SESSION 2: CRIMINAL DEFENSE ACCESS TO LAW ENFORCEMENT ADS

Primary Presenters

Somil Trivedi, Senior Staff Attorney, ACLU Criminal Law Reform Project

Kevin Vogeltanz, Founder and Managing Member, Law Office of Kevin S. Vogeltanz

Andrew Ferguson, Professor of Law, UDC Law School

Cynthia Conti-Cook, Staff Attorney, Legal Aid Society

MODERATOR:
Vincent M. Southerland, Executive Director, Center on Race, Inequality, and the Law at NYU School of Law; Area Lead, AI Now Institute

Access Key Litigation Documents Here

Session Summary

This session explored the intersection between prosecutor's obligations pursuant to the Supreme Court's decision in *Brady v. Maryland* and the use of algorithmic tools by law enforcement, including prosecutors and police officers. *Brady* imposes an affirmative constitutional duty on prosecutors to disclose to the defense exculpatory evidence material to the guilt, innocence, or punishment of the accused.[2]

Practically speaking, that means prosecutors must disclose any evidence to the defense that could cast doubt on the guilt of the accused or the punishment to be imposed. The advent of ADS in the criminal legal system has led to the production of new forms of evidence, much of which could qualify as *Brady* evidence. Against that backdrop, presenters described two cases that centered on *Brady* evidence produced by the use of algorithmic tools, explored broader concerns raised by the advent of data-driven prosecution and *Brady*, and presented a searchable police misconduct database that public defenders developed to counter efforts to relieve prosecutors of their *Brady* obligations.

Louisiana v. Hickerson

Kevin Vogeltanz presented the first case. It involved Kentrell Hickerson, who, following a trial, was convicted of what amounted to criminal conspiracy and other related charges. He was sentenced to 100 years in prison following his conviction.

The central question in Mr. Hickerson's case was whether he was a member of a gang that had been responsible for several crimes. At the time of Mr. Hickerson's prosecution, law enforcement in the city of New Orleans used a risk-assessment database called Gotham, created by the

---

2   373 U.S. 83 (1963)

company Palantir. The ostensible purpose of the program was to determine who among the city's population was likely to become a perpetrator or victim of gun violence. That information was to be used in a violence-intervention program, "NOLA For Life," in which identified individuals were warned by law enforcement of the potential consequences of their lifestyle, and were offered social services and other supports.[3]

The database created social-networking graphs based on aggregated information about the city's population, including individuals' ties and connections to other individuals. Given the centrality of the question about Mr. Hickerson's relationships to other suspected gang members, the social-networking graphs the Gotham program produced could have proven dispositive on that key point.

Despite the relevance of Gotham to Mr. Hickerson's case, he and his lawyers only learned of its existence and use after the media reported that Palantir had been operating in the city for 6 years with little public knowledge.[4] In a motion for a new trial, Mr. Hickerson advanced the claim that he was entitled to the Gotham-produced materials pursuant to *Brady*, as they might have raised reasonable doubts with the jury. Mr. Hickerson's new trial motion was denied by the district court judge based on the prosecution's claim—contested by Mr. Hickerson—that Gotham played no role in Mr. Hickerson's case.

Lynch v. Florida

Somil Trivedi presented the *Lynch* case, which centered on the arrest, prosecution, and conviction of Willie Allen Lynch, who was accused of selling 50 dollars' worth of crack cocaine to undercover officers. One key aspect of the case was that the undercover officers could not identify the individual who sold drugs to them except by his nickname, "Midnight." One of the officers surreptitiously took a cell phone picture of the individual, which they forwarded to a crime analyst, along with the suspect's nickname and the location of the drug sale. The officers left the scene without making an arrest.

The crime analyst was unable to use the nickname or location to identify anyone through law enforcement databases. She then turned to the cell phone photo and uploaded it into a facial-recognition program called the Face Analysis Comparison Examination System (FACES), which draws from a database of more than 33 million driver's license and law enforcement photos.[5] That search produced four possible suspects, along with Mr. Lynch. The quality of these matches was gauged by a star rating of unknown reliability. FACES assigned only one star to Mr. Lynch, and no stars to the other suspects. The analyst then selected Mr. Lynch from among the suspects

---

3   Emily Lane, *Mayor, Police Chief to Face Subpoenas from Convicted Gang Member Over Palantir Claim*, NOLA.com, Apr. 3, 2018, https://www.nola.com/news/crime_police/article_fa5949c4-a300-509d-90e8-2d7814f505f6.html. This program has many similarities to the Chicago Strategic Subjects List, which has been subject to extensive criticism.

4   Ali Winston, *Palantir Has Secretly Been Using New Orleans to Test its Predictive Policing Technology*, The Verge, Feb. 27, 2018, https://www.theverge.com/2018/2/27/17054740/palantir-predictive-policing-tool-new-orleans-nopd

5   Aaron Mak, *Facing Facts*, Slate, Jan 25, 2019, https://slate.com/technology/2019/01/facial-recognition-arrest-transparency-willie-allen-lynch.html

returned by the software, and sent his identification information back to the officers, who promptly arrested him. At trial, Mr. Lynch's sole defense was misidentification—claiming that he was not the person who sold drugs to undercover officers. He was convicted and sentenced to 8 years in prison.

On appeal, Mr. Lynch argued, pursuant to *Brady*, that prior to his trial he should have been given the photographs of the other individuals who matched as potential suspects through the FACES program. He learned of the use of FACES only during a pretrial deposition of the crime analyst who made the alleged match.

The Florida First District Court of Appeals affirmed Mr. Lynch's conviction, denying his appeal. The Court ruled that because Mr. Lynch could not demonstrate that his trial outcome would have been different if the other FACES results had been disclosed to the defense, he could not prevail. The Court pointed out that Mr. Lynch could not show that the other photos returned by the software resembled him and would have supported his misidentification defense.[6] The ACLU, the Electronic Frontier Foundation, the Georgetown Center on Privacy and Technology, and the Innocence Project filed an amicus curiae brief urging the Florida Supreme Court to hear Mr. Lynch's appeal. In July 2019, the Florida Supreme Court denied discretionary review of the case.

Intelligence-Driven Prosecution

Professor Andrew Ferguson presented on the emergence of intelligence-driven prosecution, which has been defined by prosecutors as focusing the collective resources of a prosecutor's office on reducing crime—violent crime in particular—through data collection and analysis, information sharing, and close coordination with law enforcement and community partners.

In practice, this means amassing data from a range of sources, with varying degrees of reliability, on individuals identified as so-called "drivers" of crime. Prosecutors use this information to determine how individuals should be treated pretrial and at sentencing, and to demonstrate relationships and connections between individuals.

Three conclusions flow from the use of intelligence-driven prosecution: first, to the extent that prosecutors' offices have created these systems, they contain significant *Brady* material, touching on everything from the credibility of witnesses and potential biases of law enforcement, to how law enforcement identifies and treats suspects and targets of their investigations. Second, the wealth of information produced by intelligence-driven prosecution means that prosecutors may unwittingly have *Brady* evidence in their possession. Third, in light of the possibility that prosecutors are unknowingly in possession of *Brady* evidence, the shift to intelligence-driven prosecution requires that *Brady* be considered more expansively and with those technological advances in mind.

---

6   *Lynch v. State*, No. 1D16-3290 (Fla. Dist. Ct. App. Dec. 27, 2018)

CAPstat: Using Technology to Uncover *Brady* Evidence

Cynthia Conti-Cook then presented on the Cop Accountability Project (CAPstat) of the Legal Aid Society of New York's Special Litigation Unit. The Project is a publicly accessible database that compiles complaints regarding officer misconduct from sources such as administrative proceedings, lawsuits, and media sources.[7] Members of the public can search the database by officer and precinct to obtain information regarding patterns of misconduct by officers; relationships among officers who may have engaged in conduct together; the use of force by police officers; and punishments imposed on officers for misconduct. In the courts, state laws generally shield an officer's history of misconduct from the accused, defense counsel, and the general public, thus leaving a broad source of potential *Brady* material inaccessible. The CAPstat database fills that gap.

Overarching Lessons Learned

This session focused on the intersection of *Brady* and algorithmic tools, highlighting critical points that warrant serious attention from criminal justice advocates and those engaged in the design, implementation, and oversight of algorithmic tools.

Of utmost importance is how the interplay between *Brady* and algorithmic tools reveals the power dynamics and differences between law enforcement and people accused of crimes. Technological tools increase the already significant power imbalance between the State and the accused. Fundamentally, *Brady* and discovery, more generally, is meant to help equalize that imbalance. When operating as designed, *Brady* shifts some power from law enforcement to the accused by forcing the State to show its hand, and by arming the accused with evidence that may help defeat the criminal allegations they face. However, *Brady* can only do so when criminal justice actors understand how these tools operate, comprehend the nature of the data they produce, and then diligently fulfill their resultant *Brady* obligations. The case studies we explore in this session made clear the difficulty of meeting those conditions, especially when the existence and inner workings of those systems are kept secret.

Knowledge Is Power

This session exposed significant knowledge gaps among criminal justice stakeholders about the ubiquitous nature of technological tools law enforcement agencies uses to advance their investigative work, as well as the breadth of the data those tools produce that can be material to a person's guilt, innocence, or punishment.

This is particularly problematic for those tasked with defending the accused. Many defense attorneys do not know which algorithmic tools law enforcement is using or how they are being deployed. They often only learn of their existence through media reports, pretrial motion practice, discovery requests, or other procedural channels. Neither the defense, nor even law enforcement officials themselves, seem fully aware of the data these algorithmic tools produce, and what that means for their *Brady* obligations. This knowledge gap—whether born of willful ignorance on the part of the prosecution, or because law enforcement actively obscures investigative techniques—has significant implications.

---

7   CAPstat, https://www.capstat.nyc/ (last visited Aug. 6, 2019)

The prosecution has an affirmative, constitutional duty to disclose *Brady* evidence. If they are unaware that such material exists, it is exceedingly difficult to ensure that they can fulfill that duty on their own. In other instances, the prosecution may know such evidence exists, yet not view it as *Brady* material. Several common justifications for nondisclosure were raised during the session. Among them are that defense counsel has access to the underlying reports and sources used by ADS to produce their analysis; that the presence of trade secrecy protections limits disclosure; and that the taint of a *Brady* violation can be cleansed at some other point in the process, such that the evidence would not have changed the outcome of a case.

Technical Concerns with Algorithmic Tools

Ensuring compliance with *Brady* is difficult when considered in light of another concern: problems with the technology itself due to biased data, technical flaws, inconsistent oversight, and other features that render the tools unreliable.

Presenters noted the data that law enforcement collects and amasses as inputs for these algorithmic tools is often not trustworthy. It is affected not only by biases and prejudices from both individuals and institutional structures but also is susceptible to the type of errors commonly found in data collected from nontraditional and nonstandardized sources, including examples such as nicknames, crime locations, and social media connections.[8] The potential for those data points to serve as the impetus for an investigative effort highlights their centrality to the *Brady* analysis.

Responses to *Brady* Resistance

Criminal defense lawyers and advocates have worked to meet the challenges of *Brady* enforcement but given how high the hurdles can be, they have started to build their own *Brady*-oriented tools and records in an attempt to essentially fulfill the State's *Brady* obligation for it.

CAPstat is one example: a publicly-accessible database that collects complaints and lawsuits related to police misconduct. CAPstat was modeled on, and inspired by, the Invisible Institute's Citizens Police Data Project—a database that tracks public-police encounters to hold law enforcement accountable. The discussion of CAPstat underscored the difficulties of maintaining such a database. It is both time- and resource-intensive, requiring constant monitoring to ensure accuracy and effectiveness. Yet such databases are critical to filling the void left by prosecutors' continued noncompliance with *Brady*.

This part of the session provided some insight into how communities and criminal justice advocates might work together to hold law enforcement more accountable. One presenter noted that by developing tools used to surveil communities, law enforcement has inadvertently created an infrastructure to surveil itself. The gaze of technological and algorithmic tools can shift from traditional targets of investigation to institutional stakeholders. That shifts the balance of power in ways that are consistent with the spirit of *Brady* and discovery more generally.

---

8   *See* Rashida Richardson, Jason M. Schultz & Kate Crawford, *Dirty Data, Bad Predictions: How Civil Rights Violations Impact Police Data, Predictive Policing Systems, and Justice*, 94 N.Y.U. L. Rev. Online 192 (2019)

Session 2 Recommendations

- **Enact open-file discovery policies for criminal cases involving ADS.**

  In a world where algorithmic tools are ubiquitous, opening prosecutorial files to defense counsel and the accused eliminates reliance on the prosecutor's good-faith judgment about what may constitute *Brady* evidence.

- **Update criminal discovery rules to treat ADS as accessible, contestable, and admissible evidence.**

  Courtroom discovery rules should be rewritten to account for the use of algorithmic tools in the criminal legal system, ensuring that defense counsel and the accused have access to ADS information, similar to the way they have access to information about analog police tools.

- **Expand prosecutorial understanding of the Supreme Court's *Brady* Rule to include ADS evidence.**

  A technology and data-driven approach to prosecution demands that *Brady* be reconceptualized and understood for its broad applicability. The tools that support intelligence-driven prosecution generate critically important data: investigative methods and sources of investigatory leads; potential suspects; alternate theories of the prosecution case; impeachment material about particular witnesses; maps of connections between potential suspects and those who may be accused of crimes; past (failed) investigations of the accused and their associates; the means of arriving at the identification of a suspect; and law enforcement field reports. All represent the kinds of material that defense counsel and the accused should have access to, and which the prosecution should fully disclose as part of its *Brady* obligation. Each may be exculpatory evidence material to the guilt, innocence, or punishment of the accused, and therefore falls squarely within *Brady*. This includes prosecutors providing the defense with a list of the algorithmic tools law enforcement has used to conduct investigation of suspects in a case; the purpose for which each tool was designed; the data on which those tools rely; and other technical specifications, all of which should be documented.

- **Develop ADS trainings and toolkits for the criminal defense community.**

  The criminal defense community must be allowed to have meaningful access to any ADS used in the criminal justice system, including training on how to understand its' operation and outputs. This also necessitates developing a defense counsel discovery toolkit to identify requests that catalog all potential discovery material in cases where the prosecution process has involved data-driven law enforcement practices.