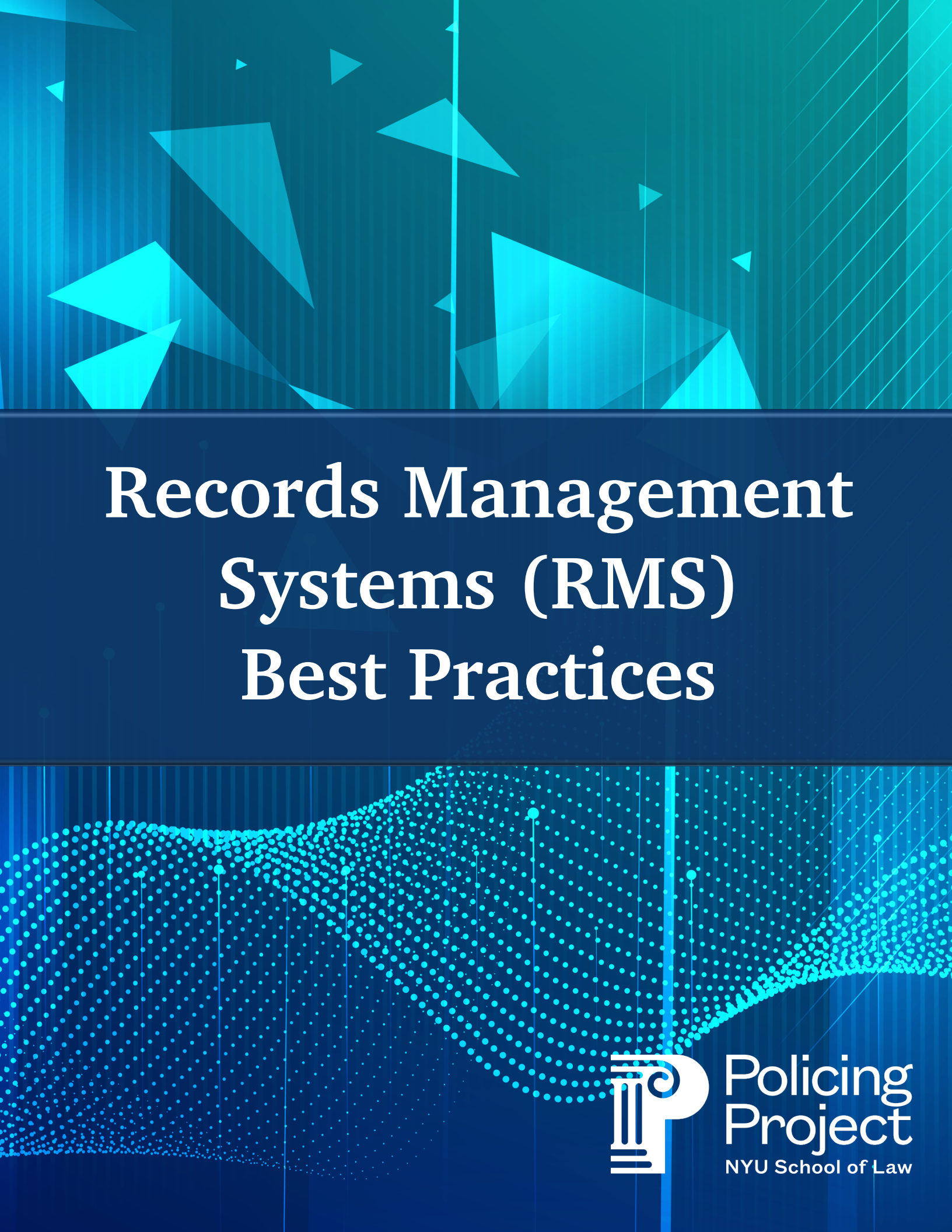
Records Management Systems (RMS) Best Practices



Policing Project
NYU School of Law

Introduction

Every day, police work generates paperwork — victims report crimes; witnesses provide statements; officers gather evidence; individuals are booked into jails.

Today, rather than relying on paper forms, most of this data can be entered into a records management system, or "RMS."

It would be a mistake to think of an RMS as nothing more than a virtual filing cabinet. RMS systems enable police to aggregate, search, analyze, and share vast quantities of data of varying types: criminal histories, incident reports, court records, photographs and physical descriptions, employment information, medical conditions, personal affiliations, and more. This data, once collected, can stay in an agency's RMS for months or even years, and can be searched and shared with ease.

The aggregation of data in RMS systems can have a substantial impact on public safety, civil rights, civil liberties, and racial justice — in ways both good and bad. For example, RMS systems can increase transparency and accountability by facilitating the collection and reporting of data about police encounters and use of force. But RMS can be used to collect data about individuals that invades personal privacy. The creation of gang databases through RMS systems can perpetuate racial bias, and there is a serious risk that inaccurate data might lead to erroneous police contact and enforcement.

The purpose of this document is to set forth some best practices for police use of RMS, with the goal of helping agencies and policymakers increase the benefits the public can derive from RMS while minimizing the harms. The intention is to provide useful guidance both to policing agencies and to the governmental officials — elected and otherwise — who fund, acquire, and use these RMS systems. Democratic accountability around police use of RMS is essential, and these best practices can serve as a framework for potential regulation. RMS vendors, too, could benefit from taking note of these suggestions.

The best practices are divided into two categories, related to (1) the collection of data about individuals and (2) the collection of data about the police. Some of what we say here is familiar, but not always (or even often) followed. Some is quite novel.

RMS systems have been adopted widely by policing agencies; yet there has been too little attention paid to how their use impacts public safety, civil rights, civil liberties, and racial justice in a variety of ways. For the most part, RMS systems do not get much attention at all — though they should. The best practices which follow are designed to address these vital issues.

1. The collection of data about individuals

Police often use RMS systems to collect, store, and search for information about individuals with whom they come into contact. These records can include a vast array of personal information — from an individual's name and physical description to their contact information, citizenship status, drug or alcohol use, and affiliations.[1] This section details the potential harms of this data collection and offers best practices designed to mitigate them.

1.2 Information accuracy, generally

Inaccurate data in RMS systems is a serious risk — such data can result in unnecessary police contact and enforcement, as well as wasted officer resources. Potentially, this can have grave real-world consequences — for example, data which erroneously indicates that an individual is known to have a weapon could prime officers to use force in any encounter.

> Beyond basic information, such as a person's name, sex, and physical description, any information in an RMS should be substantiated with objective supporting documentation.

This documentation might come from a range of sources, including court records, arrest records, officer reports, witness statements, and information derived from government databases such as DMV or firearm permit databases. Information provided by informants might also be included, provided officers document the source of the information and why the source is considered reliable.

1.2.1 Warrant database accuracy

There are serious accuracy concerns related to the use of RMS to track outstanding warrants. Warrant databases often include errors which can lead to erroneous enforcement actions. "Ghost warrants" — warrants from cases that have already been dismissed or adjudicated but continue to lead individuals to get arrested and jailed — are but one example.[2]

[1] These records are stored in a database referred to in RMS systems as a "Master Name Index." *See* Law Enforcement Information Technology Standards Council, Standard Functional Specifications for Law Enforcement Records Management Systems (RMS) 3, https://bit.ly/3pBGEGN.

[2] *See* Eli Hager, *They're Haunted by 'Ghost Warrants' Years After Their Arrests*, Marshall Proj. (Apr. 29, 2019), http://bit.ly/3rYHNJH.

If an agency uses RMS to track warrants, the agency must have a system to check entries against court records periodically to remove outdated or "stale" entries. Additionally, agencies should have a formal process ensuring that officers verify that warrants are active and correct before someone is seized or taken into custody.[3]

These processes are key in ensuring that the use of RMS to track outstanding warrants does not lead inadvertently to wrongful stops or arrests.

1.2.2 Gang database accuracy

A leading concern about RMS systems is their use to create so-called "gang databases," which often are rife with inaccurate data. An audit of California's gang database, for example, found that dozens of individuals entered in the system had birthdates indicating they were less than one year old at the time their information was entered.[4] There are many documented cases of individuals being deemed gang members for what might equally be lawful and innocuous activity — such as wearing certain attire or frequenting a particular neighborhood.[5] These gang designations can have serious consequences — suspected gang members face increased police contact and can be penalized with gang-related sentence enhancements or charged with gang-related offenses. And, troublingly, the racial makeup of gang databases tends to skew heavily toward Black and Hispanic representation — in 2018, for example, 99% of individuals in the New York City Police Department's gang database were Black or Hispanic.[6]

For these reasons, if agencies collect data on gang activity — and there is enough evidence of inaccuracy and misuse to call the practice into question generally — it is crucial that they take certain precautions:

First, limit the criteria for inclusion in a gang database. Agencies might track individuals who have been convicted of gang-related offenses, but not individuals who merely associate with gang members or frequent areas with gang activity. The latter are unreliable indicators of gang

[3] A suggested process for conducting such verification is laid out on model warrant reform legislation created by the Policing Project. *Warrant Reform*, POLICING PROJECT, https://www.policingproject.org/warrant (last visited June 22, 2023).

[4] *See Beware of Gangster Babies: Calif. Database Slammed*, CBS NEWS (Aug. 15, 2016), https://www.cbsnews.com/news/calgang-california-gang-database-slammed-listing-babies-privacy-concerns.

[5] *See* Joel Rose & Sarah Gonzalez, *Sports Jersey or Gang Symbol? Why Spotting MS-13 Recruits Is Tougher Than It Seems*, NPR (Aug. 18, 2017), https://www.npr.org/2017/08/18/544365061/identifying-ms-13-members; Mick Dumke, *Chicago's Gang Database Is Full of Errors — And Records We Have Prove It*, PRO PUBLICA (Apr. 19, 2018), https://www.propublica.org/article/politic-il-insider-chicago-gang-database.

[6] *See* Daryl Khan, *New York City's Gang Database Is 99% People of Color, Chief of Detectives Testifies*, JUVENILE JUST. INFO. EXCHANGE (June 14, 2018), https://jjie.org/2018/06/14/new-york-citys-gang-database-is-99-people-of-color-chief-of-detectives-testifies.

membership — many people have no choice but to frequent such areas or to associate with family members who have gang affiliations.

Second, require officers provide a specific reason why they believe an individual is gang-involved. A simple "gang member" label, without more, does not provide the accurate and objective information officers need to make an informed assessment about an individual. As noted above, any such indication should be supported by some form of documentation.

Third, use caution when relying on self-admission as grounds for entry in a gang database. Particularly for youth and particularly on social media, admissions can be unreliable — young people may falsely declare gang affiliation to achieve status in a community or engage in puffery to deter violence against them.[7] When relying on self-admissions, officers should collect appropriate documentation and exercise professional judgment in determining whether the admission is reliable.

Fourth, remove individuals from the database after a specified period of time unless there is new evidence of gang membership. Studies show that most youth who join a gang do not remain in it for an extended period of time — indeed, the average amount of time youth remain in a gang is one to two years, with fewer than ten percent reporting involvement for four or more years.[8] Given the consequences of being in a gang database, it is important that this information be current. Studies show it frequently is not.

Fifth, routinely audit entries in the gang database to ensure compliance with applicable laws and policies. Auditing gang database entries is crucial, as in some cases individuals have been included in gang databases without adequate documentation that they meet the agency's criteria for inclusion.[9]

1.3 Privacy

The use of RMS to collect personal information about individuals gives rise to significant privacy concerns. As discussed, RMS systems enable the collection of a vast range of data about individuals, from their contact information and employer to their personal associations and medical conditions. The collection of this data can be invasive. Collection also has the potential to undermine investigations: the knowledge that any interactions with police may result in the creation of a permanent record in police files could deter individuals from talking to police and coming forward with evidence.[10]

---

[7] *See* Forrest Stuart, *Code of the Tweet: Urban Gang Violence in the Social Media Age*, 67 Soc. Probs. 191, 197 (2020).

[8] *See Frequently Asked Questions About Gangs*, Nat'l Gang Ctr., http://bit.ly/3qfCqFI.

[9] *See, e.g.*, Office of the Inspector General for the NYPD, An Investigation Into NYPD's Criminal Group Database 7 (2023), https://www.nyc.gov/assets/doi/reports/pdf/2023/16CGDRpt.Release04.18.2023.pdf.

[10] Privacy rules encourage victim reporting, "including domestic violence and hate crimes targeting LGBTQI+ people, people of different religions, undocumented individuals, people of color, and more." *See* Nat'l Sci. & Tech. Council, Equity & Law

Agencies only should collect information about individuals that directly relates to, or is reasonably likely to lead to new evidence or information relating to, an ongoing investigation. Agencies should automatically delete information about individuals after a specified period of time, provided the underlying case has been resolved.

These minimization requirements help to reduce the amount of unnecessary and potentially invasive information agencies collect through RMS.[11] The sharing of collected data between agencies also can have significant privacy implications. Before agreeing to share data, an agency should ensure that this data is relevant to an ongoing investigation by the requesting agency.

2. The collection of data about police

RMS systems also can be used to collect data about a range of policing activity, from traffic stops to arrests to uses of force. Although this information would be useful to society, policing agencies tend not to collect it — or, if they do, they often choose not to make this data public.

This section discusses how RMS can be used to track officer performance. It also details what information about officer enforcement activity should be collected and reported to policymakers and the public.

2.1 Officer performance

Agencies often use RMS systems to track officer activities in the field. For example, supervisors might use RMS to determine how many vehicle stops an officer initiated in a given timeframe, or how many arrests they made.

Many agencies rely on this type of data in evaluating officers. These "productivity measures," (also referred to colloquially as "quotas") often are employed as a benchmark against which to measure officer performance. The measures commonly collected tend to relate to enforcement actions, such as the number of arrests made, or citations handed out.

Which activities agencies choose to track using RMS can have a powerful influence on officer behavior. An overemphasis on enforcement data as the measure of officer effectiveness can have negative consequences. It can create incentives to boost arrest and citation rates. These incentives have led to instances of officers falsifying gang entries, planting drugs on individuals, citing fictitious drivers, and

---

Enforcement Data Collection, Use, and Transparency 6 (2023), http://bit.ly/3Qh7krS.

[11] Given the potential privacy risks posed by data collection, agencies might also consider a requirement that only certain authorized and trained users have access to sensitive forms of information. An agency's policy might also specify that such information may be accessed only on a need-to-know basis.

ticketing dead people.[12] Even in the absence of misconduct, incentivizing enforcement can lead to over-enforcement, which causes its own harms, including over-criminalization, mass incarceration, and community distrust of policing in general. For these reasons, agencies may want to reconsider altogether evaluating officers based on enforcement rates.

Equally of concern, focusing on enforcement numbers neglects other important measures of officer performance — such as an officer's relationships in the community and their work to keep individuals out of the criminal legal system altogether.[13]

> Agencies should use RMS to track positive actions officers take to promote public safety.

These actions might include mentorship, speaking to violence interrupters, attending community meetings, engaging in diversion, spending time with business owners, and referring individuals to social services. Incentivizing these activities can help strengthen the relationship between police and the communities they serve, while reducing unnecessary enforcement.

> In addition, agencies should use RMS to track internal affairs data, including complaints against officers and allegations of misconduct.

These data can provide important insights in evaluating officers; agencies should use RMS to collect these data and track them over time.

2.2 Transparency and reporting

Transparency is the foundation of democratic governance. Without adequate information, the public cannot have informed opinions and policymakers cannot make informed decisions. Yet, at present, much of policing is a black box.[14] At the national level, we do not even know how many people are stopped, injured, or killed by police each year. Our data on crime rates largely is incomplete, and we know even less about how often cases are resolved. Without good data, it's almost impossible to make responsible policy choices and hold police accountable for their successes and failures.

2.2.1 Crime data

One important source of data is the FBI's National Incident-Based Reporting System, or "NIBRS," which captures detailed data about criminal incidents in order to better understand crime at the state and national

[12] *See* Shaun Ossei-Owusu, *Police Quotas,* 96 N.Y.U. L. Rev. 529, 577 (2021).

[13] *See id.* at 579–80.

[14] *See* Nat'l Sci. & Tech. Council, *supra* note 10, at 2 (noting that most agencies do not participate in the FBI's use-of-force data collection, and that "police datasets often do not include demographic, geographic, and other variables necessary to advance more equitable policing outcomes").

level. Many agencies use their RMS systems to collect and report this data. But agencies are not legally required to collect and report NIBRS data and many do not, depriving the public of critical insights about crime and policing.

Even if it is not required by law, all agencies should collect and report NIBRS data. This can be facilitated through the use of RMS systems, which can be configured to collect NIBRS data and transmit it to the FBI.

2.2.2 Use-of-force data

Police use of force is another area in which better data is sorely needed. Given the potential for death or serious injury, use of force often is at the forefront of debates about policing. For this reason, data collection and transparency around use of force incidents is imperative. Yet most agencies fail to participate in the FBI's National Use-of-Force Data Collection program — an initiative through which policing agencies can report data on their use of force and the public can access this data through an online portal.[15]

Agencies should collect and track data on police use of force and participate in the FBI's National Use-of-Force Data Collection program.

RMS features can help ensure agencies are collecting complete and accurate data by including the data points necessary to assess how officers use force, such as demographic data, details about the force used and injuries sustained, and whether the officer tried to deescalate.

2.2.3 Data on police encounters

Beyond use of force, there generally is a lack of information about how police interact with the public. Data related to police encounters could give lawmakers and the public crucial insights about policing and help guide the development of policy.

Given the countless ways in which police interact with the public, agencies may not be able to collect data on every encounter. Agencies should prioritize the collection of data on encounters which result in a stop, search, use of force, or enforcement action such as an arrest or citation.

[15] *See* Tom Jackman, *FBI May Shut Down Police Use-of-Force Database Due to Lack of Police Participation*, WASH. POST (Dec. 9, 2021), https://www.washingtonpost.com/crime-law/2021/12/09/fbi-police-shooting-data.

Officers should be required to record, in the RMS system, the specific reason for any encounters.

For encounters they indicate are consensual, officers should specify whether they suspected the individual of wrongdoing. For traffic stops, officers should indicate the basis for the stop, such as the particular infraction.

Body-worn and dash cameras can play a key role in collecting data about the reasons for police encounters. Absent exigent circumstances, officers should state on camera the reason for an encounter before initiating it. This provides documentation of the basis for the encounter, and this information can later be transcribed and entered into the RMS system.

Other information agencies should collect includes whether a search was conducted (and, if so, the type of search and the legal basis for it), whether force or a threat of force was used, whether any enforcement action was taken, and, for vehicle stops, whether a person was asked to exit their vehicle.

The collection of such data can give policymakers and the public crucial insights about how communities are policed. To this end, agencies should consider the use of "data dashboards" — tools which can be used to share data about police activity with the public.[16]

As with other categories of information, RMS can be helpful not only in collecting data, but also in reporting it to responsible state agencies. RMS providers can work to create integrations with the data management software used by state agencies, which can assist local agencies in providing complete, timely data to the state.

It is important to bear in mind that the purpose of collecting data on police encounters and enforcement activity is to increase transparency and accountability, not to implement police quotas — as explained above, enforcement data is a flawed and incomplete measure of officer performance.

Conclusion

Although they receive little attention, RMS systems play an important role in public safety. Smart policymaking can maximize the benefits and minimize the costs of these tools, enhancing transparency, accountability, and public trust in law enforcement.

[16] *See* Dave McClure et al., Designing an Effective Law Enforcement Data Dashboard, Community Oriented Policing Servs., U.S. Dep't of Just. (2023), https://cops.usdoj.gov/RIC/Publications/cops-w1011-pub.pdf.