EXECUTIVE SUMMARY

We find ourselves at a watershed moment for policing in the United States. Sparked by the continued tragic killings of unarmed Black men, women, and children by police officers – and particularly the galvanizing protests, demands, and efforts that have carried forward from the killings of George Floyd and Breonna Taylor – calls to reform, transform, defund, dismantle, and abolish law enforcement have taken center stage in cities, towns, and legislative halls throughout the United States. The families of victims who have been killed by police officers, along with other impacted residents, activists, civil rights organizations, elected officials, government agencies, and policing professionals, among many others, are pressing the need for radical change. Journalists and news organizations are reporting on and amplifying the voices for transformation.

These actions and efforts have crystalized in response to policing practices that have harmed and hyper-criminalized individuals and communities of color. Over the last several years, U.S. Department of Justice investigations have revealed what residents of Black and Brown communities have long known and expressed: that abusive and unconstitutional policing pervade their lives. The National Association of Criminal Defense Lawyers (NACDL) convened a Task Force on Predictive Policing[1] in 2017 to examine the rise, implementation, and ramifications of data-driven policing technologies, and to offer comprehensive recommendations that support transparency, safety, and due process.

From 2017 to 2019, the Task Force held meetings in Washington, D.C., Chicago, Los Angeles, San Francisco, and New York City. At these meetings, the Task Force met with a diverse array of witnesses, including technologists and industry experts, law enforcement personnel, academics, attorneys, advocates, and community stakeholders. The purpose of these meetings was to learn about the different types of technologies that police departments currently use or have used in communities throughout the country, and the impact of these technologies on individuals, families, communities, and the criminal legal system.

In recent years, police departments have been turning to and relying on rapidly developing data-driven policing technologies to surveil communities, track individuals and, purportedly, predict crime. These technologies include algorithmic decision-making that departments claim can predict where crime is likely to occur, who will likely commit crime, and who will likely be a victim. These algorithms are thus designed to interrogate massive troves of data gathered in a myriad of ways, using inputs that can range from police-generated crime reports to publicly available social media posts. The outputs are then used to make critical decisions about patrols, or to make life-altering designations of individuals.

The Task Force chose to use the term "data-driven policing" to refer to the various technologies and practices that were studied in order to avoid the shifting sands of terminology. In doing so, the Task Force understands that other technologies that do not utilize automated decision-making systems can fall under this broad terminology, but for the purpose of this report, data-driven policing is used to refer to the tools that analyze data to determine where, how, and who to police. During the time that the Task Force studied the issue, Palantir, a company that contracts with law enforcement agencies in major cities across the country, never described its tools as "predictive policing." The company instead advertises as a "data integration and analysis software platform."[2] As

the term predictive policing fell out of favor, NYPD rolled out "precision policing," which "combined predictive policing analysis and community policing."[3]

This Report identifies the racial overtones present in the historical development of data-driven policing systems and the data they utilize, and looks to case studies of specific predictive policing systems to illuminate how this technology invades personal privacy and operates as a confirmation-bias tool to justify over-policing low-income communities of color. The purpose of this Report is to: (1) call attention to the rapid development and deployment of data-driven policing; (2) situate data-driven policing within the racialized historical context of policing and the criminal legal system; (3) make actionable recommendations that respond to the reality, enormity, and impact of data-driven policing; and (4) suggest strategies for defense lawyers in places where data-driven policing technology is employed.

Brief History of Policing and the Economics of Punishment

Modern policing traces its origins to "slave patrols," a tool of racist oppression. Policing has been stitched into the fabric of the country since its founding over 400 years ago. As both a practice and a profession, policing has evolved over the centuries. Even after the Civil War and the Thirteenth Amendment, a loophole in the Amendment's text legalizing enslavement as a "punishment for crime" turned antebellum slave patrols into a policing and criminal legal system designed to criminalize, incarcerate, and otherwise punish Black people in ways that strongly resembled and replicated slavery. Black Codes and vagrancy statutes were used to hyper-criminalize, imprison, and exploit Black people for financial gain.[4]

When the criminal legal system began shifting to models rooted in incapacitation and deterrence during the 1970s, individuals and communities without social and political capital increasingly lost access to law enforcement services. Police departments were overwhelming white, were largely unresponsive, and often showed outright hostility to the needs of Black residents. In the decades that followed, policing strategies focused on zero tolerance, broken-windows, and an escalation of the War on Drugs, and systematically targeted Black communities for surveillance and incarceration. Following the 9/11 terror attacks, police departments militarized in the name of national security and terrorism prevention, but the result was heightened surveillance of the public, particularly communities of color.

One can draw a direct line from this history to the hyper-criminalization of Black men, women, and children today, along with the economic incentives embedded in the modern criminal legal system. Police officers continue to serve as arbiters of who is introduced to the system and who is not. Law enforcement strategies and tactics that criminalize and capture poor Black, Indigenous and People of Color ("BIPOC") men, women, and children, continue. A historical analysis of policing thus demonstrates two aspects of policing that are constant over time: first, policing is rooted in the control and criminalization of Black people; and second, lawmakers, prosecutors, and courts have historically given deference to law enforcement concerning their practices.

Brief History of Surveillance and the Rise of Big Data

An estimated 2.5 quintillion bytes of data are now generated every day.[5] With the ability to digitize, track, and store nearly every aspect of information, from Internet searches and social media posts to cell phone calls and retail purchases,[6] individuals are constantly contributing "to a growing trove of data as they go about their daily lives,"[7] and such data plays an ever-expanding role in the surveillance of individuals and communities, and in determining who, where, and when police officers monitor, encounter, search, and arrest.

Contemporary data-driven programs in policing emerged from repeated attempts by criminologists, legal scholars, and law enforcement agencies to quantify and measure the complex social processes behind crime and disorder. Though these programs may vary in the types of data and techniques they employ, all of them are inevitably shaped by prior policing patterns, historical crime reports, and other records compiled by the police themselves. As such, data-driven policing obscures the discretion, biases and human decision-making inherent in the production of such data.[8]

The technological tools used to organize and interrogate police data are the natural extension of tactics that have been employed over centuries of policing. Data collected and organized by law enforcement agencies have long-informed police actions, and reflect the implicit bias and explicit racism of policing as an institution. Using algorithmic tools to interrogate massive troves of police data does not correct for biased or racist policing practices; rather, it entrenches them. As such, the technological tools that are guiding modern day policing practices must be analyzed within the historical context that birthed them.

Modern-day policing is fueled by an almost unfettered access to immeasurable amounts of personal data, ensuring that officers have seamless access to criminal intelligence at the local, state, and federal level. As such, law enforcement databases are frequently exempt from complying with the same constitutional and legal standards that govern criminal investigations. Even with information that would normally require a warrant, law enforcement agencies can purchase the data from commercial data brokers without the need for a subpoena or warrant. With such an unfathomably massive amount of data being constantly generated, police departments are perpetually at risk of employing predictive algorithms trained on erroneous or irrelevant data, or even data manipulated by the police themselves. Research and scholarship have repeatedly found that these databases are often riddled with errors, and that "biases in the databases themselves, based on how data are collected, may also lead to disparate outcomes."[9] Indeed, all data-driven policing systems run the risk of being built on an incomplete and biased understanding of where crimes take place and who is actually committing them, with real costs to communities already under pervasive police scrutiny and surveillance.

The Landscape of Data-Driven Policing

Today, data-driven policing encompasses the many surveillance technologies, tools, and methods employed by police officers to visualize crime, target "at-risk" individuals and groups, map physical locations, track digital communications, and even collect data on individuals and communities. This can include any approach that incorporates a clear reliance on information technology, criminology theory, and predictive methods in policing.[10] At its core, predictive algorithms in policing programs are the "data-driven incarnation"[11] of what criminologists have been attempting to achieve for decades: to analyze past events, infer broader patterns, and to then use those insights to "prevent" future crime.

According to a report published by the RAND Corporation, predictive methods in policing can generally be divided into four broad categories: (1) methods for predicting crimes, or approaches used to forecast places and times with an increased risk of crime; (2) methods for predicting offenders, or approaches that identify individuals at risk of offending in the future; (3) methods for predicting perpetrators' identities by creating profiles that accurately match likely offenders with specific past crimes; and (4) methods for predicting victims of crimes by identifying groups, or in some cases, individuals who are most likely to become victims of crime.[12]

In order to implement these methods, predictive policing employs a variety of machine learning algorithms. Since the developers of data-driven policing technologies often assert trade secret evidentiary privileges to deny public access to the inner workings of their algorithms, the types of machine learning used in such programs are relatively unknown, and because many of these tools built on these algorithms are relatively new, or are continuing to change alongside advancements in technology, all are "are relatively untested, with only a handful of studies, reports, or empirical validation across jurisdictions."[13] Once predictions are made, "there is, generally, no standard for how police should use the predictions,"[14] meaning the technology gives an objective façade to more traditional policing tactics.

Place-based data-driven policing programs are built upon the premise that crime is not evenly dispersed geographically, and that certain places are expected to experience higher rates of crime over a certain period of time. Like "hot spot policing," or the identification of geographically-bound spaces associated with a proportionally greater number of criminal incidents or heightened victimization risk, place-based crime forecasting visualizes the spatial and temporal distribution of crime to purportedly "predict" areas with future criminal activity. NACDL found that the use of predictive algorithms in place-based crime forecasting produced harmful, self-perpetuating feedback loops of crime predictions, in which officers would repeatedly patrol neighborhoods

that had been disproportionately targeted by law enforcement in the past, and were thus overrepresented in the historical crime data used to train and build predictive crime algorithms.

Police departments also rely on person-based data-driven policing programs to predict who is most likely to commit crimes, in addition to who is likely to become the victim of a crime. The algorithms behind these programs are designed to interrogate massive troves of data gathered in a myriad of ways, with inputs ranging from police-generated crime reports to publicly available social media posts. The outputs are then used to make critical decisions about patrols, or life-altering designations about which individuals need to be suspected, surveilled, and encountered by law enforcement. These programs are enabled by law-enforcement databases and have been shown to lead to the increased enforcement and arrests of predominantly Black and Brown young men.

Among these databases are gang databases, which are localized within cities or similar jurisdictions, and encompass a broad swath of identifying data on individuals known, suspected, believed, or assumed to be gang members, associated with gang members, or affiliated with gang members. BIPOC communities comprise the vast majority of individuals listed on these databases, with Black men being the most overrepresented group. Individuals can be certified as gang members simply based on their appearance or location, or even their likes, comments and connections on social media, often without being notified of their inclusion in such a database or given the opportunity to challenge that designation. In addition to being over-inclusive, hyper-racialized, and non-transparent, NACDL found that these databases are riddled with errors, and have even included young children and infants.

Though data-driven policing programs may be designed to lower citywide violence levels and marketed as intervention opportunities for the benefit of communities, empirical research studies have repeatedly found that such tools fundamentally remain a law enforcement deterrence tool. Some programs have resulted in heightened risk of arrest, in addition to enhanced federal and state sentencing options, for designated individuals sweapt into their broad net. For example, individuals included in gang databases are subject to increased police surveillance and monitoring, and can also face enhanced criminal charges upon arrest.

Person-based data-driven policing programs have historically been shrouded in secrecy, with police departments frequently using social media monitoring tools and techniques to surveil individuals, groups, and communities without their knowledge. Data obtained through social media posts and text messages are increasingly being used to not only populate gang databases, but as primary evidence in criminal investigations, with no effective means of oversight to limit the extent of surveillance.

Critical Analysis of Data-Driven Policing

Methodological Problems

Though prediction has always been a fundamental part of policing,[15] the emergence of predictive algorithms in policing was considered particularly novel for its alleged ability to apply artificial intelligence to quantities of data once considered too large and too complex for police departments to analyze.[16] Its proponents have since claimed that predictive policing programs can lower crime, revolutionize public safety, and help under-resourced departments "do more with less,"[17] while critics have argued that such programs produce self-perpetuating feedback loops of crime prediction, placing historically over-policed individuals and communities at further risk of harm. The Task Force found the latter, that these programs entrench existing biases and exacerbate the disproportionate impact of policing on BIPOC, low income and other marginalized communities.

If crime data is to be understood as a "by-product of police activity,"[18] then any predictive algorithms trained on this data would be predicting future policing, not future crime.[19] Neighborhoods that have been disproportionately targeted by law enforcement in the past will be overrepresented in a crime dataset, and officers will become increasingly likely to patrol these same areas in order to "observe new criminal acts that confirm their prior beliefs regarding the distributions of criminal activity." [20] As the algorithm becomes increasingly confident that these locations are most likely to experience further criminal activity,[21] the volume of arrests in these areas

will continue to rise, fueling a never-ending cycle of distorted enforcement.[22] The biases held by police officers and those reporting crimes, and correlations between attributes like race and arrest rates, will not only be recognized and replicated by the algorithm, but directly integrated into the software "in a way that is subtle, unintentional, and difficult to correct, because it is often not the result of an active choice by the programmer."[23]

With an increasing number of police departments already succumbing to the "pressures of managerial techniques that emphasize quantitative measures of effective policing,"[24] some experts have suggested that data-driven policing strategies and tools have facilitated the return of broken windows policing. Since people also have a tendency to believe a computer-generated report over that of a human-created report, predictive policing programs and other automated decision-making systems often run the risk of "being trusted above human judgment while simultaneously concealing potential unchecked errors."[25] Biases in machine learning algorithms pose a "particularly insidious risk to disadvantaged groups by creating a pseudo-scientific justification for discriminatory treatment,"[26] and while transparency can help prevent deliberate or semi-deliberate discrimination, it cannot singlehandedly "correct the effects of the unintentional, institutional discrimination embedded in the data itself."[27]

Transparency, Trade Secrets, and Non-Disclosure Agreements

Intensified public scrutiny of these predictive algorithms has raised questions about how they are developed, implemented, and marketed; why they are not subject to more review; and whether there are mechanisms in place to properly assess their risks, vulnerabilities, and potential for greater societal harm. Moreover, the private companies that build, market, and sell data-driven policing technologies not only claim propriety rights over their methodologies, but assert such claims in response to subpoenas;[28] effectively denying defense attorneys and those accused in criminal cases information central to the defense.[29]

The lack of transparency with data-driven policing and its fundamental business model are deeply interwoven. With private companies competing to build, market, and sell technology, police departments "are customers or clients of private companies"[30] — with some companies even providing technology to police departments initially for free, with the goal of selling departments on the need to continue using the technology. As a result, many departments often possess little to no insight into the inner workings of the systems they employ and lack incentive to do so without explicit transparency measures in place. This lack of transparency jeopardizes fundamental constitutional rights, public trust, and privacy, and cedes too much control to companies in the private sector. This lack of transparency also extends to the adoption and use of the technology, and the ways in which it undermines democratic governance. Most police departments do not inform impacted communities, let alone legislators, that they are utilizing data-driven policing technologies, and rarely provide justification or disclose the policies that govern a technology's use.

While policing as a practice remains largely unchanged, the decisions that guide law enforcement today are being outsourced to private entities with no perceived obligation to publicly disclose details of how their tools actually work. It is consistent with historical trends that police departments are unchecked in their use of expanding and invasive technology to surveil the public, and that law enforcement deploys this technology in ways that continue to hyper-criminalize Black and Latinx individuals. By "tech-washing" racially biased policing practices and hiding behind data-driven tools that collect, use, and produce skewed data, law enforcement agencies are able to justify increased policing and surveillance in historically over-policed communities under the veneer of technological neutrality and objectivity. In this way, data-driven policing perpetuates a self-reinforcing cycle of bias and inequity.

Impact on Youth

Children possess special protections in the juvenile court system, such as different sentencing guidelines, an emphasis on rehabilitation over punishment, and criminal records that are sealed and typically expunged once they turn eighteen years of age. In spite of this, many continue to be criminalized by highly secretive data-driven policing technologies, tools, and programs that cause lifelong collateral consequences. These inscrutable systems have been documented to be racially skewed, are riddled with errors, and have historically

included children as young as eleven years old. Moreover, users rarely notify minors of their inclusion or offer the ability to seek their removal from such systems.

Since the inception of these databases, "police officers have been racially profiling and tracking people – primarily youth of color – suspected of 'gang involvement' often based on what they look like, where they live, and how they dress."[31] These databases also allow law enforcement officers to share extensive information about gangs, and to "collect, store, and analyze personal information about alleged gang members;"[32] with many of them "filled with the names and pictures of thousands of young people of color who have not been convicted of any crimes."[33] As a result of these data-driven policing technologies, tools, and programs, many children continue to be treated as adults in the criminal legal system, in violation of their fundamental rights to special protection and to be tried by a specialized juvenile justice system.

For example, CalGang, a database widely used in California, listed 42 infants under the age of 1 as active gang members.[34] Moreover, because there is "no clear, consistent and transparent exit process" for those on the database, it can be assumed that a significant proportion of "gang" designees were added in their teens and preteens.[35] The Chicago Police Department (CPD)'s database includes more than 7,700 people who were added to the database before they turned 18, including 52 children who were only 11 or 12 years old at the time of their inclusion.[36] An investigation published by *The Intercept* identified hundreds of children between the ages of 13 and 16 listed in the New York Police Department (NYPD)'s gang database in 2018.[37] The Boston Police Department (BPD) uses a point system to determine whether to include someone in its "Gang Assessment Database";[38] making it possible for teenagers to be designated as gang members "simply because of the people they're being seen with,"[39] and without any actual allegation of violence or criminal activity.

This provides "disturbing insights into the police targeting of young people,"[40] and the ease with which officers can add a minor to a database for having a tattoo symbolizing a gang, for wearing clothing associated with a gang, or for repeatedly visiting "a gang area."[41] Because of the secrecy surrounding gang databases, some have even referred to them as hidden "surveillance tool[s] for monitoring children;"[42] with such monitoring often taking place on social media, where officers can search a user's publicly available account and posts; establish an undercover account to interact with a targeted user; or use a search warrant to get additional information about a specific user.[43]

Critics have additionally argued that gang databases — with opaque methods used to obtain intelligence and data for such systems and little information available on how someone gets on or off these lists — function like "black boxes," making them a prime tool for racial profiling.[44] Studies have also shown that once an individual is listed in a gang database, they will likely encounter increased police attention and harassment. Since gang databases make gang identification information significantly more accessible to law enforcement officers, this has resulted in the more widespread stopping of young people of color, even without suspicion of criminal activity.[45]

Impact on Constitutional Rights and the Criminal Process

Data-driven policing has proliferated so quickly that solutions lag for the myriad constitutional rights that are implicated by its deployment and use. The aggregation and classification of vast and disparate types of personal information raises serious concerns about the First, Fourth, Fifth, Sixth, and Fourteenth Amendment rights for those suspected and accused in criminal cases.

Data-driven policing raises serious questions for a Fourth Amendment analysis. Prior to initiating an investigative stop, law enforcement typically must have either reasonable suspicion[46] or probable cause.[47] Does a person loitering on a corner in an identified "hotspot" translate to reasonable suspicion? What if that person was identified by an algorithm as a gang member or someone likely to be involved in drug dealing or gun violence? Can an algorithm alone ever satisfy the probable cause or reasonable suspicion requirement?[48] The lack of transparency and clarity on the role that predictive algorithms play in supporting reasonable suspicion determinations could make it nearly impossible to surface a Fourth Amendment challenge while replicating historic patterns of over-policing.

Data-driven policing databases may also work an end run around the Fourth Amendment by making law enforcement privy to information that would otherwise require a warrant to access. The government rarely discloses its use of data-driven policing technologies. Even if the use of the technology is a matter of public record, the inputs used, training data, and algorithms are proprietary and therefore shielded from scrutiny. This raises a number of due process issues that implicate a person's right to a fair trial.

In *Brady v. Maryland*,[49] the Supreme Court found that the government has an obligation to provide defendants with evidence that is material to a determination of either guilt or punishment. The government's failure to disclose the use of certain technologies or databases may raise a *Brady* issue since defense attorneys will not have the opportunity to challenge whether the results or the tools themselves were inaccurate or improperly deployed.

Algorithmic tools often use claims of proprietary software and trade secrets to shield their technology from outside scrutiny. The companies that develop the tools conduct their own validation studies, rather than rely on independent verification and validation, which is the accepted practice. Allowing companies with a financial interest in the success of their tools to validate their own technologies with no outside scrutiny is scientifically suspect.[50] It also frustrates the ability of the defense to challenge the reliability of the science underlying the novel software.

As the Task Force heard throughout their investigation, data-driven policing tools often reinforce or even exacerbate the racial biases that have always existed in policing. In other words, the government's use of data-driven policing software has a disparate impact on individuals of different races. Problematically, technological tools often enhance the discriminatory effect even as they make it more difficult for individuals to bring an Equal Protection claim. According to legal scholar Aziz Huq:

> The concerns of constitutional law simply do not map onto the ways in which race impinges on algorithmic criminal justice. The result is a gap between their legal criteria and their objects.... The replacement of unstructured discretion with algorithmic precision, therefore, thoroughly destabilizes how equal protection doctrine works on the ground.[51]

Part of the issue is that an Equal Protection claim against facially neutral government action requires that a litigant show discriminatory intent as a threshold element.[52] Data-driven tools are designed in a manner whereby bias is buried beneath the technology. Because any bias is filtered through an algorithm, critics have accused data-driven tools of "techwashing"[53] the biases inherent in the data. There is an inherent conflict between the reality that machine learning is not advanced enough to formulate intent, and the fact that "the unthinking use of algorithmic instruments will reinforce historical race-based patterns of policing."[54]

Although First Amendment concerns are not primary in criminal prosecutions, there are several First Amendment issues raised by data-driven policing programs and technologies. When people are criminalized based on their associations and their participation on social media, they are subject to what Professor Elizabeth Joh calls the "surveillance tax." As Joh writes, the intrusiveness of surveillance extends beyond arrest: "Knowledge of surveillance alone can inhibit our ability to engage in free expression, movement, and unconventional behavior."[55]

Gang designations and inclusion on lists of potential offenders are often based on proximity, associations, social media interactions, comments and posts rather than facts and evidence. The low bar for inclusion in such databases, the lack of notice, the inability to challenge one's inclusion on the list and the real-world consequences of such designations create circumstances where young people are forced to live with the potentially life-changing consequences of such designations based on communications that should be protected speech under the First Amendment.

TASK FORCE RECOMMENDATIONS ON DATA-DRIVEN POLICING TECHNOLOGIES

1. Top-Line Recommendation

Police departments must not utilize data-driven policing technologies[56] because they are ineffective; lack scientific validity; create, replicate and exacerbate "self-perpetuating cycles of bias";[57] deeply entrench

existing inequities in the system; hyper-criminalize individuals, families, and communities of color; and divert resources and funds from communities that should be allocated towards social services and community-led public safety initiatives.

While the Task Force believes these technologies should never be used, it is clear that these technologies are being considered or have been implemented in cities and towns across the country. Lack of access and transparency will hamper defense lawyers' ability to properly represent their clients. The following recommendations are for areas that are already using these technologies. These recommendations are in no way intended to serve as principles for implementing such technologies. Rather, they are mitigation efforts intended to ensure the most transparency and equity for people ensnared by these technologies, and to give defense attorneys the notice and transparency they need to defend their clients.

2. Governing Use

Police departments seeking these tools must not adopt any data-driven policing technology without first meaningfully engaging the communities where it would be deployed and without first securing approval for the technology from the elected governing bodies that represent the impacted communities.

This process must include the residents of the communities where the data-driven policing technologies would be deployed, community organizations, organizations focused on youth from the impacted communities, and attorneys with expertise in upholding the constitutional rights and civil liberties of residents from impacted communities.

As part of engaging impacted communities about the proposed data-driven technology, resources must be allocated to local governing bodies to host forums to present and describe the proposed law enforcement technology to the residents of the impacted communities. These forums would also provide a space for impacted communities and law enforcement to discuss the law enforcement need for the proposed technology, detailing how the policies governing the use, scope, and limitations of the technologies would be implemented within the defined law enforcement need. Resources and space should also be allocated to enable and empower community members to provide feedback about the technology, and to address community concerns about transparency, racial bias, and the impact of the proposed technology on civil liberties and constitutional rights. If there is a majority consensus by state or local governments and impacted communities that the proposed technology should not be used by law enforcement, then the technology should be prohibited.

3. Transparency

Prior to implementing any data-driven policing technology, law enforcement must adopt written policies governing the technology's use. Before adopting these policies, law enforcement departments must make draft policies available to the public, provide the public with opportunities to comment on the draft policies orally and/or in writing, and incorporate public comments into the final policies. For any technology already in use but lacking such policies, law enforcement departments should immediately implement clear public policies that detail the parameters, requirements, and conditions of use.

Tech companies and developers of data-driven policing technologies have asserted trade secret evidentiary privileges as reason to deny defense discovery requests and subpoenas.[58] To facilitate transparency and avoid the exclusion of highly probative evidence,[59] companies that create and supply data-driven policing technology must waive, or otherwise not assert, claims of "trade secret privilege"[60] and must disclose the methodologies used to build the technology to law enforcement, the impacted communities where law enforcement departments intend to deploy the technology, the legislative bodies that represent the impacted communities, and the attorneys within the jurisdiction who specialize in criminal defense and civil liberties to ensure that the technologies are scientifically sound, are employed as intended, and are limited in scope to meet the articulated law enforcement need.

Any data-driven policing technologies that are used should undergo validation studies that allow them to be subjected to a *Daubert* or *Frye* analysis. As matters of constitutional due process rights guaranteed by the Fifth

and Fourteenth amendments, all individuals must be notified of their presence on data-driven databases that law enforcement departments access and utilize, including gang databases, strategic subject lists, and other data collected through social media monitoring. These individuals must also be provided the opportunity, through a private attorney or, if they cannot afford an attorney, an appointed attorney, to challenge their inclusion on such databases, the data accumulated from the databases, and law enforcement's interpretation of the data, as well as to seek removal from the databases.

All individuals, in accordance with constitutional due process rights guaranteed by the Fifth and Fourteenth Amendments, must be notified of their removal from any data-driven databases that law enforcement departments access and utilize, including, but not limited to, gang databases and strategic subject lists.

4. Race Equity

The analysis that jurisdictions undertake when considering whether to adopt any data-driven policing technology must be conducted through a race equity lens and include a racial impact statement. The "racial equity impact assessment"[61] must be conducted by experts trained in institutional and structural racism, as well as the history of racialized policing. These experts should work with legislators, law enforcement, and community members to examine the racialized impact of the proposed data-driven policing technology. If the racial equity impact assessment of the proposed data-driven policing technology concludes that use of the technology would harm the impacted community, the technology should be prohibited from use by law enforcement.

5. Accountability

If, through the processes detailed in Recommendations #2, #3, and #4, data-driven policing technologies have been approved, law enforcement departments must adopt and issue written protocols ensuring integrity and accountability, to ensure that the departments and the impacted communities can continuously monitor and otherwise gauge the use and effectiveness of these technologies.

Integrity and accountability measures must include data-keeping, annual departmental reports on the use and accuracy of the technology, measuring and evaluating the effectiveness of the technologies through auditing, and, based on the results of these accountability measures, determining whether the use of the technology should be modified or discontinued. All reports, evaluations, data, and accountability measures produced in relation to data-driven policing technologies should be made available to the public.

6. Resources and Access for Defense Attorneys

In accordance with the constitutional rights to discovery and confrontation guaranteed by the Sixth Amendment, prosecutors must provide to defense counsel notice and a description of data-driven policing technology that law enforcement has employed or has otherwise relied upon in the case, as well as any data based on the technology that the officers relied upon, assessed, or otherwise used in relation to the accused, including *Brady* material and any other data accumulated against the accused. Defense counsel must then be afforded time and resources to engage experts to analyze and interpret the data.

Defense lawyers must receive notice and training regarding the data-driven policing technologies employed by law enforcement departments in their jurisdictions, including the federal and state constitutional rights implicated by the technologies.

Defense lawyers should collaborate with other attorneys, technologists, and experts who understand the data-driven policing technologies employed against their clients, and should seek to incorporate law enforcement's use of the relevant tool(s) against their clients into all aspects of their representation.

Defense lawyers must have access to data-driven technology experts who can break down the technologies and consult on defense strategies vis-à-vis the data-driven tools that law enforcement relied upon to suspect, surveil, approach, or arrest, or otherwise employed against the accused.

Resources for public defenders and court-appointed counsel must be increased to respond to data-driven policing technologies in order to meet their constitutional obligation to provide zealous representation to clients impacted by these technologies.

7. Courts

Courts and prosecutors must be trained annually on the data-driven policing technologies employed by law enforcement departments, including the federal and state constitutional rights implicated by the technologies.

Judges must assess the reliability of a data-driven policing technology employed against the accused before determining whether it justified a Fourth Amendment intrusion. Data-driven technology must not form part of an officer's calculation of reasonable suspicion, unless the technology can be shown through typical evidentiary burdens that it is reliable.

Law enforcement authorities cannot utilize or otherwise rely upon data-driving technologies, such as gang databases, in any way that infringes upon the right to association guaranteed by the First Amendment.

8. Children and Youth

State and local jurisdictions must enact laws, policies, and protocols that protect the federal constitutional rights, state constitutional rights, and dignity interests of children and youth who are implicated or otherwise at risk of being criminalized by data-driven policing technology.

Law enforcement authorities should not include children under the age of 18 on any law enforcement database, or otherwise accumulate or access data specific to children under the age of 18 through social media monitoring or other data gathering practices.

Young people between the ages of 18 and 25 are especially vulnerable, disproportionately included on data-driven policing databases,[62] and therefore must be provided notice of their presence on any databases that law enforcement departments access and utilize, including gang databases, strategic subject lists, and other databases that incorporate social media monitoring. Individuals must be provided the opportunity, through a private attorney or, if they cannot afford an attorney, an appointed attorney, to challenge their inclusion on such databases, the data accumulated, and law enforcement's interpretation of the data, and, also, to seek removal from the databases.

An individual's ability to challenge their designation and inclusion on such databases, the data accumulated, and law enforcement's interpretation of the data should be ongoing, particularly given the impact of law enforcement interactions with children and youth on their personal development, self-esteem, and educational outcomes — including school attendance, suspensions, expulsions, and matriculation — and the correlation between these factors and involvement with the juvenile and criminal legal systems.

Any data, records, or other information contained in any law enforcement database through any data-driven policing technology and/or social media monitoring should be sealed and purged when the individual reaches 25 years of age, at which point the adolescent brain is fully formed.[63]