Policing Project
NYU School of Law

NYU School of Law
40 Washington Square South
New York, NY 10012

info@policingproject.org
@policingproject
212.992.6950

March 30, 2023

Office of Science and Technology Policy ("OSTP")
Executive Office of the President
Eisenhower Executive Office Building
1650 Pennsylvania Avenue
Washington, DC 20504

Submitted electronically to equitabledata@ostp.eop.gov

Re: Request for Information (RFI) on Criminal Justice Data (88 Fed. Reg. 10150)—Comments of Policing Project at New York University School of Law

The Policing Project is a non-partisan center at New York University School of Law dedicated to promoting public safety through transparency, equity, and democratic engagement. Our work has long recognized that equitable and comprehensive policing data collection & publication is critical to furthering these values, especially at the state and local level.

This comment draws on a number of resources that the Policing Project and its staff members have developed over the years around data collection and transparency:

- Our co-founder, Professor Barry Friedman, served as the Reporter on the American Law Institute's *Principles of the Law, Policing* project, which developed high-level principles on all aspects of sound and equitable policing, including data collection and transparency.[1]

- Drawing on the ALI work, we drafted a model statute on data collection and transparency by state and local law enforcement agencies.[2] The statute, among other things, sets forth the categories and fields of policing data that law enforcement agencies should be required to collect and publish to ensure policymakers and community members have the information they need to assess whether policing practices in their jurisdiction are equitable and sound. The statute was vetted by an advisory committee consisting of law enforcement officials, academics, police reform experts, and affected community members,[3] and informed by the best practices in existing state and local legislation.

[1] *See* Principles of Policing §§ 14.10 (*Data Collection & Transparency*), American Law Institute https://www.policingprinciples.org/chapter-14/14-10-data-collection-and-transparency/, 14.11 (*Research in Support of Sound Policing*), American Law Institute, https://www.policingprinciples.org/chapter-14/14-11-research-in-support-of-sound-policing/.
[2] *Data Collection and Transparency Statute*, Policing Project, https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/62cdcc9f669e1b7afd48fa43/1657654431547/Data+Collection+and+Transparency+Statute_1.27.22+v2.pdf.
[3] https://www.policingproject.org/legislative-advisory-committee.

- We also developed a broader Data & Transparency Framework for Policing Agencies that sets out additional categories of data and information that agencies should endeavor so share with their communities.[4]

- Finally, in partnership with the Center for Policing Equity and the California Department of Justice, we developed a comprehensive Stop Data Guidebook, which provides detailed guidance to agencies and communities on the collection and analysis of traffic and pedestrian stop data.[5]

This Comment is primarily responsive to question 3 (which datasets to collect) of the RFI, but also touches on questions 2, 8, 10, 12, and 17.

I. The Transformative Potential of Policing Data

Comprehensive data is vitally important to help lawmakers and the public assess whether policing in their jurisdiction is conducted in a manner that furthers the goals of public safety while minimizing any attendant harms.

Time and again we have seen that when agencies and lawmakers are confronted with evidence of harmful, discriminatory, or ineffective practices, policies change. For example, in 2017, the Policing Project worked with the Nashville police department to assess the department's strategy of making large numbers of traffic stops in order to investigate and deter crime. Working with researchers from the Stanford Computational Policy Lab, we found that the high volume of stops had no impact on surrounding crime rates, and that only a tiny fraction of stops—less than 1 percent—resulted in the discovery of a weapon or an arrest for a more serious crime.[6] At the same time, the department's stop practices generated significant racial disparities and undermined the department's efforts to forge stronger relationships with Black and Hispanic residents. In response to the study, Nashville police cut traffic stops by more than 80 percent and adopted more targeted strategies to address violent crime.[7] Similarly, after traffic stop data from across Connecticut revealed substantial racial disparities in low-level traffic stops, law enforcement agencies across the state significantly reduced such stops, while increasing stops for DUI.[8]

II. The Current State of Data Collection

Although a number of states and localities have made important advances on data collection and transparency, the reality is that in most jurisdictions data collection is either non-existent or insufficiently robust.[9] Fewer than half of all states require their law enforcement agencies to collect any form of stop

---

[4] *Data & Transparency Framework for Policing Agencies*, Policing Project, https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/5f8effc4cdd45f4e7654de73/1603207108603/Policing+Project+Transparency+Framework+.pdf.

[5] *Collecting, Analyzing, and Responding to Stop Data: A Guidebook for Law Enforcement Agencies, Government and Communities* ("Stop Data Guidebook"), Center for Policing Equity & Policing Project (2020), https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/5f7335d7294be10059d32d1c/1601385959666/COPS-Guidebook+Final+Release+Version.pdf.

[6] *Policing Project Finds Nashville Traffic Stops Ineffective for Reducing Crime*, The Policing Project & Stanford Computation Policy Lab (Nov. 19, 2018), https://www.policingproject.org/news-main/Nashville-report-released.

[7] Samantha Max, *Nashville Police Report Major Drop in Traffic Stops Following Accusations of Racial Bias*, WPLM News (March 25, 2021), https://wpln.org/post/nashville-police-report-major-drop-in-traffic-stops-following-accusations-of-racial-bias/.

[8] Tom Condon, *After a poor start, CT's anti-racial profiling effort is making progress*, CT Mirror (Jan. 30, 2022), https://ctmirror.org/2022/01/30/after-a-poor-start-cts-anti-racial-profiling-effort-is-making-progress/.

[9] *See generally* Barry Friedman and Elizabeth G. Janszky, *Policing's Information Problem*, 99 Tex. L. Rev 1 (2020), https://texaslawreview.org/wp-content/uploads/2020/11/Friedman.Printer.pdf.

data—and of those that do, most collect far too little information to enable any sort of meaningful assessment about law enforcement policies and practices.[10] Even fewer states require that agencies collect data on the use of force. To this day, much of the best data on police killings comes from media publications as opposed to law enforcement agencies themselves.[11] Finally, when it comes to other essential categories of data—such as data on police officer misconduct—only a small number of jurisdictions require agencies to collect and publish the information that communities and lawmakers need.

III. What Data Agencies Should Collect and Publish

The various Policing Project resources discussed above—including our data and transparency framework, and our model data and transparency statute—identify the various categories of data that agencies should collect and publish to provide lawmakers and members of the public with even a basic sense of the impact and efficacy of various department practices. In this Comment, we would like to draw your attention to five particularly important categories of policing data.

a. Officer Encounter & Stop Data

Traffic stops account for the most common interaction between police and members of the public. Estimates suggest more that police pull over more than 20 million drivers every year.[12] Although stops for certain traffic offenses can promote important traffic safety benefits, traffic stops also have the potential to generate significant harm by exacerbating racial disparities within the criminal justice system, facilitating revenue-driven policing, and creating opportunities for potentially violent encounters between officers and members of the public. The collection and publication of traffic and pedestrian stop data thus is essential to generating equitable policing. This data can reveal not only racial and other biases in whom the police are stopping, but also whether the stops are generating any significant public safety benefit to justify their substantial cost.

The Officer Encounter Data section of our model statute (section V, pp. 5-8)[13] sets forth all the data points agencies should collect & publish when it comes to stops and arrests. Here, we highlight some of our key recommendations based on both the statute and our Stop Data Guidebook:

First, agencies should collect demographic data on both traffic *and pedestrian* stops. While a fair number of states require that agencies collect traffic stop data, very few states collect data on pedestrian stops as well. The data then ends up dramatically understating the number of officer-resident encounters in more densely populated areas where pedestrian stops are more prevalent.

Second, it is important that agencies collect enough data on each stop to facilitate meaningful analysis. At a minimum, officers should be required to record:

> (1) The perceived race or ethnicity, gender, and age of the person stopped;
>
> (2) The reason for the stop, i.e. whether the stop was conducted on the officer's own initiative or in response to a call-for-service, and whether the stop was based on a moving violation, an equipment violation, or suspicion of criminal activity;

[10] *Traffic Stop Data*, NCSL, https://www.ncsl.org/civil-and-criminal-justice/traffic-stop-data.
[11] *See, e.g.*, *Fatal Police Shootings Database*, The Washington Post (updated March 21, 2023), https://www.washingtonpost.com/graphics/investigations/police-shootings-database/; *Data and Methodology*, Mapping Police Violence, https://mappingpoliceviolence.org/methodology.
[12] *Findings*, The Stanford Open Policing Project, https://openpolicing.stanford.edu/findings/.
[13] *Data Collection and Transparency Statute*, Policing Project.

(3) The actions that the officer took during the stop, including whether the officer asked for consent to search, whether a search was in fact performed either based on consent or suspicion of criminal activity, and whether the officer resorted to force during the stop; and

(4) The outcome of the stop, including whether the officer issued a warning or a citation, whether any contraband was found, and whether the stop resulted in an arrest.

The above data fields are essential to enable agencies and researches to assess, among other things, (a) the extent to which certain categories of stops are furthering public safety by resulting in the discovery of contraband or generating arrests and charges for serious crimes; (b) whether particular categories of stops are disproportionately responsible for any racial or other disparities; (c) how often police are conducting searches based on consent rather than probable cause; and (d) how often police stops escalate into violent encounters.

Third, with respect to demographic data, agencies should require officers to indicate the *perceived* race or ethnicity, gender, and age of the person stopped. This means officers should record data based on initial perceptions, at the earliest point in time that the officer perceives these characteristics. As the Stop Data Guidebook explains, "[u]sing the officer's perception is broadly supported in social science research as the best way to assess disparities and potential bias in stops: if bias is factoring into an officer's decision to make a stop, perception is the relevant variable."[14] Indeed, racial information is often not provided on a driver's license, and asking someone stopped to self-report race could needlessly escalate the stop.

Fourth, incident-level stop data should include a unique identification number for the officer who conducted the stop. Doing so would enable lawmakers and researchers to determine whether troubling patterns in the data are driven by a few officers, or are indicative of an agency-wide problem.

Fifth, states should facilitate public analysis of traffic and pedestrian stop data by aggregating and publishing local agency data in an accessible manner. A number of states do a particularly good job of this. Virginia, for example, publishes and visualizes its stop data on an easy-to-navigate open data portal, and makes incident-level data available for download.[15] Several other states, including California and Connecticut, provide easy access to local incident-level stop data as well.[16]

b. **Use of Force Data**

Agencies should similarly collect comprehensive data on officer use of force in order to enable the public to determine how frequently officers are using force against members of the public, the degree of force used, and whether force is used disproportionately against particular demographic groups. Section VI of our model statute (pp. 8-10)[17] sets forth the use of force data fields that agencies should collect and publish. Again, we highlight our key recommendations below:

First, agencies should collect data on all significant use of force incidents—not just those that result in death and serious bodily injury. At present, most of the 19 states that require law enforcement agencies to collect use of force data limit collection to critical incidents, including police shootings or other uses of

[14] Stop Data Guidebook at 16.
[15] *Community Policing Act Data Collection,* Virginia Open Data Portal, https://data.virginia.gov/stories/s/Virginia-Community-Policing-Act-Data-Collection/rden-cz3h/.
[16] *RIPA Stop Data,* CA DOJ OpenJustice Data Portal, https://openjustice.doj.ca.gov/data; *Connecticut Traffic Stop Data,* CT Data Collaborative, http://trafficstops.ctdata.org.
[17] *Data Collection and Transparency Statute*, Policing Project.

force that result in death or serious bodily injury.[18] The FBI's own (voluntary) national use of force data collection program is similarly limited.[19] These data collection efforts are substantially underinclusive. They omit, for example, instances in which an officer uses a chokehold, deploys a canine to bite a suspect, punches a suspect in the face, or deploys a Taser or other weapon. We recommend that agencies, at a minimum, collect data on all uses of force that (i) result in physical injury or (ii) involve the use of a weapon or deployment of a canine.

Second, as with stop data, agencies should collect and publish enough information about each use of force incident to facilitate meaningful analysis. That includes essential data fields like whether the officer perceived a subject of the use of force to be armed, whether they were in fact armed, and what they were armed with. These data points are critical for determining whether officers have a pattern for using excessive or disproportionate force. Similarly, to get a more complete picture of the harm imposed by officer that use force, officers always should log both the type and severity of any injuries sustained. Finally, agencies should be collecting (i) the officer's unique identification number and (ii) the perceived race or ethnicity, gender, and age of each person at whom force was directed, for the same reasons discussed above.

c. Complaint & Disciplinary Data

Agencies also should collect and publish data on complaints of police officer misconduct filed by members of the public. Such data can help lawmakers and researchers identify patterns of misconduct and determine whether agencies are adequately investigating and imposing discipline on officers who engage in misconduct. Again, our model statute (at Section VII, pp. 10-11)[20] sets forth the definitions and data fields that should apply to the collection and publication of complaint data. Here we highlight two points of particular importance in any complaint data collection statute or policy:

First, states or the federal government should ensure that agencies are using a uniform—and sufficiently broad—definition of what constitutes a "complaint." One of the challenges in making sense of complaint data is that data often are susceptible to conflicting interpretations. A small number of complaints, for example, may indicate that an agency's officers rarely engage in misconduct—or that the agency has put up far too many barriers to dissuade members of the public from filing legitimate complaints. Uniform definitions can help to address these concerns, at least to some extent.

A uniform definition should make clear that agencies must report *all* complaints submitted to *all* relevant entities (e.g., police department, police oversight agency); "complaint," too, should be defined broadly enough to include *any* allegation of misconduct by an officer against any member of the public. And the policy should make clear that anonymous/unsworn complaints, complaints submitted by a third party, or complaints communicated over the phone or by e-mail all must be logged.[21]

Second, agencies need to collect enough information about each complaint to facilitate meaningful analysis. Such fields include the nature of the misconduct, whether the complaint was investigated and the status or conclusion of any investigation conducted, a name/unique ID and beat for each officer alleged to have engaged in misconduct, and any disciplinary action taken by the agency and whether that action is final. These data can help lawmakers and researchers determine, among other things, whether agencies are regularly and timely investigating allegations of serious misconduct, whether agencies are imposing

[18] *Use of Force Data*, NCSL, https://www.ncsl.org/civil-and-criminal-justice/use-of-force-data-and-transparency-database.
[19] *See National Use-of-Force Data Collection*, FBI, https://www.fbi.gov/video-repository/national-use-of-force-data-collection/view.
[20] *Data Collection and Transparency Statute*, Policing Project.
[21] *See, e.g., id.* at VII(1)(c), p. 11 (definition of complaint being "received").

adequate discipline on officers with substantiated misconduct complaints, and whether particular officers or beats are disproportionately drawing complaints.

—

Finally, we would like to draw your attention to two additional buckets of data that may well be held by entities other than law enforcement agencies, but which can nonetheless provide important insights on agency practices.

d. Police Misconduct Settlement & Judgment Data

Lawmakers and the public should know how much of the public's tax dollars states and municipalities are spending on payouts (by way of settlements or court judgments) following alleged police misconduct. Yet only a tiny number of states or localities collect and publish such data, leaving taxpayers and lawmakers in the dark about the complete costs of police misconduct. Our model statute section on settlement and judgment data (at Section IV, pp. 4-5)[22] sets forth the appropriate data fields to collect—including not only the amount and basis for any settlement and judgment, but also the amount that the jurisdiction pays in insurance premiums or risk pool contributions in order to insure against such payouts.

e. Device-Generated Data

Every day, policing technologies generate enormous quantities of data. Each time a Taser is fired, a body-worn camera is activated, an automated license plate reader generates an alert, or evidence is accessed in a digital evidence management system, a record of this activity is generated automatically.[23]

In the right hands, this data could do much to shed light on current police practices. For example, data generated by Tasers can reveal not only how often the devices are fired (and whether they are fired multiple times in a single incident), but how often they are drawn or "arced"—actions sometimes used by officers as an intimidation tactic.[24] Data from body-worn cameras and the systems used to store body-worn camera footage could be used to determine how often cameras are activated and how often footage is reviewed by supervisors.[25] Data from digital evidence management systems can show the types and quantities of evidence police collect—everything from documents and photos to data extracted from cell phones through mobile digital forensic tools.[26] Automated license plate readers (or "ALPRs") often are configured to alert

---

[22] *Data Collection and Transparency Statute*, Policing Project.

[23] Often this data is accessible to agencies in the form of an "audit trail"—logs of user activity automatically generated by many policing technologies. *See, e.g.*, *Device Audit Trail Information*, Axon, https://my.axon.com/s/article/Device-Audit-Trail-Information?language=en_US.

[24] *See, e.g.*, *Policy 719—Conducted Electrical Weapon* 7 (2016), Baltimore Police Dep't, https://www.baltimorepolice.org/transparency/bpd-policies/719-conducted-electrical-weapon-cew (describing an arc as a "show of force" used to warn a suspect that "a [Taser] may be used on him or her"); *Taser 7 Pulse Graph Overview*, Axon, https://my.axon.com/s/article/TASER-7-Pulse-Graph-Overview?language=en_US (displaying some of the data generated by Taser devices) .

[25] Some vendors offer additional tools enabling analysis of agency-wide data related to body-worn camera use. Motorola's system, for example, can create reports which "provide insight into body camera usage and adoption, such as average video length and volume, policy compliance, officer behavioral changes and storage consumption." *See Capture Every Encounter: The V300 Body-Worn Video Solution*, Motorola Solutions, https://www.motorolasolutions.com/content/dam/msi/docs/products/body-worn-cameras/v300-brochure.pdf.

[26] *See Digital Evidence Management: The Definitive Guide*, Axon, https://www.axon.com/news/digital-evidence-management-guide (discussing the types of evidence that can be stored through a digital evidence management system, including evidence from "body worn cameras (BWCs), dashboard cameras, smartphones, and even TASER energy weapons").

police when they detect a vehicle on a "hotlist" of wanted vehicles; these systems generate data which can reveal how often agencies receive alerts associated with felonies, property crimes, outstanding warrants, and the like.[27]

That this data exists but has not widely been made available to researchers, policymakers, and the public is a missed opportunity. Because this data is generated automatically, there is little or no administrative burden involved in its collection. Indeed, in the case of systems in which data across policing agencies is stored in the vendor's cloud, there already is something akin to nationwide data collection, and the data could be obtained directly from vendors.

Accordingly, we believe that the federal government should begin to explore ways that this device-generated data could be collected and made publicly available for the purpose of understanding and improving police practices.

A starting point would be to consider where this device-generated data might live. The federal government might consider the feasibility of creating a central repository where data can be collected and made available to researchers and the public, similar to the Federal Bureau of Investigation's collection and publication of crime and use of force data.[28] Ideally, this database would enable the public both to access the raw data and to make comparisons across jurisdictions and over time.

The federal government might also consider ways to incentivize vendors and/or policing agencies to provide this data voluntarily. This might include examining whether, consistent with existing law, grant funding for policing technologies can be conditioned on the provision of non-law enforcement sensitive data related to the technology. For example, a Justice Assistance Grant enabling an agency to purchase ALPRs could be conditioned on the agency providing data related to hotlist hit rates and the offense types for which the devices alerted.

In short, device-generated data could lend valuable new insights about police practices along a number of dimensions. We believe the idea of collecting and publishing this data for the benefit of researchers, policymakers, and the public is worthy of further exploration.

Thank you for the opportunity to comment.

Respectfully submitted,

Barry Friedman
Founder and Faculty Director

Josh Parker
Senior Counsel

Maria Ponomarenko
Co-Founder and Counsel

Max Isaacs
Staff Attorney

---

[27] *See Axon AI & Policing Tech. Ethics Bd., Automated License Plate Readers* (2019), Axon, https://static1.squarespace.com/static/58a33e881b631bc60d4f8b31/t/5dadec937f5c1a2b9d698ba9/1571679380452/Axon_Ethics_Report_2_v2.pdf (discussing law enforcement use of ALPR hotlists).

[28] *See Crime Data Explorer*, Federal Bureau of Investigation, https://cde.ucr.cjis.gov/LATEST/webapp/#/pages/home.