The Bill Blackwood
Law Enforcement Management Institute of Texas

Law Enforcement Data Sharing: It's Not an Option

A Leadership White Paper
Submitted in Partial Fulfillment
Required for Graduation from the
Leadership Command College

By
Jeremy Polk

University of North Texas Police
Denton, TX
February 2021

ABSTRACT

Law enforcement case information mostly exists within the silo walls of each individual agency. The FBI runs the N-DEx (National Data Exchange) that collects law enforcement case information, making it available to other agencies through an online search portal. Some Texas agencies voluntarily contribute to this database in conjunction with their records management systems (RMS), but only a relatively small number out of all in Texas (and the nation) participate ("Texas Data Exchange," n.d.).

Making an agency's case and suspect information available to all law enforcement entities seems like a common-sense approach to law enforcement in the 21st century, yet the simple act of sharing information has not taken its rightful place in mainstream law enforcement today. Many professional decisions are made without all available information, and worse yet, made without regard to the work and experience that has come before them. In addition to better statewide information sharing, it is likely all police agency divisions could work together and more efficiently if they had a more complete picture of any given situation.

Any new mandate or additional workload provided to a police agency by an outside influence can create resistance or opposition based on the challenges presented by that new process. Technology is not exempt from this phenomenon and any list of problems to be overcome with the implementation of new technology or policy is not often a short one. However, the problems named in the realm of information sharing are easily overcome or have already been solved. Therefore, the State of Texas should mandate police department data sharing and contribution to the FBI N-DEx database.

TABLE OF CONTENTS

INTRODUCTION

In the history of criminality as a profession, criminals have long since operated in the blind spots of law enforcement officials. Knowledgeable criminals exploited the information sharing limitations of the lawman, especially those in smaller agencies and more rural areas (Hollywood & Winkelman, 2015). Adding to the complexity of pre-technological investigations, many such pursuits were often multi-jurisdictional. As technology advanced, each branch of law enforcement moved forward with their own agendas, in a competitive, almost sealed environment. This professional arrogance and penchant for individuality led to an environment not conducive to collaboration.

Prior to September 11th, 2001 (9/11), the bureaucratic impediments and hermit-like law enforcement culture at all levels served as blinders to cross-jurisdictional criminal activity. This has even been likened back to the days of the post spy game-era of the 1970s when the act of chasing criminals was simply done in secret ("The Need to Share," 2007). In one of the more scathing criticisms of modern governmental function, the 9/11 Commission chided law enforcement for storing intelligence and data in "silos" ("The 9/11 Commission Report," 2004), a failure of thinking, leadership, and procedure that ultimately led to the development of a gaping blind spot, eventually allowing for the terrorist attacks now cemented into our country's history.

One of the best recommendations to come from the commission's report was the call for improved information sharing between law enforcement entities ("The 9/11 Commission Report," 2004). Every agency likely has massive amounts of data stores built up through their daily activities, and although most of those data entries could be thought of as superfluous, there undoubtedly sits in every repository of digital 1s and 0s

a metaphorical key to another's criminal puzzle. However, due to the way each individual agency creates, stores, and accesses their own data, there has never been a state or national push to make such data available to outside personnel.

The Federal Bureau of Investigations' (FBI) National Data Exchange (N-DEx) (n.d.), a national data repository built for law enforcement data sharing and collaboration, was brought online just a few years after 9/11, but, the adoption of its architecture and use of the system by agencies in the U.S. has been slow. For example, at the time of this writing in the state of Texas alone, the Texas Department of Public Safety reports there are only a few more than 500 agencies contributing data to the exchange ("Texas Data Exchange," n.d.) out of a total 2696 commissioned entities ("Current Statistics," n.d.), which is a paltry participation rate of 19%.

Almost two decades later, a failure by any Texas agency to participate in data submission to N-DEx, given the current availability and capability of this system, further creates blind spots and inefficiencies (Sizer, 2018). Information supplied to the National Crime Information Center (NCIC) by agencies is considered "high-level" data, which almost all utilize to some degree. However, the "low-level" data consisting of general case and incident information, arrest, jail and court records, traffic citations/warnings, vehicle information, etc. make up an estimated 97% of the agencies' data stores. This is likely data that receives little attention but could be invaluable in clearing lower level crimes (Reynolds, Griset, & Scott, 2006). The sharing of one's agency data to the national repository, which in turn allows for immediate access by any other approved entity, would provide access to more information in less time (Wertheim & Badgett, 2018), help solve past crimes and those occurring daily, allow searchers to resolve

larger patterns, and more effectively deploy resources (Plecas, McCormick, Levine, & Neal, 2011; Sanders & Henderson, 2013; Sizer, 2018; “The Need to Share,” 2007).

In addition to the obvious advantage of speed of information discovery, investigators have long utilized such information sharing networks, both informal and formal. However, patrol officers could use this information to help bolster their decision making in the field during live incidents, thereby providing an immediate effect on public safety and helping all divisions of an agency work together more efficiently. Along with the ability to impact public safety in a more rapid way, officers may develop a better sense of self and ability, while helping work product improve in quality. Given that many of the cost and technological hindrances have been eliminated and privacy concerns addressed, there may be no reasonable argument against an agency’s participation.

Having learned many lessons, larger national law enforcement agencies such as the FBI admit that no one besides local and state jurisdictions are better positioned to identify and target crime in their communities (Joyal, 2012). It is clear that change is necessary, but alone the voluntary suggestions of the 9/11 Commission are not bringing the recalcitrant law enforcement profession into the modern era with the best practices of data sharing without a clear requirement and support by police organizations and political machines. As a result, all law enforcement agencies should mandate the submission to and use of a central data repository, such as the FBI’s N-DEx.

POSITION

The amount of information available to a decision-maker has always been considered an important factor in that process. If the preponderance of a topic was dependent upon seeking out knowledge, whether or not the existence of that knowledge

was known, then it would be prudent to do so. If someone knew that there was likely a large amount of information relating to their problem, it would be categorically derelict to *not* explore that path. It is understood that more available information leads to better decision making.

While upper-level federal agencies and large departments with active counterterrorism units have used information sharing and fusion centers for years now, state and local agencies mostly use N-DEx at the detective level (Skogan & Hartnett, 2005). It is likely that this use has been limited to major crimes work. Other than internal records, most patrol officers' only link to shared data is the NCIC system that provides suspects' criminal histories, which are often used in decision-making and suspicion-building processes.

Tillyer (2014) found that officers' knowledge of prior suspect behavior affected their own discretionary enforcement behaviors. The same study also reported that in instances when officers used data such as criminal histories to gain more complete views of suspects, race was lessened as a statistically significant variable in their use of discretionary searches on traffic stops. Although a reduction in bias-based decision making is not a main topic of this paper, the surprise benefit should be appreciated by all.

Although criminal histories are a great indicator of a person's past and possible future behavior, they are limited in scope. Access to central data shares would provide patrol officers with not only historical data of past crimes, but historical data of past and current investigations and other general contacts with police, allowing for better pattern recognition and more robust building of probable cause in some situations. Additionally,

not only would patrol officers benefit from this data, other civilian support staff such as dispatchers, jail and court staff, and analysts can be granted access by each agency. Without limiting access to traditional daytime office staff such as detectives, the speed and reach of access is also increased, which can be critical (Reynolds et al., 2006; Wertheim & Badgett, 2018).

With access to more information, patrol officers can make more confident enforcement decisions and use prior behavior as a factor in their decisions to pursue or not pursue further police action, whether punitive or protective. In addition to better performance, officers who have access to data stores are likely to reap other benefits. The educating of officers to hone their decision-making skills and a supervisory expectation of having an information sharing mindset would convince officers to gather potentially useful information beyond what is normally required, such as email addresses, work numbers and locations, and contact information for associates (Peterson & Miller, 2017).

Agrawal, Rao, and Sanders (2003), along with Sanders and Henderson (2013), noted that computer use and data availability led to increased officer satisfaction and exercised deterrence. This improved self-efficacy might also consist of a higher level of ownership in their work. In a regional Chicago area experiment where shared data access was rolled out to local departments, Skogan and Hartnett (2005) found that users reported that the system helped them identify offenders, improved their own skills, and that the staff seemed enthused to participate. A similar study added that participants believed their productivity was enhanced along with their ability to clear cases (Reynolds et al., 2006).

The difficulty of working together amongst intra-agency units is widely known, however in his study on inter-agency communication, Cotter (2017) observed an overreliance on ad-hoc, informal sharing networks. While detectives were often found communicating in groups via email or over list servs about casework, many of these occurrences were fishing attempts, whereby random queries were sent asking for information about suspects or certain criminal modus operandi. Self-searching an automated data exchange would mitigate the worry of whether a query truly deserved no responses due to lack of information or whether it simply went unseen by the others in the group. Detectives could instead have an instant response indicating other agencies held records that could further their investigation.

Whereas information is often sought by “old-fashioned” methods such as cold calling another agency, such a plan is littered with uncertainty. Contacting the right person or knowing where to call in the first place can be elusive. Personal communication or follow ups may still be required, and even preferred, but data sharing would provide an intermediary role and help solve personal communication barriers and ineffectiveness (Joyal, 2012).

Contributing data to central repositories provides many positive outcomes. The data contained therein is more suited to birds-eye and predictive views of criminality, not only to investigators. The furtherance of case content and work that could be accomplished by patrol would help patrol and investigations divisions work together, rather than competitively (Sizer, 2018). The access to and availability is of concern to command staff as well (Sanders & Henderson, 2013), as agency administrations have vested interests in their agency’s ability to identify, work, and clear cases.

COUNTER ARGUMENTS

Like many functions of government, there are also roadblocks to immediate implementation of data sharing services, both real and perceived. One major concern with any new concept is cost, specifically for smaller agencies (Hollywood & Winkelman, 2015). The FBI's N-DEx system has been live now for over ten years and is fully funded, advertising a no-fee initial account set up, no fees to access the system thereafter, and even offering data integration assistance for free to help agencies begin submitting their own case and records data ("National Data Exchange," 2016; Wertheim & Badgett, 2018). Even if a small investment of staff labor and some possible fees from the parent technology company were required, the benefits of contributing to and accessing the system would far outweigh a small monetary outlay (Plecas et al., 2011). Even still, small agencies are numerous and overwhelmingly outnumber their large counterparts and should contribute their data despite any budget or cost constraints (Carter, Carter, Chermak, & McGarrell, 2017).

Also of great concern to many agencies, managers, and individuals is that of data privacy. While there are a great many court cases and federal laws and guidelines for how *not* to release information to other parties, these legal issues are sometimes merely used as a cloak for a lack of policy guiding such releases. Federal guidelines outline who can access data and how to protect it, but not how it is shared, and the security procedures and guidelines by which agencies request access and then grant user access is strict (Hollywood & Winkelman, 2015). The often-cited Federal Privacy Act does not legally prevent the sharing of law enforcement information when it can be justified (Plecas et al., 2011).

Hollywood and Winkelman (2015) also noted that many entities have a hesitancy to relinquish control of data. This is a valid concern for case notes may include an ongoing investigation along with sensitive victim or suspect information. The N-DEx allows for user-configurable data restrictions using an easily understood green/yellow/red color-coding system (Prest, 2018), whereas “green” tagged data is viewable by all users, “yellow” by only authorized viewers, and “red” data only by the contributing agency. While this would create an extra step for agencies wishing to restrict access to submitted data, it does offer an agency-controlled solution. Agencies could also simply choose to submit data at longer time intervals to avoid continually uploading numerous incomplete cases.

Civil rights and public watchdog groups may raise concerns over public and private data being intermingled and misused. This is a valid concern, but police records being shared already exist in each individual agency’s data stores, loading them to a central repository simply speeds up the gathering of investigative leads (Reynolds et al., 2006). Moreover, privacy issues from the private sector or the medical field do not apply to public entities (Carter et al., 2017). Privacy and access rights concerns are valid worries, but overall, the repositories are controlled by strict policies and procedures well beyond that of financial institution and shopping websites used every day by millions.

An additional problem many agencies face is the lack of information technology (IT) staff or a limited-ability staff that do not have advanced networking skills (Hollywood & Winkelman, 2015). Fortunately, many technological barriers to effective data sharing have been remedied (Reynolds et al., 2006; “The Need to Share,” 2007). Currently,

most agencies use an electronic records management system (RMS) or computer-aided dispatch (CAD) in some form. Most of these function as a simple database program with a flashier user interface tailored to the needs of law enforcement. They generally consist of “off the shelf” programming and are already compatible. Officers can even continue to use their current reporting or narrative formats (Peterson & Miller, 2017), as the main computing task data sharing encompasses is simply text storage.

The most worrisome task for IT staff is the act of setting up the data sharing protocols and the requisite knowledge in doing so. Although the automated means of data submission would be the most convenient and least intrusive on the daily activities of the IT staff, the FBI offers several submission methods to suit the needs of any agency. An agency can set up one of two internet-based and direct upload methods using standardized protocols that can be adapted to current software, the creation of physical storage media to submit to N-DEx for entry (hard drive, DVD, CD, etc.), and lastly, a user can manually enter records through a web interface (“N-DEx Connections Overview,” 2016). While there is an inherent inconvenience that would occur having to manually enter numerous records, it does preclude an excuse of having no means of participation. However, given the rebuttals noted here, setting up the required network protocols for an automated process is not beyond the capability of even the most average of technology staffers.

RECOMMENDATION

It is estimated that 12% of the U.S. population will move each year (Sizer, 2018). This highlights the need for a higher-level view beyond jurisdictional borders. It is

imperative that agencies in Texas, and nationally for that matter, require the contribution of their criminal case data and police records to a central data warehouse.

Law enforcement has gone through a few technological epochs, but for the most part, has done those things individually, and with a self-serving and even arrogant attitude. The dangers of this became clear during the grim Reconstructionist years following the fall of the Twin Towers on 9/11. No longer could law enforcement agencies rely on any other single agency to solve problems or be responsible for any subset of national security or public safety.

The ability to instantly search through the criminal records and databases of other agencies, especially when the point of nationwide contribution is reached, would bring police work to a new technological era. Not only benefitting detectives, a subset of law enforcement who has historically enjoyed access to such information through both formal and informal sharing networks, patrol officers could also use information to help respond to and improve their decision making during real-time events. Officers who had access to such data also perceived their abilities to have improved and had higher enthusiasm for their job. They also took more ownership in their work product. If all divisions of the department add access to shared data and improved their work product, it stands to reason that they would also be working together more efficiently, while expectations for quality of work would also rise.

Some common trepidations that agencies express are that of costs, data privacy and access control concerns, and that of accessibility to knowledgeable IT staff. Cost, other than the time and labor involved in the planning and implementation of the technology, should always be a consideration of any public governmental agency.

Given that the FBI both absorbs the costs of running and maintaining the central data warehouse N-DEx and offers data integration assistance, along with allowing users to access the database for free, there is no deterrence to participation that is excessively monetary.

The sharing of pre-existing data of law enforcement organizations with other law enforcement organizations is not prohibited by law. Also, the FBI maintains a very secure online environment with restricted access procedures that is governed by both the FBI and the end user agency. Once granted access, the individual agency then decides who in its membership should have access. The data access concerns are addressed by leaving control with the submitting agency, who can use color-coded tags to restrict viewing by unauthorized persons.

The apprehension of having access to advanced or full-time IT staff is a valid concern. Many smaller or rural agencies have limited access to networking experts. By providing both automated and manual entry methods as options for data submission, the FBI has removed the excuse of inability to adapt to overly complex database technologies. Most RMS and CAD products currently being used by agencies are already compatible or are easily converted with typical IT skills.

In examining the benefits and arguments for requiring police agencies to contribute their records data to a data storage warehouse such as the FBI N-DEx, it becomes clear that it is as simple as deciding to do so. Political and organizational leaders must communicate a message of sharing throughout their region of influence and refrain from making policies confusing or complex (“The Need to Share,” 2007). Policymakers are conventionally a hard sell when it comes to budget and effectiveness

of new programs (Carter et al., 2017), but despite these political barriers there must be a message of unity. If local or county agencies will not mandate the sharing of information, then the state of Texas should do so. It is the only way forward in today's minefield of counterterrorism, mass attacks, and public safety in general.

REFERENCES

Agrawal, M., Rao, H.R., & Sanders, G.L. (2003, June). Impact of mobile computing terminals in police work. *Journal of Organizational Computing and Electronic Commerce*, *13*(2), 73-89.

Carter, J., Carter, D., Chermak, S., & McGarrell, E. (2017, March). Law enforcement fusion centers: Cultivating an information sharing environment while safeguarding privacy. *Journal of Police & Criminal Psycholog*y, *32*(1), 11–27.

Cotter, R. S. (2017). Police intelligence: Connecting-the-dots in a network society. *Policing & Society*, *27*(2), 173–187.

Current statistics. (n.d.). Retrieved from https://www.tcole.texas.gov/content/current-statistics

Hollywood, J. S., & Winkelman, Z. (2015). *Improving information-sharing across law enforcement - Why can't we know?* Retrieved from https://www.ncjrs.gov/pdffiles1/nij/grants/249187.pdf

Joyal, R. G. (2012). How far have we come? Information sharing, interagency collaboration, and trust within the law enforcement community. *Criminal Justice Studies*, *25*(4), 357–370.

National data exchange (N-DEx) connections overview. (2016). Retrieved from https://www.fbi.gov/file-repository/n-dex-connections-overview.pdf/view

National data exchange (N-DEx) system. (n.d.). Retrieved from https://www.fbi.gov/services/cjis/ndex

Peterson, K. A., & Miller, C. A. (2017, May). Why your department needs a law enforcement information sharing solution: “Prevent, Stop, Solve, and Share.” *Police Chief*, *84*(5), 18–19.

Plecas, D., McCormick, A.V., Levine, J., & Neal, P. (2011). Evidence-based solution to information sharing between law enforcement agencies. *Policing: An International Journal*, *34*(1), 120–134.

Prest, E.M. (2018, August 29). *Privacy impact assessment for the national data exchange (N-DEx) system*. Retrieved from https://www.fbi.gov/file-repository/pia-national-data-exchange-n-dex-system.pdf/view

Reynolds, K. M., Griset, P. L., & Scott Jr., E. (2006). Law enforcement information sharing: A Florida case study. *American Journal of Criminal Justice*, *31*(1), 1–18.

Sanders, C. B., & Henderson, S. (2013). Police ‘empires’ and information technologies: Uncovering material and organisational barriers to information sharing in Canadian police services. *Policing & Society*, *23*(2), 243–260.

Sizer, T. (2018, August). An amplified need for cross-jurisdictional data sharing. *Police Chief*, *85*(8), 94–96.

Skogan, W. G., & Hartnett, S. M. (2005). The diffusion of information technology in policing. *Police Practice & Research*, *6*(5), 401–418.

Texas data exchange. (n.d.). Retrieved from https://www.dps.texas.gov/administration/crime_records/pages/texasdataexchange.htm

The 9/11 commission report. (2004). Retrieved from http://govinfo.library.unt.edu/911/report/911Report.pdf

The need to share: The U.S. intelligence community and law enforcement. (2007, April). Retrieved from https://www.afcea.org/mission/intel/documents/SpringIntel07whitepaper_000.pdf

Tillyer, R. (2014). Opening the black box of officer decision-making: An examination of race, criminal history, and discretionary searches. *Justice Quarterly*, *31*(6), 961–985.

Wertheim, K. E., & Badgett, K. (2015, December). FBI -- The FBI's national data exchange (N-DEx). *FBI Law Enforcement Bulletin*, 24–29.