recommendations on the witness's behalf, [r]elocation assistance, and [c]onsideration or benefits to . . . third parties”).

they can be used as impeachment.²²⁵ Similarly, a deal with the prosecution for a more lenient sentence can demonstrate bias in favor of the government.²²⁶ In *Bagley*, the Supreme Court found that a prosecution witness's deal with prosecutors should have been disclosed, noting that "[t]he jury's estimate of the truthfulness and reliability of a given witness may well be determinative of guilt or innocence, and it is upon such subtle factors as the possible interest of the witness in testifying falsely that a defendant's life or liberty may depend."²²⁷

A witness's past agreement with prosecutors as a cooperating witness is also relevant to evaluate present credibility,²²⁸ as is the witness's past work as an informant (which might give the witness incentive to curry favor in the future).²²⁹

A witness may also harbor personal animosity toward a defendant. Individuals in rival gangs,²³⁰ with adverse financial interests, or who harbor a personal animus may also generate evidence relevant to bias.²³¹ If prosecutors have this information in their files, *Brady* would require disclosure.²³²

225. *Banks v. Dretke*, 540 U.S. 668, 702–03 (2004) (concluding that the *Brady* rule was violated when the prosecution failed to disclose a witness's status as a paid informant).

226. See *Tassin v. Cain*, 517 F.3d 770, 778–79 (5th Cir. 2008) (concluding that the *Brady* rule was violated when the prosecution did not disclose that a witness expected to gain beneficial sentencing reduction for testifying on behalf of the government).

227. *United States v. Bagley*, 473 U.S. 675, 676 (1985) (quoting *Napue v. Illinois*, 360 U.S. 264, 269 (1959)).

228. See *Giglio v. United States*, 405 U.S. 150, 154–55 (1972) (holding that the *Brady* rule was violated when the government failed to disclose a nonprosecution agreement with a cooperating witness); *Maxwell v. Roe*, 628 F.3d 486, 509–11 (9th Cir. 2010) (discussing how the *Brady* rule was violated when the prosecution failed to disclose details of a witness's agreement which reduced his sentence in another case).

229. See generally *Robinson v. Mills*, 592 F.3d 730, 737 (6th Cir. 2010) ("Accordingly, since 'a defendant is entitled to broad latitude to probe credibility by cross-examination and to have the issues submitted to the jury with careful instructions,' the State's suppression of this evidence deprived Robinson of the opportunity to demonstrate Sims' untrustworthiness. Given juries' negative predisposition regarding informants, the trial jury would likely have been suspicious of Sims and cautious about her testimony. Such suspicion could have very likely redounded to Defendant's benefit." (quoting *On Lee v. United States*, 343 U.S. 747, 757 (1952))); *Schledwitz v. United States*, 169 F.3d 1003, 1015 (6th Cir. 1999) ("Bias is always relevant in assessing a witness's credibility.").

230. *Amado v. Gonzalez*, 758 F.3d 1119, 1139 (9th Cir. 2014) (discussing why the *Brady* rule was violated when the government did not disclose a probation report in the government's own records showing that the witness was in a rival gang).

231. See *Schledwitz*, 169 F.3d at 1015–16 (discussing why the *Brady* rule was violated when an expert that the prosecution claimed was "disinterested" was revealed to have been involved earlier in the criminal investigation than was disclosed to the defense).

232. See *Mendez v. Artuz*, 303 F.3d 411, 412–13 (2d Cir. 2002) (concluding that the *Brady* rule was violated when prosecutors did not disclose motive evidence of another suspect); *Schledwitz*, 169 F.3d at 1015 ("Bias is not limited to personal animosity against a defendant or pecuniary gain. Courts have found bias in a wide variety of situations, including familial or sexual relationships, employment or business relationships, friendships, common organizational memberships, and situations in which the witness has a litigation claim against another party or witness.").

b. Motive/Bias in Intelligence-Driven Systems

Big data systems contain information about witnesses' involvement in a particular case, as well as information about their relationships in the community and interaction with the criminal justice system more broadly. But these systems do not necessarily link the pieces of information together. For example, a witness might be recorded as describing his observation of a crime in one part of the prosecution database, and in a separate part of the prosecution database there might be a Wiki page about his status in a gang or his prior involvement in the criminal justice system. The link between the witness (as a witness) and the witness with motive or bias in a case, however, might not immediately be evident.

The question is how witness information can be vetted for possible motive or bias and automatically flagged in the system. For example, the accusation of a gang member will be subject to impeachment if he is in a rival gang, perhaps giving him a motive or animus against the defendant, or reason to protect a fellow gang member.²³³ The same factual statement may take on a different context when it is discovered that the defendant is a sworn ally (or even a close friend of) the witness. Gang rivalry, geographic rivalry, past acts of violence, or revenge will be mapped against others in the larger data system.²³⁴ The impeaching information may not be discovered unless a system is designed to identify the status of a witness and link that status favorably or unfavorably to other witnesses or cases in the relevant geographic area.

A witness's past relationship with law enforcement may also be important for determining the witness's motive to testify. Information about witnesses who have obtained benefits from prosecutors in the past, worked with police in the past, or

233. The term "gang member" is clearly simplistic and pejorative, yet, gang databases that label people as gang members have a significant role in modern policing. See Alice Speri, *In New York Gang Sweeps, Prosecutors Use Conspiracy Laws to Score Easy Convictions*, INTERCEPT (July 12, 2016, 10:25 AM), <https://theintercept.com/2016/07/12/in-new-york-gang-sweeps-prosecutors-use-conspiracy-laws-to-score-easy-convictions> [https://perma.cc/KU3P-MCTF] (describing a large gang prosecution in which the label of gang member was used in part to establish the conspiracy); see also K. Babe Howell, *Gang Policing: The Post Stop-and-Frisk Justification for Profile-Based Policing*, 5 U. DENV. CRIM. L. REV. 1, 16 (2015) (discussing the rise of gang databases in New York City); Kevin Lapp, *Databasing Delinquency*, 67 HASTINGS L.J. 195, 209–12 (2015).

234. IMPLEMENTATION GUIDE, *supra* note 25, at 23 ("[Violence] timelines are helpful tools to explain the history of violence in an area, educate law enforcement and prosecutors as to the significance of a defendant or gang, and analyze the nexus between recent violence and past violence. Typically, these violence timelines are accompanied by a map showing the location of the violent occurrence.").

themselves been accused of crime must be disclosed as impeachment evidence.²³⁵ Complicating matters is the fact that witnesses may have longstanding relationships with police that might not necessarily relate to a particular case or be obvious in a data management system. Cooperating witnesses, confidential informants, and people wishing to get out of their own criminal charges are central to modern prosecutions, but the relationships and deals with prosecutors are not always memorialized in the system (for security, privacy, and other reasons).

Motive and bias are more difficult to capture on surveillance or in other unstructured data systems. A video of a witness statement might provide clues about demeanor, attitude, and responsiveness in ways that might be impeaching to credibility. A witness who is clearly enraged or angry while giving a statement about a crime could be revealed as having an emotional bias against a party. Similarly, a reluctant witness, perhaps intimidated by law enforcement or hesitant for other reasons, will be shown on video to be reticent in ways that would not be visible in a paper record or acknowledged in testimony. Video can offer new clues that would otherwise be sanitized in the ordinary course of written documentation and trial testimony. But, of course, the difficulty is figuring out a way to identify human emotion or sensibilities in a way that could be useful for cases. Such subjective evaluations are both difficult in the ordinary course of human interaction, but even more so when it is not in the officer's interest to interpret a witness's motivations. The video may speak for itself about a witness's motivation for testifying and emotional state, but the video would not flag itself as relevant to motive or bias for particular witnesses in particular cases.²³⁶

At a more basic level, some motive/bias evidence might arise from location. As many violent crimes involve rival groups of individuals with territorial tendencies, the location of a video independent of its content might provide a clue to possible bias. Gang boundaries have been the site of identified violence and can be evidence of motive to defend a particular area.²³⁷ Intelligence-driven

235. See generally *Giglio v. United States*, 405 U.S. 150, 154–55 (1972) (asserting that impeaching evidence such as past deals with the prosecution falls under the Brady doctrine).

236. There is a growing concept that sentiment analysis can be programmed into artificial intelligence systems. See, e.g., Sophie Kleber, *3 Ways AI Is Getting More Emotional*, HARV. BUS. REV. (July 31, 2018), <https://hbr.org/2018/07/3-ways-ai-is-getting-more-emotional> [<https://perma.cc/96J6-FFUW>]. Although, there are also many others quite critical of this effort. See, e.g., Lauren Rhue, *Emotion-Reading Tech Fails the Racial Bias Test*, CONVERSATION (Jan. 3, 2019, 6:23 AM), <https://theconversation.com/emotion-reading-tech-fails-the-racial-bias-test-108404> [<https://perma.cc/JAZ6-2AML>].

237. Meg Sullivan, *Model Show Crimes Cluster on Gang Turf Borders*, U. CAL. (June 25, 2012), <https://www.universityofcalifornia.edu/news/math-model-shows-crimes-cluster-gang-turf-borders> [<https://perma.cc/ETL3-HBCW>] (discussing P. Jeffrey Brantingham et al., *The Ecology of Gang Territorial Boundaries*, 50 CRIMINOLOGY 851 (2012)).

prosecution has paid special attention to location-based crimes based on the understanding that those patterns can allow for intervention or deterrence of reciprocal acts of violence.²³⁸ Because digital cameras will have geolocational detail, and because those geolocational details may correlate with known gang rivalries, the location itself might provide potentially impeaching facts in trial.

3. Capacity

A related form of witness impeachment involves capacity—meaning whether there are external factors (physical or mental impairment) that might undermine the accuracy of a witness’s statement.²³⁹ A witness’s inability to accurately convey information to a factfinder raises a question of capacity and can be a source of impeachment.

a. Capacity and *Brady*

Capacity evidence generally involves impeachment evidence demonstrating that a witness’s ability to tell the truth or to accurately recall events may be impaired. For example, a witness might be under the influence of alcohol or some other mind-altering substance.²⁴⁰ A witness might have physical, cognitive,²⁴¹ or mental health²⁴² issues that could call into question the accuracy of their testimony. Knowledge about the inability to accurately provide testimony can be the basis for impeachment and, in the prosecution’s possession, may be *Brady* material.

238. Prosecutors with the Manhattan DA have brought cases against individuals that center in large part on the location of particular gangs. Alice Speri, *New York Gang Prosecutions Use Conspiracy Charges to Criminalize Whole Communities*, INTERCEPT (June 7, 2018, 8:50 AM), <https://theintercept.com/2018/06/07/rico-gang-prosecution-nyc> [https://perma.cc/C3YG-NN37].

239. 3 CHRISTOPHER B. MUELLER & LAIRD C. KIRKPATRICK, *FEDERAL EVIDENCE* § 6:80 (4th ed. 2019) (“Proof of sensory or mental incapacity is always relevant or (as the decisions often comment) ‘never collateral.’” (quoting *Behler v. Hanlon*, 199 F.R.D. 553, 558 (D. Md. 2001))).

240. See DAG Guidance Memo, *supra* note 212 (requiring review for disclosure of “[k]nown substance abuse or mental health issues or other issues that could affect the witness’s ability to perceive and recall events.”).

241. See *United States v. Kohring*, 637 F.3d 895, 906–07 (9th Cir. 2011) (determining that the *Brady* rule was violated when the prosecution did not disclose notes “that tend to show [prosecution’s witness] had difficulty remembering the details of key events”).

242. See *Gonzalez v. Wong*, 667 F.3d 965, 981 (9th Cir. 2011) (“There is a colorable argument that the psychological reports could have been used to impeach Acker. Impeaching Acker was important for Gonzales’s defense in both phases. Gonzales can, therefore, make a colorable argument that the withheld evidence was favorable to him.”); *Silva v. Brown*, 416 F.3d 980, 986–89 (9th Cir. 2005) (determining that the *Brady* rule was violated when the government did not disclose a deal requiring a witness to refrain from undergoing a psychiatric examination prior to testifying).

b. Capacity in Structured Big Data Systems

Witness capacity issues may be fairly easy to spot in big data systems. Notations about a witness's state of intoxication might make it directly into the digital file. Other circumstances leading to the inference of substance abuse might also be in the notes, including the place or time of the incident of the crime. A shooting early in the morning at a nightclub or in an area known for drug use might suggest the potential for intoxication (a capacity issue).

But other forms of capacity limitations might not make it into the files. Concerns about mental illness or physical impairments might not be recorded. Long term addiction problems may not be noted. Information from other government data sources (mental health services, addiction services) will not be easily available. A witness who might have a long history of drug arrests, low level quality of life crimes, and other indicia of addiction and mental health needs might have a documented history of red flags but not a documented record of capacity limitations. Unless there is a place to comment on the capacity of a witness, the information may never be memorialized.

In many ways, the information in police body cameras might be more revealing about capacity issues, although it is rarely marked as such. A review of the body camera footage may reveal intoxication, mental health crises, addiction, and other capacity defects (involving concerns around eyesight, age, infirmity, etc.). An elderly lady squinting hard to see would be quite revealing if caught on video but is the type of information that is less likely to make it into a detective's written notes. While usually not flagged as possible impeaching evidence, the footage of such a witness recounting events might be revealing of these physical or mental capacity issues and important evidence for impeachment.

One challenge with stored body camera footage is that it is collected and organized by event, not by person. Police might actually have footage of the witness inebriated or seriously compromised in other contexts and at other times, but not able to obtain that footage for review. Officers on patrol may routinely interact with individuals with chronic mental health issues or physical limitations, such as visual impairment, and while observable on video, the information likely would not be memorialized in a police report. While most footage about an event will be searchable through a data storage system like Evidence.com,²⁴³ historic or other information about the witnesses will be untraceable unless flagged in some manner.

243. See *Evidence.com for Prosecutors*, AXON, <https://www.axon.io/products/evidence-for-prosecutors> [<https://perma.cc/6P2K-3ZAM>] (last visited Apr. 11, 2017).

4. Credibility

A related form of witness impeachment involves credibility—specifically, when the prosecutor knows that a witness has not told the truth.²⁴⁴ Prior acts of dishonesty might involve past perjury,²⁴⁵ criminal acts demonstrating a level of deceit,²⁴⁶ or even past convictions which are relevant to credibility and, under the rules of evidence, admissible for impeachment.²⁴⁷

a. Credibility and *Brady*

Credibility issues can be raised with civilian witnesses and police witnesses. Relevant credibility determinations for civilian witnesses usually involve specific instances of proven false statements.²⁴⁸ For example, a conviction for perjury, a finding of deceit by a judicial officer, or an admitted false statement under oath would all impact credibility.²⁴⁹ Less clear is the impact on credibility of prior inconsistent statements not under oath or without a formal finding that the statement was untrue.²⁵⁰ Under ordinary rules of evidence, these types of credibility markers can be introduced into evidence to show a pattern of inconsistency in testimony but not for the truth of the matter asserted in the statements. In addition, reputational or opinion evidence about a witness can be introduced to attack credibility.²⁵¹ Prosecutors in possession of this type of information about a witness must make case-by-case determinations about whether this type of credibility evidence constitutes *Brady* material.

A parallel analysis accompanies police witnesses, although with added complications. Police officers routinely testify but are not always credited as

244. See, e.g., *United States v. Quinn*, 537 F. Supp. 2d 99, 109 (D.D.C. 2008) (“[T]he government itself concedes that when it has information about a witness who it is planning to call in its case in chief that indicates the witness has lied to the government about material matters during the course of the investigation, that information is *Brady* material.”).

245. *United States v. Cuffie*, 80 F.3d 514, 515, 518–19 (D.C. Cir. 1996) (holding that the *Brady* rule was violated when the government failed to disclose a witness’s prior perjury).

246. See *Benn v. Lambert*, 283 F.3d 1040, 1054–56 (9th Cir. 2002) (determining that the *Brady* rule was violated when the government failed to disclose prior acts of theft and lying by government witness); see also DAG Guidance Memo, *supra* note 212 (requiring review for potential disclosure of “[p]rior acts under Fed. R. Evid. 608” which covers a witness’s character for truthfulness or untruthfulness).

247. See DAG Guidance Memo, *supra* note 212 (requiring review for potential disclosure of “[p]rior convictions under Fed. R. Evid. 609” which covers impeaching convictions relevant for a witness’s credibility).

248. FED. R. EVID. 608(b)(1).

249. See FED. R. EVID. 608(b), 609.

250. See FED. R. EVID. 801(d)(1)(A), 613(b).

251. FED. R. EVID. 608(a).

testifying truthfully.²⁵² The problem of police perjury and “testilying” has been well documented in academic literature and in court experience.²⁵³ Many prosecution offices maintain a “do not call” list of police officers whose testimony cannot be trusted under oath and who should not be called to testify in court because of impeachment concerns.²⁵⁴ In some jurisdictions, prosecutors can obtain internal disciplinary records on police officers who might have credibility problems.²⁵⁵ For example, issues of police misconduct (failure to follow regulations, constitutional violations, avoidance of disciplinary consequences) can be introduced to impeach the credibility of officers and might be relevant to particular cases.²⁵⁶ Similarly, threats about past or future internal professional discipline can be considered motive to fabricate or to curry favor with the prosecution.²⁵⁷ Because police officers tend to be repeat players in criminal trials, information about prior bad acts or dishonesty may need to be turned over to the

252. See, e.g., Morgan Cloud, *Judges, “Testilying,” and the Constitution*, 69 S. CAL. L. REV. 1341, 1346 (1996).

253. See *id.* at 1350–55; Christopher Slobogin, *Testilying: Police Perjury and What to Do About It*, 67 U. COLO. L. REV. 1037, 1041–48 (1996).

254. See Terrence P. Dwyer, *Don’t Destroy Your Career: The Brady List and the Ruinous Impact of a Lie*, POLICEONE (Nov. 3, 2016), <https://www.policeone.com/legal/articles/dont-destroy-your-career-the-brady-list-and-the-ruinous-impact-of-a-lie-N8hzrj6qsZxZZPbe> [<https://perma.cc/UF3Q-JTN4>]; Pauline Repard, *The Secret List That Police Officers Don’t Want You to See*, SAN DIEGO UNION-TRIB. (Aug. 23, 2017, 2:35 PM), <https://www.sandiegouniontribune.com/news/public-safety/sd-me-brady-notebook-20170823-story.html> [<https://perma.cc/NTU7-XPZF>]; see also Emily Gillespie, *Legal System, Law Enforcement at Odds Over Brady List*, COLUMBIAN (Nov. 15, 2015, 6:02 AM), <http://www.columbian.com/news/2015/nov/15/legal-system-law-enforcement-at-odds-over-the-brady-list> [<https://perma.cc/QE8U-23AW>].

255. See Nick Place, *Double Due Process: How Police Unions and Law Enforcement “Bills of Rights” Enable Police Violence and Prevent Accountability*, 52 U. S.F. L. REV. 275, 293–94 (2018) (“If a police officer has credibility issues while testifying in court, prosecutors may put that officer on a ‘do not call’ or ‘Brady’ list as an unreliable witness not to be put in front of a court again.”).

256. See Jonathan Abel, *Brady’s Blind Spot: Impeachment Evidence in Police Personnel Files and the Battle Splitting the Prosecution Team*, 67 STAN. L. REV. 743, 749–51 (2015); see also *Mendez v. Artuz*, 303 F.3d 411, 416 (2d Cir. 2002) (“The defendant could also have used the suppressed information to challenge the thoroughness and adequacy of the police investigation. . . . Presented with detailed information about a contract murder plot and no indication that Mendez was involved or even associated with the participants, the police essentially did nothing.” (citation omitted)).

257. See, e.g., *Milke v. Ryan*, 711 F.3d 998, 1013–19 (9th Cir. 2013) (finding a *Brady* violation when prosecution failed to disclose that testifying officer had been suspended for abuse of authority and lied about the misconduct); see also INT’L ASS’N OF CHIEFS OF POLICE, *BRADY DISCLOSURE REQUIREMENTS: MODEL POLICY § IV(B)(1)(I)* (2009), <https://www.theiacp.org/sites/default/files/all/b/BradyPolicy.pdf> [<https://perma.cc/QVG5-CYV8>] (recommending disclosure of “[a]n officer’s excessive use of force, untruthfulness, dishonesty, bias, or misconduct in conjunction with his or her service as a law enforcement officer.”).

defense before testifying.²⁵⁸ In addition, other forms of professional misconduct may be relevant.²⁵⁹ The lack of investigation, or the sloppiness of an investigation, for example, may undermine the prosecution's case.²⁶⁰ As one goal of the defense is to discredit the prosecution's case, facts that go toward discrediting the trustworthiness of the police investigation can be considered *Brady* material.²⁶¹

b. Credibility Markers in Intelligence-Driven Systems

Court databases have long allowed prosecutors to run the records of testifying witnesses, and networked systems only increase the ease of this process. Criminal convictions in general and convictions for false statements in particular are now easily obtainable. Other types of credibility determinations (short of conviction), however, are harder to uncover. Even when a factfinder discredits a witness, there is usually no memorialization of this determination. A police witness could be found incredible after testifying in a hearing concerning one

258. See *United States v. Brooks*, 966 F.2d 1500, 1502–04 (D.C. Cir. 1992) (holding *Brady* requires a prosecutor to search internal police affairs files for possible impeachment information); see also *Nuckols v. Gibson*, 233 F.3d 1261, 1267 (10th Cir. 2000) (“There is no question here that the State willfully or inadvertently failed to disclose Ware’s involvement in the thefts and the Maxwell case. Those facts are impeaching. They would have provided the defense with the opportunity to call into question whether Ware had a motive for his testimony regarding the initiation of the interrogation resulting in Petitioner’s confession.”); *Milke*, 711 F.3d at 1013–19 (finding a postconviction *Brady* violation where the government failed to disclose testifying officer’s documented history of misconduct, pattern of *Miranda* violations, and false testimony).

259. See Abel, *supra* note 256, at 749 (2015) (“Because officers are members of the prosecution team, and because they know of the misconduct in their own files, *Brady* requires the prosecutor to learn of and disclose this information. But this duty to learn raises difficult line-drawing questions about how far the prosecutor must go in scouring the officer’s past.”).

260. See *Bowen v. Maynard*, 799 F.2d 593, 613 (10th Cir. 1986) (finding *Brady* information would have enabled trial counsel to raise serious questions concerning the “manner, quality, and thoroughness of the investigation that led to Bowen’s arrest and trial”).

261. See *id.* (“A common trial tactic of defense lawyers is to discredit the caliber of the investigation or the decision to charge the defendant, and we may consider such use in assessing a possible *Brady* violation.”); *Workman v. Commonwealth*, 636 S.E.2d 368, 375–77 (Va. 2006) (holding *Brady* material admissible in order to “discredit the police investigation”).

motion and yet still testify in another.²⁶² Most court systems do not capture this information, making it relatively difficult to study.²⁶³

As currently designed, intelligence-driven prosecution systems do not incorporate police misconduct records. This is a policy choice, not a technological choice, and one that could change. As a technical matter, incorporating links of each officer in the investigation system to perjury or credibility concerns would not be difficult.²⁶⁴ Each officer whose name appears in the files could be linked to the personnel database with any flags about his or her ability to testify. This would give prosecutors a sense of particular officers' conduct and behavior and, more importantly, their level of candor and truthfulness when testifying. The current system hides this information from prosecutors. Of course, prior unrelated misconduct is not necessarily *Brady* material, and professional discipline does not necessarily equate with impeachable evidence.²⁶⁵ But the fear of professional discipline can influence the ability to admit mistakes or to acknowledge actions that do not comport with standard practice. For example, while a prior use of force investigation might not impeach officer testimony in a drug case, it might be relevant in a resisting arrest case when the officer used force to subdue a suspect. The issue will be whether the officer's testimony is shaped by a desire to avoid another use of force investigation, thus providing a motive to testify a certain way.²⁶⁶

As prosecutors build their own big data systems, a choice must be made about whether information about testifying witnesses (civilian or police) will be included. In some jurisdictions like New York City, due to local rules, prosecutors

262. See Jon Loevy, *Truth or Consequences: Police "Testilying"*, LITIG., Spring 2010, at 13, 15 ("After examining more than 1,000 court dockets in gun cases, reporter Benjamin Weiser came to the conclusion that even when judges have rejected police officer testimony as disturbingly untruthful, nothing ever happens beyond a ruling adverse to the state in that particular case. The judge might find the sworn testimony of the police witnesses patently incredible or just plain false, but that is the end of it. Every prosecutor and judge who was interviewed seemed surprised when asked if perhaps something more should happen." (citing Benjamin Weiser, *Police in Gun Searches Face Disbelief in Court*, N.Y. TIMES (May 12, 2008), <https://www.nytimes.com/2008/05/12/nyregion/12guns.html> [<https://perma.cc/N75K-KV2Z>])).

263. But see John Kelly & Mark Nichols, *Search the List of More Than 30,000 Police Officers Banned by 44 States*, USA TODAY (Oct. 14, 2019, 5:26 PM), <https://www.usatoday.com/in-depth/news/investigations/2019/04/24/biggest-collection-police-accountability-records-ever-assembled/2299127002> [<https://perma.cc/2FCR-XXHN>] (a journalistic effort to compile a national list of police officer misconduct records).

264. See, e.g., *id.*

265. The misconduct would need to be material to credibility, reliability, motive to fabricate, etc.

266. Officers with prior use of force allegations may have a motive to fabricate to defend themselves from another such charge.

are unable to obtain access to police disciplinary records.²⁶⁷ In fact, in a striking open letter to NYPD, the Manhattan DA's office all but admitted it cannot meet its *Brady* requirements because the police will not provide prosecutors access to police disciplinary files.²⁶⁸

Unstructured data sets are also valuable for visualizing policing practices in a city. Data about officers can be mapped with precision—even, or especially, data that might undercut claims made by those officers in their reports. For example, if police claim to respond to the scene at a particular time, but their GPS coordinates show they were somewhere else at that moment, that data can be impeaching to their credibility. Recent instances of police body camera videos capturing the planting of evidence, the use of derogatory language, and instances of police brutality, underscore the type of *Brady* evidence that might exist in camera footage.²⁶⁹ With the political will to turn police surveillance inward on police, a whole host of revealing facts could be discovered,²⁷⁰ some of which might be impeaching evidence.

5. Exculpatory Facts

In a criminal prosecution, the government has the burden of proof. In order to meet that burden, it must demonstrate all of the elements of an offense. Evidence in prosecutor files that undermines any element of the crime charged, however, is potential *Brady* material.²⁷¹

267. McKinley, *supra* note 33.

268. Mike Hayes & Kendall Taggart, *The District Attorney Says the NYPD Isn't Telling Prosecutors Which Cops Have a History of Lying*, BUZZFEED NEWS (June 2, 2018, 6:02 PM), <https://www.buzzfeednews.com/article/mikehayes/nypd-cops-lying-discipline-disrict-attorneys-prosecutors> [<https://perma.cc/HC27-9GNF>].

269. See, e.g., Aamer Madhani, *Chicago Cops Accused of Covering Up Laquan McDonald Shooting to Go to Trial*, USA TODAY (Nov. 26, 2018, 8:11 PM), <https://www.usatoday.com/story/news/nation/2018/11/26/laquan-mcdonald-police-trial-david-march-joseph-walsh-thomas-gaffney/2115017002> [<https://perma.cc/LY6D-JTLY>]; Kevin Rector, *Baltimore Police Officer Found Guilty of Fabricating Evidence in Case Where His Own Body Camera Captured the Act*, BALT. SUN (Nov. 9, 2018, 12:00 PM), <https://www.baltimoresun.com/news/maryland/crime/bs-md-ci-pinheiro-ruling-20181109-story.html> [<https://perma.cc/7KUE-M9Q7>].

270. See Andrew Guthrie Ferguson, *The Exclusionary Rule in the Age of Blue Data*, 72 VAND. L. REV. 561, 594–635 (2019) (discussing inverting big data surveillance technologies to track police officers' conduct in an effort to improve police accountability).

271. See also U.S. DEP'T OF JUSTICE, JUSTICE MANUAL § 9-5.001(A)–(C) (2018) [hereinafter JUSTICE MANUAL], <https://www.justice.gov/jm/jm-9-5000-issues-related-trials-and-other-court-proceedings> [<https://perma.cc/KH7L-MDJY>] (requiring disclosure of “information that is inconsistent with any element of any crime charged”). This requirement may go beyond the mandate of *Brady*, but is largely consistent with its spirit.

a. Exculpatory Facts and *Brady*

Examples of exculpatory evidence might include evidence of self-defense in a murder case (undermining the unlawful nature of the killing).²⁷² Evidence supporting affirmative defenses like duress²⁷³ or insanity²⁷⁴ could mitigate culpability.²⁷⁵ Similarly, expert evidence that exonerates (nonmatching DNA in a sexual assault case, or nonmatching hair samples in a burglary) would be *Brady* material.²⁷⁶ Other expert testimony or evidentiary reports that might undercut the theory of prosecution must be turned over as *Brady* material.²⁷⁷ Finally, of course, direct evidence that shows someone else was involved in the crime would constitute *Brady* material.²⁷⁸

In prosecutions with identified suspects, these types of exonerating facts can show up through witness statements, physical evidence, forensic reports, or expert reports. In investigations without clear identified suspects, the facts that can build

272. See *Mahler v. Kaylo*, 537 F.3d 494, 500–03 (5th Cir. 2008) (finding a *Brady* violation where the prosecution did not disclose statements that decedent and defendant were actively fighting when gun went off, which could have been used for impeachment purposes during trial).

273. See *United States v. Udechukwu*, 11 F.3d 1101, 1105–06 (1st Cir. 1993) (finding a *Brady* violation when government did not disclose information that person defendant claimed coerced her to smuggle drugs was a known, prominent drug-trafficker supporting her duress defense).

274. See *United States v. Spagnuolo*, 960 F.2d 990, 993–96 (11th Cir. 1992) (finding a *Brady* violation when the government withheld a psychiatric report demonstrating that defendant may have a disorder, which could have made an insanity defense viable and otherwise changed defense strategy).

275. See JUSTICE MANUAL, *supra* note 271, § 9-5.001(C)(1) (requiring disclosure of information “that establishes a recognized affirmative defense”).

276. See *Sawyer v. Hofbauer*, 299 F.3d 605, 611–13 (6th Cir. 2002) (withholding of biological tests in sex assault case was found to be a *Brady* violation); *DiLosa v. Cain*, 279 F.3d 259, 265 (5th Cir. 2002) (finding a *Brady* violation when prosecution did not disclose exculpatory hair samples and evidence of another neighborhood break in, which supported defendant’s assertion that other men robbed his house and killed his wife); *Mitchell v. Gibson*, 262 F.3d 1036, 1061–64 (10th Cir. 2001) (inconsistent DNA testing found to be a *Brady* violation).

277. See *Benn v. Lambert*, 283 F.3d 1040, 1060–62 (9th Cir. 2002) (finding investigative report that fire was not caused by an arson was a *Brady* violation); *United States ex rel. Smith v. Fairman*, 769 F.2d 386, 391 (7th Cir. 1985) (finding that withholding ballistics results from the defense was a *Brady* violation); *Johnson v. State*, 38 S.W.3d 52, 56–59 (Tenn. 2001) (finding that withholding a police report was a *Brady* violation); *State v. Larimore*, 17 S.W.3d 87, 94 (Ark. 2000) (finding a withheld original medical examiner report was a *Brady* violation).

278. See *Trammell v. McKune*, 485 F.3d 546, 551–52 (10th Cir. 2007) (finding a *Brady* violation when evidence linking another person to the crime was not disclosed); *Scott v. Mullin*, 303 F.3d 1222, 1230–32 (10th Cir. 2002) (finding a *Brady* violation when prosecutors did not disclose another person had confessed to the crime); *Smith v. Sec’y of N.M. Dep’t of Corr.*, 50 F.3d 801, 834–35 (10th Cir. 1995) (finding a *Brady* violation when prosecutors did not disclose evidence that indicated third party rather than defendant had likely committed the offense); *Miller v. Angliker*, 848 F.2d 1312, 1323–24 (2d Cir. 1988) (finding a *Brady* violation when state did not disclose significant evidence of investigation into the guilt of another).

a case can also unravel it. Because prosecutors are sometimes required to build a case not knowing the ultimate target, the collection of evidence can often include information not helpful to their case. Sifting through the evidence required to build a case necessarily means putting aside less than helpful inconsistencies. Yet, if significant enough, those inconsistencies, false leads, and other suspects can constitute *Brady* material and should be turned over to the defense.

b. Exculpatory Facts in Intelligence-Driven Systems

The potential for case-weakening facts grows exponentially in big data prosecution systems. More facts provide more possible clues for other perpetrators or other theories of the case. Take, for example, an oft-used trial strategy called the “some other guy did it” defense.²⁷⁹ The defense strategy concedes that the crime occurred but claims that it was not the defendant but someone else who did the criminal act. Such defenses are difficult to bring because, unless the defense counsel can point to “some other guy” in actual fact (with motive and opportunity), judges are reluctant to allow defense lawyers to manufacture doubt about some hypothesized possible other suspect. But intelligence-driven systems offer a rich tapestry of other suspects, geographically connected to the precise area of the crime and tagged as being involved in similar types of crime. The systems even provide digital photo arrays of possible other suspects all included in the list of twenty-five priority offenders for each location. Defense lawyers could argue that police suspected two dozen other men of being the perpetrators of violence in this community, and that one of them just as likely committed the alleged crime. In fact, if the charged defendant is not on the primary target list, this alone could be useful if there were other individuals in the same area with the same pattern of criminality who might be more plausible suspects.

The same problem can happen in particular locations. For example, if police memorialize in their big data systems that two rival gangs control a particular geographic area and that reciprocal gang violence is fueling the shootings in that

279. See, e.g., *Patlan v. Ducart*, No. 15-CV-2372-TEH, 2016 WL 1056081, at *5 (N.D. Cal. Mar. 17, 2016) (“While a specific additional instruction might have been warranted if defendant had raised a complex theory regarding his innocence, his theory—essentially, ‘the other guy did it’—is a commonly encountered defense.” (quoting *People v. Patlan*, No. H038200, 2014 WL 772608, at *4 (Cal. Ct. App. Feb 26, 2014))); *Stanley v. Ayers*, No. CIV. S-95-1500-FCD-GGH-DP, 2008 WL 719234, at *3 (E.D. Cal. Mar. 17, 2008), *aff’d sub nom. Stanley v. Cullen*, 633 F.3d 852 (9th Cir. 2011) (“[T]he jury could have inferred guilt if counsel moved to determine petitioner was incompetent, which would have undermined petitioner’s ‘the other guy did it’ defense.”).

area, this information might create doubt in a prosecution of a suspect who is not a part of either gang but who is charged with a shooting in that area. The defendant would argue that the carefully detailed maps of gang violence and gang presence in the area of the shooting provide a reason to doubt that he was the perpetrator.

Patterns can also emerge from the data. A series of related crimes might be observable in the data that could identify the actual suspect, but also might be used to undercut the prosecution's case if another suspect's actions fit the pattern. In fact, the NYPD created an algorithm to identify such patterns for investigative use.²⁸⁰ The algorithm's *Brady* consequences, however, were not addressed. For example, if police suspect John to be involved in a series of robberies, then if not-John is arrested for a robbery in that specific area and fits that robbery pattern, the earlier suspicion of John will be potential *Brady* material in not-John's case by establishing suspicion of another person for a similar crime in a similar location. In the traditional prosecution system, these counterfactuals would be discounted and largely invisible to prosecutors, defenders, and judges, but now the mapping of criminal activity and the Crime Prevention Systems (CPS) of uncharged crimes makes this type of suspicion easy to visualize and difficult to ignore. There will be a visual representation in the file that police suspect John of robbing people in that exact area during that time period. Such a fact in a police detective's notebook would be *Brady* material, so it follows that it would also be *Brady* material in digital form.²⁸¹

As a final puzzle, consider how prosecutors investigating a case can create their own messy and distracting data trail of possible suspects simply by using big data investigatory tools. Imagine there is a shooting at 155th and Broadway with no known suspects.²⁸² The only clue given to responding officers is that someone with the nickname BamBam might have been the shooter. Using a system like Palantir Gotham—a powerful social network analysis system that can be used by investigators to identify places, people, and groups at specific geographic locations—prosecutors could geotag the location and draw up a list of known suspects who have been arrested for past shootings in the area. A map of three names pops up in the recent timeline of past shootings. Next, prosecutors query the priority offenders in a close geographic location. A list of twenty-five names (priority offenders) pops up, with five in the same general area of the shooting.

280. See Andrew Liptak, *The NYPD is Using a New Pattern Recognition System to Help Solve Crimes*, VERGE (Mar. 10, 2019, 6:09 PM), <https://www.theverge.com/2019/3/10/18259060/new-york-city-police-department-patternizer-data-analysis-crime> [<https://perma.cc/C2TH-L7L4>].

281. See Oran, *supra* note 23, at 116 (“Disclosure requirements under *Brady* do not vary by the nature of the evidence; the mandate is the same whether the source of the information is from a digital or traditional medium.”).

282. This is a hypothetical without a basis in real world facts.

Prosecutors also see that the area is controlled by a known violent gang with six active members. None of the three prior shooters or the five priority offenders or the six gang members can be associated with BamBam so the prosecutor queries the Manhattan DA system for any persons with the alias BamBam. The system returns the names of four individuals, BamBam, BamBam Cash, Bambi, and Bamba, none of whom live in the immediate area or are associated with the gang. But, using good old-fashioned police skills, detectives talk to each of the four and suspect that one of them is the shooter.

In one sense, this is terrific big data investigation, taking a single clue and narrowing the possible suspects down to one individual out of the millions who live in New York City. From another angle, however, prosecutors have created a host of other possible suspects. Prosecutors initially thought to investigate three other suspects who have committed the same crime in the same location. Prosecutors also identified five priority offenders who are known risks for violence in close geographic proximity. Prosecutors also thought to investigate the six active gang members in the area. Then police talked to three other possible BamBams. Each prosecutorial choice is revealed by the digital trail queried, making it hard to argue that it was not considered. Are these investigative actions of other suspects *Brady* material? While prosecutors might well believe they caught the correct BamBam, should defense lawyers merely accept that judgment or are they entitled to impeach the detective's conclusions? Should the data trail be turned over so that the defense can investigate the other suspects? This dilemma clearly raises privacy and secrecy problems for the other suspects, yet, in an analog world, a detective's notes about the three other BamBams and the suspicion of gang motivated shooting would likely be considered *Brady* material, so why not the digital equivalents? If prosecutors relied on this system to explain their narrowing of the suspect to this particular individual, the other suspect information might need to be revealed. Thus, it seems that simply using the technology potentially creates its own impeaching material.

C. *Brady's* Structural Weaknesses

The weaknesses of identifying *Brady* material in big data systems must be overlaid on top of longstanding concerns with the doctrine—a system of rules that many observers believe have largely failed to protect defendants.²⁸³ While beyond

283. See ANGELA J. DAVIS, ARBITRARY JUSTICE: THE POWER OF THE AMERICAN PROSECUTOR 130–32 (2007) (citing studies that show how often *Brady* doctrine fails to be applied resulting in the conviction of innocent defendants); Angela J. Davis, *The Legal Profession's Failure to Discipline Unethical Prosecutors*, 36 HOFSTRA L. REV. 275, 278–80 (2007) (discussing how *Brady* doctrine

the scope of this Article, other scholars have cataloged general concerns about why prosecutors fail to turn over exculpatory evidence and the consequences to the fair administration of justice.²⁸⁴ Structural pressures, lack of legal remedies, lack of professional discipline, and other reasons have been documented in a long line of court opinions and legal commentary.²⁸⁵ Intelligence-driven prosecution has the potential to worsen the existing *Brady* problems already identified in the literature.

Three traditional drivers of *Brady* failures are exacerbated by the move to big data prosecution. First, the growing volume of data heightens the problems of information sharing. By design, the volume of information increases beyond anything prosecutors ever had to handle before. There is simply more information being inputted into the system and thus requiring evaluation. Accompanying this expansion of information, however, is a corresponding reduction in markers of credibility and reliability. The information uploaded to a cloud system might have all sorts of reliable and unreliable clues without a way to flag which clues can be trusted. Similarly, debriefing statements are typed into the suspect's Wiki page with little ability to evaluate whether the source can be trusted, whether the facts have been verified, or if the information is out of date.²⁸⁶

Second, the proactive role prosecutors play in intelligence-driven investigation colors the perceived objective lens of charging decisions.²⁸⁷ Prosecutors become more akin to investigators, moving beyond the traditional

has largely failed in practice); Adam M. Gershowitz, *The Challenge of Convincing Ethical Prosecutors That Their Profession Has a Brady Problem*, 16 OHIO ST. J. CRIM. L. 307, 310–12 (2019) (noting statistics and cases about the prevalence of *Brady* violations).

284. E.g., Bennett L. Gershman, *Reflections on Brady v. Maryland*, 47 S. TEX. L. REV. 685, 715–21 (2006); Adam M. Gershowitz & Laura R. Killinger, *The State (Never) Rests: How Excessive Prosecutor Caseloads Harm Criminal Defendants*, 105 NW. U. L. REV. 261, 279–92 (2011); Jones, *supra* note 201, at 92; see also Alafair S. Burke, *Talking About Prosecutors*, 31 CARDOZO L. REV. 2119, 2131–35 (2010); Bruce A. Green, *Beyond Training Prosecutors About Their Disclosure Obligations: Can Prosecutors' Offices Learn From Their Lawyers' Mistakes?*, 31 CARDOZO L. REV. 2161, 2163–65 (2010); Medwed, *supra* note 201.

285. See, e.g., KATHLEEN M. RIDOLFI & MAURICE POSSLEY, N. CAL. INNOCENCE PROJECT, PREVENTABLE ERROR: A REPORT ON PROSECUTORIAL MISCONDUCT IN CALIFORNIA 1997–2009 (2010), <https://digitalcommons.law.scu.edu/cgi/viewcontent.cgi?article=1001&context=ncippubs> [<https://perma.cc/9GF2-E77M>]; see also Ken Armstrong & Maurice Possley, *Part 1: The Verdict: Dishonor*, CHI. TRIB. (Jan. 11, 1999, 2:00 AM), <https://www.chicagotribune.com/investigations/chi-020103trial1-story.html> [<https://perma.cc/S7UU-X98D>]; Steve Weinburg, *Breaking the Rules: Who Suffers When a Prosecutor Is Cited for Misconduct?*, CTR. FOR PUB. INTEGRITY (May 19, 2014, 12:19 PM), <https://publicintegrity.org/federal-politics/state-politics/harmful-error/breaking-the-rules> [<https://perma.cc/54NJ-F84M>].

286. This concern about data accuracy goes well beyond *Brady*, undermining the core of all data-driven criminal justice systems. See Wayne A. Logan & Andrew Guthrie Ferguson, *Policing Criminal Justice Data*, 101 MINN. L. REV. 541, 559–63 (2016).

287. See Ferguson, *supra* note 1, at 720.

role of merely evaluating the case brought to them by police.²⁸⁸ Prosecutors are studying criminal patterns and primary targets to proactively, aggressively prosecute them. As investigators, proactive prosecutors may see facts through the lens of guilt, minimizing or excusing impeaching or exculpatory facts that do not fit the investigative narrative. This is a natural human reaction, well documented in social studies about investigative bias.²⁸⁹ Such a proactive approach becomes even more of a problem with “primary targets” who are being targeted not necessarily for past crimes that can be prosecuted, but precisely because those crimes cannot be prosecuted. Combined, these factors can lead to targeting without the ability to double-check assumptions of guilt.

Finally, the longstanding problem of determining “materiality” in a pretrial status is now made even harder with more pieces of fragmentary evidence to consider.²⁹⁰ A *Brady* violation occurs when material exculpatory or impeaching evidence is withheld from the defense. But the definition of “material” (in *Brady* and other cases) originally arose from a posttrial appellate context when the import of the suppressed information could be evaluated based on the entire trial record.²⁹¹ A *Brady* violation, thus, only occurs on appeal when a court finds that the withheld evidence was material to the final outcome of the case. But a prosecutor’s *Brady* obligation kicks in before trial, not after appeal.²⁹² In a pretrial context, then, prosecutors have a *Brady* obligation that is broader than what an

288. See *supra* note 15.

289. See, e.g., Alafair Burke, *Neutralizing Cognitive Bias: An Invitation to Prosecutors*, 2 N.Y.U. J.L. & LIBERTY 512, 515 (2007); see also generally Alafair S. Burke, *Improving Prosecutorial Decision Making: Some Lessons of Cognitive Science*, 47 WM. & MARY L. REV. 1587 (2006); Keith A. Findley & Michael S. Scott, *The Multiple Dimensions of Tunnel Vision in Criminal Cases*, 2006 WIS. L. REV. 291.

290. *United States v. Bagley*, 473 U.S. 667, 682 (1985) (“[*Brady*] evidence is material only if there is a reasonable probability that, had the evidence been disclosed to the defense, the result of the proceeding would have been different.”).

291. See Michael Serota, *Stare Decisis and the Brady Doctrine*, 5 HARV. L. & POL’Y REV. 415, 422–25 (2011) (discussing *United States v. Sudikoff*, 36 F. Supp. 2d 1196 (C.D. Cal. 1999), and the trial court’s recognition that the posttrial materiality standard should not apply to pretrial considerations of whether information is material to the defense).

292. As Justice Anthony Kennedy once had to explain to government counsel during oral argument: “I think you misspoke when you . . . were asked what is . . . the test for when *Brady* material must be turned over. And you said whether or not there’s a . . . reasonable probability . . . that the result would have been different. That’s the test for when there has been a *Brady* violation. You don’t determine your *Brady* obligation by the test for the *Brady* violation. You’re transposing two very different things.” Transcript of Oral Argument at 49, *Smith v. Cain*, 565 U.S. 73 (2012) (No. 10-8145), http://www.supremecourt.gov/oral_arguments/argument_transcripts/10-8145.pdf [https://perma.cc/7S2Z-4SKH] (statement of Justice Kennedy to government’s appellate counsel).

appellate court might consider on appeal to be a *Brady* violation.²⁹³ With more big data information, and more complex relationships between witnesses, places, and groups, this pretrial materiality question becomes even more fraught.

D. The Duty of Disclosure

Despite the challenges, and despite the fact that the scope of *Brady* remains contested, the duty to search for *Brady* information remains clear (even in big data systems).²⁹⁴ Prosecutors have a constitutional and ethical duty to search for favorable information in their possession.²⁹⁵ This duty to disclose *Brady* material developed in response to traditional (predigital) prosecution practices. *Brady*'s initial requirement was that prosecutors reveal exculpatory information in their casefile,²⁹⁶ a requirement that was extended to make clear that prosecutors had an affirmative duty to learn about *Brady* information beyond those files (for fear that a prosecutor could simply choose not to search in order to avoid triggering the disclosure requirement).²⁹⁷

The Supreme Court subsequently extended the *Brady* duty to require a search of files from the entire prosecution team, investigating agents, and the police.²⁹⁸ *Brady* disclosures, thus, do not turn on any individual prosecutor's knowledge, but on the imputed knowledge of the entire prosecution team. The Court in *United States v. Bagley* articulated a constructive knowledge/possession rule to hold prosecutors responsible for the information known and possessed by

293. See Gershowitz, *supra* note 283, at 311 ("Multiple scholars have observed that it is quite difficult for prosecutors, who are looking at a case from the prosecution's perspective with the belief that a defendant is guilty, to easily see all of the evidence that a defendant might use to show he is innocent." (footnote omitted)).

294. See Oran, *supra* note 23, at 115–16 ("*Brady* established a sweeping obligation on prosecutors. As noted, the doctrine requires prosecutors to shoulder the responsibility of providing the defense with all favorable evidence they know of, or should know of, that could 'undermine the confidence' in a trial's outcome."). But see Jones, *supra* note 201, at 98 ("More than fifty years after the Court decided *Brady*, there is still a constant flow of litigation in state and federal courts to resolve fundamental issues regarding the scope of the *Brady* disclosure duty.").

295. See Jonathan M. Fredman, *Intelligence Agencies, Law Enforcement, and the Prosecution Team*, 16 YALE L. & POL'Y REV. 331, 349 (1998) ("But beyond information already in its possession, the prosecution may need to search for material in the hands of some other agency.").

296. See *Banks v. Dretke*, 540 U.S. 668, 696 (2004) ("A rule... declaring 'prosecutor may hide, defendant must seek' is not tenable in a system constitutionally bound to accord defendants due process.").

297. *Kyles v. Whitley*, 514 U.S. 419, 437 (1995) ("[T]he individual prosecutor has a duty to learn of any favorable evidence known to the others acting on the government's behalf in the case, including the police.").

298. See *id.* at 437–38.

law enforcement investigators.²⁹⁹ Further, in *Pennsylvania v. Richie*, the Court extended this due diligence duty to search beyond traditional law enforcement and to records not even known to the prosecutor.³⁰⁰ Moreover, the Court held in *Kyles v. Whitley* that prosecutors must develop systematic “procedures and regulations” to meet the prosecution’s *Brady* obligation resulting from many different lawyers and investigators working the same case.³⁰¹

This intentional broadening of the affirmative duty to search prosecution materials has been incorporated into internal prosecution rules and ethical standards.³⁰² In practical effect it means that prosecutors are responsible to search and disclose information from formal and informal investigative reports,³⁰³ police records,³⁰⁴ expert records, and other branches of government closely aligned with the prosecution.³⁰⁵ The current standard—still based on the fact that government

299. See *United States v. Bagley*, 473 U.S. 667, 689–90 (1985); see also *Jones*, *supra* note 201, at 90 (“The Court has also recognized that *Brady* imposes on the prosecutor a due diligence obligation to investigate and collect all favorable information in the prosecutor’s own files, as well as information held by any member of the prosecution team (i.e. law enforcement officers, forensic analysts).” (footnote omitted)).

300. See *Pennsylvania v. Ritchie*, 480 U.S. 39, 57–58 (1987).

301. *Kyles*, 514 U.S. at 438.

302. See DAG Guidance Memo, *supra* note 212 (“Prosecutors should have candid conversations with the federal agents with whom they work regarding any potential *Giglio* issues . . .”); *id.* (requiring prosecutors to review “case-related communications” which “*may be* memorialized in emails, memoranda, or notes” (emphasis added)); *id.* (requiring review of an investigative agency’s files and noting that if favorable “information is contained in a document that the agency deems to be an ‘internal’ document . . . it may not be necessary to produce the internal document, but it will be necessary to produce all of the discoverable information contained in it”).

303. See *id.* (acknowledging that “the format of the information does not determine whether it is discoverable,” that the government must search for favorable information in “factual reports” “factual discussions” or “factual information obtained during interviews” and “information that the prosecutor receives during a conversation with an agent or a witness is no less discoverable than if that same information were contained in an email”).

304. See *Barbee v. Warden, Md. Penitentiary*, 331 F.2d 842, 846 (4th Cir. 1964) (“Failure of the police to reveal such material evidence in their possession is equally harmful to a defendant whether the information is purposely, or negligently, withheld The police are also part of the prosecution, and the taint on the trial is no less if they, rather than the State’s Attorney, were guilty of the nondisclosure.”).

305. See DAG Guidance Memo, *supra* note 212, 9-5.001 (B)(2) (defining the “prosecution team” to which the obligation of *Brady* extends, and noting that “[i]t is the obligation of federal prosecutors, in preparing for trial, to seek all exculpatory and impeachment information from all the members of the prosecution team. Members of the prosecution team include federal, state, and local law enforcement officers and other government officials participating in the investigation and prosecution of the criminal case against the defendant.”); see, e.g., *United States v. Bryant*, 439 F.2d 642, 650 (D.C. Cir. 1971) (“The duty of disclosure affects not only the prosecutor, but the Government as a whole, including its investigative agencies.”); see also *Smith v. Sec’y of N.M. Dep’t of Corr.*, 50 F.3d 801, 824 (10th Cir. 1995) (“[T]he ‘prosecution’ for *Brady* purposes encompasses not only the individual prosecutor handling the case, but also extends to

evidence might be physically dispersed across different agencies and agents—requires affirmative due diligence to search for possible *Brady* material. All these rules about constructive possession, due diligence, and systematic procedures also apply to the digital realm and whatever type of big data or cloud-based information storage system a prosecution office chooses to adopt.

In fact, if designed appropriately, big data prosecution systems should make this due diligence obligation easier to manage. Searchable data collection systems reverse the trend of information diffusion. Instead of needing to search the files of various different actors who might have favorable information in different locations, big data systems centralize data collection. Instead of needing to search a detective's notebooks, now the notebooks are part of the prosecutor-driven data storage system. If designed thoughtfully and conceived of as a central trove of law enforcement data, this linkage should simplify the prosecutor's burden to search for favorable information.

In centralizing data into a single searchable and accessible system, the move toward intelligence-driven prosecution also simplifies the question of whether a prosecutor has possession (real or constructive) of exculpatory or impeaching information. They do. And, because they do, prosecutors have an obligation to find and retrieve any constitutionally relevant material. The harder question is how to build systematic procedures and regulations to find information when the systems were not originally designed to flag potential *Brady* information. This is the subject of the next Part.

III. REENGINEERING INTELLIGENCE-DRIVEN *BRADY*

The design problem at the heart of intelligence-driven prosecution requires both a theoretical and technological fix. The theoretical response parallels the intelligence-driven prosecution strategy itself, recognizing that a move from a reactive, suspect-based prosecution strategy to a more proactive, contextual understanding of places, people, groups, and patterns requires a new way to visualize *Brady*. In an intelligence-driven prosecution system, *Brady* should be understood to include a proactive search for relationships and patterns, a deeper and broader quantitative search through shared systems, a structured process for

the prosecutor's entire office, as well as law enforcement personnel and other arms of the state involved in investigative aspects of a particular criminal venture." (footnote and citation omitted)); *United States v. Brooks*, 966 F.2d 1500, 1503 (D.C. Cir. 1992) (duty to search for *Brady* extends to "branches of government closely aligned with the prosecution" (quoting *United States ex rel. Smith v. Fairman*, 769 F.2d 386, 391 (7th Cir. 1985))).

qualitative assessments, and even the possibility of predictive analytics to flag potential *Brady* material.³⁰⁶

The technological response involves redesigning intelligence-driven systems to flag and find *Brady* material consistent with this theory. Fortunately, precisely because of the networked technology at issue, big data information systems can be reengineered to flag, link, evaluate, and predict relevant data for prosecutors. This Part suggests a way to engineer a theoretical and technological fix to *Brady* practice.

A. Theory: Networked *Brady*

Brady, and every case that makes up the *Brady* doctrine, came out of a reactive, traditional, “small data” prosecution system. Unsurprisingly then, courts often conceive of the scope of exculpatory or inculpatory evidence through *Brady*’s small data lens. Usually, the facts are suspect-focused, case-specific, and brought to the prosecutor’s direct attention through police reports or investigation. Even if the duty of disclosure extends outwards to the entire prosecution team, the *Brady* material usually lives somewhere in the physical file that the trial prosecutor keeps in her office.

Networked data sharing systems, linking tens of thousands of case files, an equal number of uncharged cases, and potentially millions of other sources of information, necessarily broaden how prosecutors should think about *Brady*. A new theory must incorporate the changes inherent in intelligence-driven prosecution, including: (1) a relational understanding of places, groups, people, crimes, uncharged acts, motives, cooperation agreements, and patterns; (2) an understanding of the broadened scope (different systems across different jurisdictions) and depth (spanning many years) of available data; (3) a qualitative assessment of the facts and witnesses; and (4) a proactive approach that analyzes, and perhaps even identifies, case weaknesses.

1. Relational Understanding

As discussed throughout this Article, big data prosecution adds complexity to the idea of exculpatory or impeaching information because there are more relationships to consider. How witnesses relate to one another, to a location, to a pattern of criminal activity, or to a group are all made a bit more difficult because

306. Of course, this creates the same concerns as those raised against predictive analytics to identify criminal actors. See generally Andrew Guthrie Ferguson, *Policing Predictive Policing*, 94 WASH. U. L. REV. 1109 (2017). The reliability of such predictive systems is still contested.

there is more connected information in the same searchable data system. Uncharged activities that would not necessarily make it into a casefile may need to be considered. Cooperation agreements, debriefing notes, motives, or just the accumulated suspicions and neighborhood rumor in a Wiki might now need to be factored into a more complex analysis of the facts, witnesses, and contextual background of the crime. While the basic process is the same as it always has been for a prosecutor, the amount of information and the overlapping connections is now just more complex. A case is not just a case but an event in a longer timeline of relational and connected actions and reactions. A criminal actor is not just an individual but a part of a connected network of groups, associations, and motivations. A place is not just a background fact but part of the environmental backcloth³⁰⁷ of a pattern of criminal activities and geographical vulnerabilities. The result of this change in mindset is that, instead of a single casefile of notes, theories, interviews, and possible leads, now the entire collected and collective understanding of a city's crime patterns and relationships is in prosecutors' hands. This means prosecutors must think about a broader conception of possible (and available) *Brady* material.

2. Quantitative Understanding

Big data also creates a very real (and related) quantitative change. Prosecutors can now visualize years' worth of historical data and information from outside their jurisdiction. Traditional temporal limitations and geographic silos are broken down by data collection and information sharing. In the same way that mapping historic crime patterns strengthens investigations, so it might unearth evidence that undermines those investigations. Similarly, information that might be known by another jurisdiction or another part of the criminal justice system (probation, parole, immigration, gang intelligence) will now be searchable and accessible in one unified system. The growing move to seamlessly share data correspondingly creates new clues that might undercut the clarity of a criminal case. The digital equivalent of the traditional casefile will now include years' worth of data from all types of sources. These sorts of changes do not impact the responsibilities of a prosecutor, but they significantly expand the scope and depth of how prosecutors must think about *Brady*.

307. See Joel M. Caplan, *Mapping the Spatial Influence of Crime Correlates*, CITYSCAPE: J. POL'Y DEVELOPMENT & RES., Jan. 2011, at 57, 60 (discussing how the terminology of an "environmental backcloth" is used to describe the dynamic realities of areas of heightened crime with "crime attractors" and "crime generators" which contribute to the existence of crime hotspots).

3. Qualitative Understanding

The sheer amount of data available today also demands a more careful qualitative assessment from prosecutors. Traditionally, prosecutors were able to make educated qualitative assessments about their evidence because they had direct access to witnesses, police officers, evidence, and the casefile. Prosecutors put on evidence they could trust and could vet that evidence because they could identify the provenance of the information. If the casefile said, “Witness 1 only got a quick look at the shooter. Believes it was gang related,” prosecutors can follow up with the witness and the officer and ask the meaning of “quick” or why they perceived it to be “gang related.” But if that same comment sits on a month-old CPS Wiki, there might not be any way to figure out how to qualitatively assess its worth as evidence. The link to the gang might be impeaching to the government’s prosecution theory, or it might be completely mistaken and misleading. Without some way to qualitatively assess the credibility, reliability, and source of the information, its value as evidence erodes. As such, prosecutors must think about the inputs going into the system in qualitative ways. One way to think about this problem is by asking about the “lineage” of the information or its “traceability.”³⁰⁸ Being able to find the source of a fact can help the process of evaluation. All evidence is not of the same caliber, and with growing information systems this reality will become more important. *Brady* in this context will require more emphasis and investment in systems to verify and trace information sources.

4. Proactive Understanding

Finally, in the same way hidden patterns and predictive assessments can emerge from the investigatory data, such patterns and predictive assessments can improve the proactive identification of *Brady* material. Again, this is just applying the theory of intelligence-driven prosecution to the *Brady* problem. As one relatively simple example, imagine that prosecutors arrest an individual and, in exchange for his testimony, provide him with a nonprosecution agreement.³⁰⁹ In the case in which he is a witness, this impeaching information about his motive to

308. As will be discussed in the next Part, some technologies can trace lineage as part of their operation. See generally Joe Depeau, *Graph Technology is in the POLE Position to Help Law Enforcement*, NEO4J (Apr. 19, 2018), <https://neo4j.com/blog/graph-technology-pole-position-law-enforcement> [<https://perma.cc/3QK8-MMTN>].

309. A nonprosecution agreement is a contractual understanding that prosecutors will drop certain charges or reduce charges against a defendant in return for the defendant’s helpful assistance in criminal prosecutions.

curry favor with the government is straightforward *Giglio*³¹⁰ material that would be disclosed under ordinary practice.³¹¹ But it may not resurface in another case at all or for several years. Yet, the relationship of being a past government witness who has received benefits is still material to the witness's credibility. In fact, every witness who has received government favors (*Giglio*) or government money (*Banks v. Dretke*)³¹² should be proactively identified so that this affirmative identification of a possible *Brady* issue is flagged if they show up in the system again. Furthermore, family members with whom they are associated via social network analysis should also receive a potential flag. Similar types of proactive identification can be done for witnesses who have been found not credible due to perjury, capacity issues, or other problems.

The same type of proactive mentality should extend to big data video and sensor systems. Whereas an exculpatory video in the prosecutor's immediate file would be turned over to the defense, a proactive vision of *Brady* would encourage prosecutors to consider finding the potential video or sensor data available using the maps of networked cameras or sensors around the city. If, for example, after a shooting in which the lookout identification was for a man in a black coat and a suspect in a black coat is arrested, the relevant surveillance video showed five men in black coats fleeing the scene, such footage should be turned over as potential *Brady* information. Again, instead of simply relying on reactive investigatory clues, prosecutors will need to affirmatively search for related evidence. The availability of more data requires a proactive approach to that data.

To be clear, the suggestion of a networked theory of *Brady* is not a critique that prosecutors have not been thinking in broad or proactive ways. Obviously, prosecutors understand that the constitutional commands of the Due Process Clause must be followed. But the shift from a small data, reactive model of prosecution to a big data, proactive model makes following those constitutional commands more difficult. Reworking and broadening *Brady* theory makes it possible to align the constitutional requirements to the new challenges. The open question is how to actually reengineer the system. This technological fix is the subject of the next Subpart.

B. Technology: Incorporating Networked *Brady* by Design

Designing a system to proactively find *Brady* information requires a focus on flags and network links built within structured and unstructured data systems.

310. *Giglio v. United States*, 405 U.S. 150 (1972).

311. *See id.* at 154–55.

312. *Banks v. Dretke*, 540 U.S. 668 (2004).

Again, fortunately, these are exactly the type of technologies that underlie the growth of intelligence-driven prosecution and big data analytics. This Subpart examines what such a redesign project might look like, borrowing a bit from an analogy to the Intelligence Community in the national security context. Whether intentional or unintentional, the intelligence-driven model of prosecution parallels intelligence collection methodologies in the national security space. Lessons from that area can be adapted to ensure that prosecution offices interested in turning their offices into quasi-intelligence operations learn from a full embrace of the cautions of data systems built for the Intelligence Community.

1. Flags—Inputting *Brady*

Inputs are foundational to intelligence-driven prosecution. Each case, crime, debriefing, or Wiki page involves the inputting of information. As it currently stands, the inputs come from all types of sources (police, prosecutors, community members, witnesses, defendants) and are entered into the system without differentiation in terms of reliability, connection, or more nuanced categorization. Whether 100 percent credible or largely fanciful, a debriefing tip is included in a digital file. Connections might be recognized (relating to prior cases or gang affiliation), but the information is not automatically linked to those other cases or digital files. Events are categorized by crime type but not by a whole host of other possible identifiers (location, associations, motive). Essentially, the intelligence-driven system was built to vacuum up data potentially useful for identifying perpetrators in particular prosecutions (generating suspects), but not to evaluate the quality of the information or its relationship to other cases, places, or events.

Introducing technology to flag inputs for various criteria would allow the system to better identify exculpatory or impeaching evidence. This type of flagging system is routinely used in intelligence gathering where systems exist to weigh credibility determinations of tips, study link analysis across countries, and record categorical identifiers for a host of different intelligence agencies,³¹³ thus allowing

313. See U.S. GOV'T, A TRADECRAFT PRIMER: STRUCTURED ANALYTIC TECHNIQUES FOR IMPROVING INTELLIGENCE ANALYSIS 2 (2009) [hereinafter TRADECRAFT PRIMER], <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/Tradeecraft%20Primer-apr09.pdf> [<https://perma.cc/2F93-4ENW>] (providing an example of how the intelligence community uses structured analytic techniques for investigation and monitoring); see also STEPHEN ARTNER ET AL., ASSESSING THE VALUE OF STRUCTURED ANALYTIC TECHNIQUES IN THE U.S. INTELLIGENCE COMMUNITY 2 (2016) ("SATs are methods of organizing and stimulating thinking about intelligence problems. These methods aim to make the analytic process conscious and transparent, thus reducing the probability of errors caused by numerous cognitive biases that go unchallenged in unstructured and intuitive analysis.").

analysts to keep track of disparate clues of information across the international stage.³¹⁴

A flagging system for inputs in the big data prosecution context would involve three additional steps for data files: (1) weighting the reliability and validity of information; (2) marking potential links to other cases, persons, or groups; and (3) identifying the crime type, place, group, and time of the information to see its relationship to past crime patterns. This flagging of information inputs can be done manually, established as part of system templates, or potentially even automated.³¹⁵ This Subpart will briefly sketch out the design concepts, and then address some of the problems with the suggestion.

a. Reliability Flags: Credibility

As discussed, not all information in big data systems is of the same quality. A witness could be completely trustworthy or a complete fraudster, and the investigating officer might have a good sense about their credibility. The task is to build into the system a place to mark the level of reliability of the information provided. In so doing, the system will be able to signify the qualitative reliability of different sources of evidence. A detective talking to an arrestee who appears to be under the influence of drugs might have reservations about the information the arrestee provides. The Intelligence Community has rules for “credibility assessment” and “source validation,” in such a context,³¹⁶ both of which require formal evaluation of the reliability of the information. Tips from intelligence assets do not become unquestioned fact without thorough assessments of the validity

314. A flagging system is also used for domestic law enforcement purposes in the context of suspicious activity reports and gang intelligence workflows. See generally Nicolas Duque Franco, *Suspicious to Whom? Reforming the Suspicious Activity Reporting Program to Better Protect Privacy and Prevent Discrimination*, 43 N.Y.U. REV. L. & SOC. CHANGE 611, 621 (2019); K. Babe Howell, *Fear Itself: The Impact of Allegations of Gang Affiliation on Pre-Trial Detention*, 23 ST. THOMAS L. REV. 620, 628 (2011); Alice Speri, *NYPD Gang Database Can Turn Unsuspecting New Yorkers into Instant Felons*, INTERCEPT (Dec. 5, 2018, 12:16 PM), <https://theintercept.com/2018/12/05/nypd-gang-database> [https://perma.cc/9FUM-FP53].

315. In fact, these flags are already entered during the investigation. See IMPLEMENTATION GUIDE, *supra* note 25, at 10 (“For example, the management of the Trial Division, which supervises all street crime cases, flags certain cases as “Executive Significant Matter”. That notation will appear on the first screen that an ADA sees when the case is accessed. In this way, the ADA knows that this defendant has been identified as a driver of crime and that significant efforts should be made on the case in order to reduce crime long-term and improve public safety.”).

316. See OFFICE OF COUNTERINTELLIGENCE, DEF. INTELLIGENCE AGENCY, TERMS AND DEFINITIONS OF INTEREST FOR DoD COUNTERINTELLIGENCE PROFESSIONALS (2011), https://www.dni.gov/files/NCSC/documents/ci/CI_Glossary.pdf [https://perma.cc/A55A-5SEL].

behind the information.³¹⁷ The same type of cautionary flag system needs to be built into information systems collecting investigative police data. The information can be inputted, but some form of cautionary marker should be included so that prosecutors can review the information with the appropriate context. In the Intelligence Community, such cautions have been formalized into specific analytical structures and tools.³¹⁸

All that is required for big data prosecution systems is to create a flagging system for any information that might warrant further qualitative evaluation or investigation. This is consistent with the suggestion in *Kyles* that prosecution offices develop systematic practices (“procedures and regulations”) to identify *Brady*. So, for example, in the debriefing of a detoxing heroin addict, the statement that someone did a shooting would be coded with a flag for caution. Again, the goal would not be to evaluate every statement, but to flag those that warrant some skepticism.³¹⁹ Because there are far fewer analysts in the policing context than there are in the intelligence context, this virtual warning flag is even more imperative. A prosecutor learning of a fact would also be able to have some sense

317. Recognizing the inherent difficulty of analyzing complex, ambiguous, and overwhelming amounts of information, the intelligence community adopted new techniques to avoid mistakes, unearth incorrect baseline assumptions, and avoid cognitive biases. See TRADECRAFT PRIMER, *supra* note 313, at 1–5.

318. For example, Structured Analytical Techniques were created to counter the proven tendency for humans investigating a problem to fall into all too human cognitive traps. RICHARDS J. HEUER JR. & RANDOLPH H. PHERSON, STRUCTURED ANALYTIC TECHNIQUES FOR INTELLIGENCE ANALYSIS 32 (2011); see also ARTNER ET AL., *supra* note 313, at 2 (“In recent years, the IC has greatly increased its use of SATs to promote rigorous analysis, lessen the risk of intelligence failure, and make analysts’ reasoning more transparent to consumers.”). Examples of these Structured Analytic Techniques involve techniques like the “Quality of Information Check” which “evaluates completeness and soundness of available information sources.” TRADECRAFT PRIMER, *supra* note 313, at 10.

319. The focus is on the reliability of sources, and in the intelligence context this understanding of available information sources is critical and is built into the data collection systems. The same issues arise in intelligence-driven prosecution big data systems. An automated quality information check system modeled on the intelligence community version could ensure better accuracy of the information flows going into the system. At a minimum, the system should be designed to allow such queries—recognizing that one should start with the assumption of potentially faulty or incomplete information. A second technique is called the “Key Assumptions Check,” which involves a “review [of] the key working assumptions on which fundamental judgments rest.” TRADECRAFT PRIMER, *supra* note 313, at 7. In the context of developing targets for surveillance, the idea is to question the underlying beliefs leading to suspicion. In the intelligence world, checking these assumptions prevents conclusions that might be faulty, biased, or politically motivated. In the prosecution world, similar assumptions about suspicious groups or individuals, or even the perpetrator of a crime, can be analyzed through this method. If prosecutors are designing a system based on identifying primary offenders for criminal incapacitation, the system doing the identification should have similar checks.

of the credibility or lack of credibility of its source. Technologies now exist that can flag and map the history of information, its lineage, and sourcing.³²⁰

The result of this flagging system will be that when prosecutors review their witness statements, witnesses, or other evidence in the system, any possible red or yellow flags will be reviewed for possible reliability issues. The ultimate decision to turn over the information will remain with the prosecutor, but at least the information will be highlighted for their review.

b. Associational Flags: Links

The magic of social network analysis is that it draws links among data points that would not otherwise be discovered. As has been explained, this technological feat is done by coding the data to track relationships. Everything coded to be linked can be automatically displayed via links. For example, a nickname that shows up in one place could be identified every other place it is found in the larger data set. The result would be that a prosecutor could view all the names in a particular file and see links identifying wherever else these names appear in the larger dataset. Or a prosecutor could view the location of a crime and see links to all the other crimes related by geography. The key is setting up the inputting of data so that information can be automatically found in any particular document within a rapidly expanding dataset. The system could automatically search for and link matched information, so that every name, phone number, or address could be recognized and linked. The goal, again, would not necessarily be to find smoking gun evidence but to identify otherwise unconnected pieces of evidence that might reveal more fruitful relationships or inconsistencies. In this way, an expanded quantitative command of the data is developed. And, once developed, prosecutors can apply a broader theory of *Brady* to the information.

c. Category Flags: Patterns

Structured datasets are built around categories. The search fields and data fields in a database control what can be seen and found. As a result, big data prosecution systems need to design for a broader relational set of categories. Some of this is already being done. The Manhattan CPS system created a checkbox system with crime categories of homicide, shots fired, stabbing, home invasion, robbery, burglary-commercial, and police involved, and other search fields for locations, victims' names, ages, addresses, and geocoordinates.³²¹ This is exactly

320. See Depeau, *supra* note 308.

321. See *supra* notes 77–92 and accompanying text (describing the CPS system).

the type of structured analysis that can allow systems to flag connections. But the categories were designed for prosecutors without thinking about *Brady*. A full set of categories would also include some of the relevant *Brady* issues like motive, bias, capacity, credibility, and inconsistency.³²² A more complete set of categories will lead to a more complete flagging system. A workable system should be designed with automated prompts (dropdown boxes, check boxes, or other simple identifiers). So, while categorizing the information will take some consideration, the inputting should be easy for line officers doing their jobs. The result will be a tool that will reveal different relational connections between people, crimes, and areas.

An analogy to the Intelligence Community again helps demonstrate how a system can be developed even in data heavy professions. All analysts, lawyers, and workers who handle classified information in the Intelligence Community know that each document has a classification system (denoting the sensitivity of the information) that must be marked before being sent.³²³ In government agencies, these classification decisions are made every day, at every level, and are largely managed without incident. Every document has a space to identify whether or not the information is classified and, if so, at which level it is classified, why, and sometimes even the category of information. Like the intelligence analyst, a police officer in an intelligence-driven system could follow the same process by adding a *Brady* classification to the input data. Instead of secrecy, this classification could include considerations of reliability (do you trust the source), links (connections to other cases/incidents), lineage (how it was traced), and particular prosecution-related categories (ways to structure the information by case, place, time, etc.). The inputs could then be searched for by flag. Similar information systems are now in place in the health field with electronic medical records and in the legal field, which has added predictive coding for many document intensive cases.³²⁴

322. See *supra* Part II (describing the possible types of *Brady* material).

323. See 2 ARVIN S. QUIST, U.S. DEP'T OF ENERGY, SECURITY CLASSIFICATION OF INFORMATION § 7 (1993), https://fas.org/sgp/library/quist2/chap_7.html [<https://perma.cc/DH4F-P37U>]; see also 4 OFFICE OF THE DIR. OF NAT'L INTELLIGENCE ET AL., INTELLIGENCE COMMUNITY CLASSIFICATION AND CONTROL MARKINGS IMPLEMENTATION MANUAL 10–12 (2d ed., 2011) https://fas.org/sgp/othersgov/intel/capco_imp.pdf [<https://perma.cc/A4KF-Q3CA>].

324. See, e.g., Shannon Brown, *Peeking Inside the Black Box: A Preliminary Survey of Technology Assisted Review (TAR) and Predictive Coding Algorithms for eDiscovery*, 21 SUFFOLK J. TRIAL & APP. ADVOC. 221, 244–45 (2016); Charles Yablon & Nick Landsman-Roos, *Predictive Coding: Emerging Questions and Concerns*, 64 S.C. L. REV. 633, 634 (2013); see also Nicholas Barry, *Man Versus Machine Review: The Showdown Between Hordes of Discovery Lawyers and a Computer-Utilizing Predictive-Coding Technology*, 15 VAND. J. ENT. & TECH. L. 343, 344 (2013).

2. Intelligence-Driven Checks: Filling *Brady*'s Gaps

This change in *Brady* categorization and identification not only responds to technological gaps in the big data prosecution systems but remedies longstanding gaps in traditional practice. As previously discussed, *Brady* failures usually arise from three types of error. First, due to the volume of information and the requirement to be aware of evidence not directly under prosecutors' control, trial lawyers may well miss material *Brady* evidence in the files. Second, prosecutors may make mistakes about the relevance or materiality of a particular fact. Either because they do not know the defense theory of the case or because other evidence overwhelms a particular inconsistency, prosecutors may minimize the importance of certain information and in turn inadvertently conceal it.³²⁵ Third, on rare occasions, prosecutors even make malicious decisions to conceal exculpatory evidence. A networked system of *Brady* can help identify missed or mistaken conceptions of *Brady* (leaving the problem of malicious concealment and malicious actors to other mechanisms of accountability).

The technological suggestions identified here can assist prosecutors in sorting through the volume of data. A flag system of possible impeaching evidence, credibility problems, or reliability issues provides a response to prosecutors who might otherwise miss the significance of a particular fact. If designed correctly, prosecutors will see more potential *Brady* information in their growing data systems. In fact, these changes might reduce *Brady* challenges and litigation. But more importantly, prosecutors will know they work in a system designed to check for their missed connections. By design, the system will search for the signals in the noise, recognizing that there will always be impeaching signals in the complex reality of crime patterns. This does not mean that *Brady* material will be discovered in every case, but only that the prosecutor will possess more information about possible missed connections, concerns with evidence and witnesses, and case weaknesses.

325. In both policing and intelligence gathering there exists the real concern that perceptual biases will impact objective analysis. Again, the development of structured analytics techniques arose from stated concerns that intelligence analysts would "perceive what they expect to perceive," resist change, assimilate new information into preconceived ideas, and dismiss or ignore conflicting information. See TRADECRAFT PRIMER, *supra* note 313, at 2. These perceptual biases would prevent investigators from seeing inconsistent or incongruent information that diverged from their initial hypothesis. In essence, cognitive biases blinded analysts to information that ran counter to their theory of the problem. Obviously, these same cognitive traps can befall proactive prosecutors seeking to prosecute a primary target with a proactive, intelligence driven prosecution mindset.

Flagging potential *Brady* information also potentially eases resolution of longstanding arguments over materiality.³²⁶ A technological flagging system changes the *Brady* decisionmaking process—both pretrial and on appeal. In the pretrial context, a prosecutor using a digital flagging system will be faced with a clear record of possible impeaching or exculpatory flags. A decision to ignore those flags may be the same, but the availability of a digital record offers two possibilities that did not exist before such a flagging system. First, a relatively straightforward double-check would be available for supervisors (or colleagues) to review the casefile. A simple internal review process might even help protect prosecutors making the ultimate judgment about materiality. Second, on occasion, the information could be turned over to a judge for an *in camera* review. The former would be a relatively basic internal policy change for departments concerned about *Brady*, and the latter could be saved for particularly difficult judgment calls on the need to turn over information. But, just as importantly, the digital record could be preserved for appeal. If the record of information about flags that was identified (and ignored) turned out to be a material issue, the fact that the prosecutor had the information available would be clear in the digital record.

3. A *Brady* Button

Finally, a more advanced technical system might provide an automated “*Brady* Button” whereby certain searches could be automated across the platform. The goal would be to discover possible flags for concern consistent with a prosecutor’s standard *Brady* obligation. If one can tag every witness, participant, officer, location, weapon, etc., the building blocks of a searchable system will be created.

The purpose of engineering a big data system to identify *Brady* information is not an argument for automation. *Brady* is a contextual judgment and prosecutors will still have to make that final human judgment. But automating a system of flags, searches, and networks can help the human prosecutor see the larger patterns and connections at play. This networked understanding

326. A longstanding frustration with *Brady* is that prosecutors and defense lawyers disagree on how to weigh the significance of impeaching evidence, with prosecutors occasionally making mistakes about the material significance of a piece of evidence. An inconsistent identification or potential motive evidence in the larger context of a criminal case may seem unimportant to a prosecutor convinced of the strength of other evidence pointing toward guilt. But to the defense, that particular piece of evidence may be the key to their theory. A prosecutor weighs the evidence one way and the defense another, and usually in contested cases neither side litigates it until after a conviction on appeal.

can help the prosecutor double-check the assumptions underlying the strength of the evidence.

Again, an analogy to the Intelligence Community is useful. Due to the inherent uncertainty in the information gathering processes, on occasion, the Intelligence Community sets up so-called red teams to double check or rethink their assumptions. A “red team analysis”³²⁷ “[m]odels the behavior of an individual or group by trying to replicate how an adversary would think about an issue.”³²⁸ In the context of intelligence, this red team might involve a rival nation. In the context of criminal trial, it might involve thinking like a defense lawyer. The goal is to look at a problem anew, without the natural bias that comes from having done the original investigation on the matter.

In the big data prosecution world, the goal would not be to create a human red team, as such a project would be too time-consuming and largely unnecessary. Instead, the goal would be to use the technology to do an automated red team assessment. Like a technologically created red team that is designed to check accuracy in the intelligence world, the system would offer cautions for a prosecutor to evaluate and integrate into their *Brady* obligations.³²⁹ The goal of automating *Brady* is to see the interrelations over time, place, and group and to force the prosecuting authority to evaluate and consider possible warning flags.

CONCLUSION

Building a prosecution system that creates warning flags, allows links to be visualized, and creates categories of evidence will engender more effective searches for *Brady* information and will change what is thought of as *Brady* material. Prosecutors following an intelligence driven prosecution model should recognize that their duty to discover *Brady* information now includes analyzing the relationships among witnesses, crimes, suspects, places, groups, gangs, families, and any past relationship with the government and law enforcement.

327. TRADECRAFT PRIMER, *supra* note 313, at 31.

328. *Id.* (“Once established and separated from traditional analysis, the [red] team members should: Put themselves in the adversary’s circumstances and react to foreign stimuli as the target would[, and] [d]evelop a set of ‘first-person’ questions that the adversary would ask, such as: ‘How would I perceive incoming information; what would be my personal concerns; or to whom would I look for an opinion?’”).

329. See Erik Luna & Joshua A.T. Fairfield, *The Open Society and Its Digital Enemies: A Reply to Professors Bambauer and Garrett*, 99 CORNELL L. REV. ONLINE 217, 228 (2014) (“The current use of Big Data in law enforcement lacks debugging or ‘red-teaming,’ as it is called in software parlance. ‘Red teams’ are groups tasked with testing software for fatal flaws.” (footnote omitted)).

This obligation must include more than simply looking at the facts about each of the players in a case (the traditional process). It should also include an examination of how those players relate to each other and relate to the criminal justice system over time. In a traditional system, an eyewitness might just be an eyewitness. In a big data system, that eyewitness might be better thought of as the accumulated connections, statements, and relationships that can be found in the larger prosecution dataset. In a traditional system, an address might just be the location of a shooting. In a big data system, that address has a complex history which must be understood for possible motives, connections, and rivalries.

Of course, the dangers of designing a system to identify *Brady* information are significant. If designed too restrictively, *Brady* information could be not only hidden but essentially passed over as not-*Brady* information based on the design or choices of those inputting the data. Thus, it is imperative that substantial training, reminders, and systems are implemented to audit the accuracy of the processes developed. On the other hand, if the flagging system is designed too expansively, the system could generate so much impeaching noise that legitimately related or truthful information could be lost. Errors in inputs, analysis, or wholesale confusion are real concerns in implementing a technological fix to *Brady*.

Currently, however, because *Brady* information has not been a substantial consideration in existing intelligence-driven prosecution systems, the choice to ignore it also seems unwise. Building a digital investigation system that collects but cannot identify material evidence jeopardizes the legitimacy of individual criminal prosecutions and of the criminal justice system more broadly.

While expanding the duty mandated by *Brady* would undoubtedly create more work for prosecutors, this additional effort is, in truth, just the negative image of the investigative process that is already being used in intelligence-driven cases. The goal is for prosecutors to see crime and criminal actors in a relational context with both inculpatory and exculpatory evidence to be uncovered. A more expansive approach to *Brady* is possible through redesigning the technological architecture of these intelligence driven big data prosecution systems.