Addressing Emerging Trends to Support the Future of Criminal Justice

Findings of the Criminal Justice Technology Forecasting Group

Appendixes D, E, and F

John S. Hollywood, Dulani Woods, Andrew Lauland, Brian A. Jackson, Richard Silberglitt

For more information on this publication, visit www.rand.org/t/RR1987

Published by the RAND Corporation, Santa Monica, Calif.

APPENDIX D

The Criminal Justice Technology Forecasting Group's Discussions on Technological and Social Trends: Complete Notes and Mind Map

Discussion of Trends from CJTFG Meetings 1 Through 4

In this appendix, we describe the CJTFG's discussions of themes, their constituent trends, and potential responses, going clockwise from the top right of Figure D.1 (starting with trends in the *lack of business cases and processes* theme).

First, however, we start with discussing a central narrative that reaches across several thematic clusters, shown by the red lines in Figure D.1.

Opportunities in Information Technology Are Hampered by a Lack of Business Cases, Implementation Processes, and Security, Privacy, and Civil-Rights Knowledge

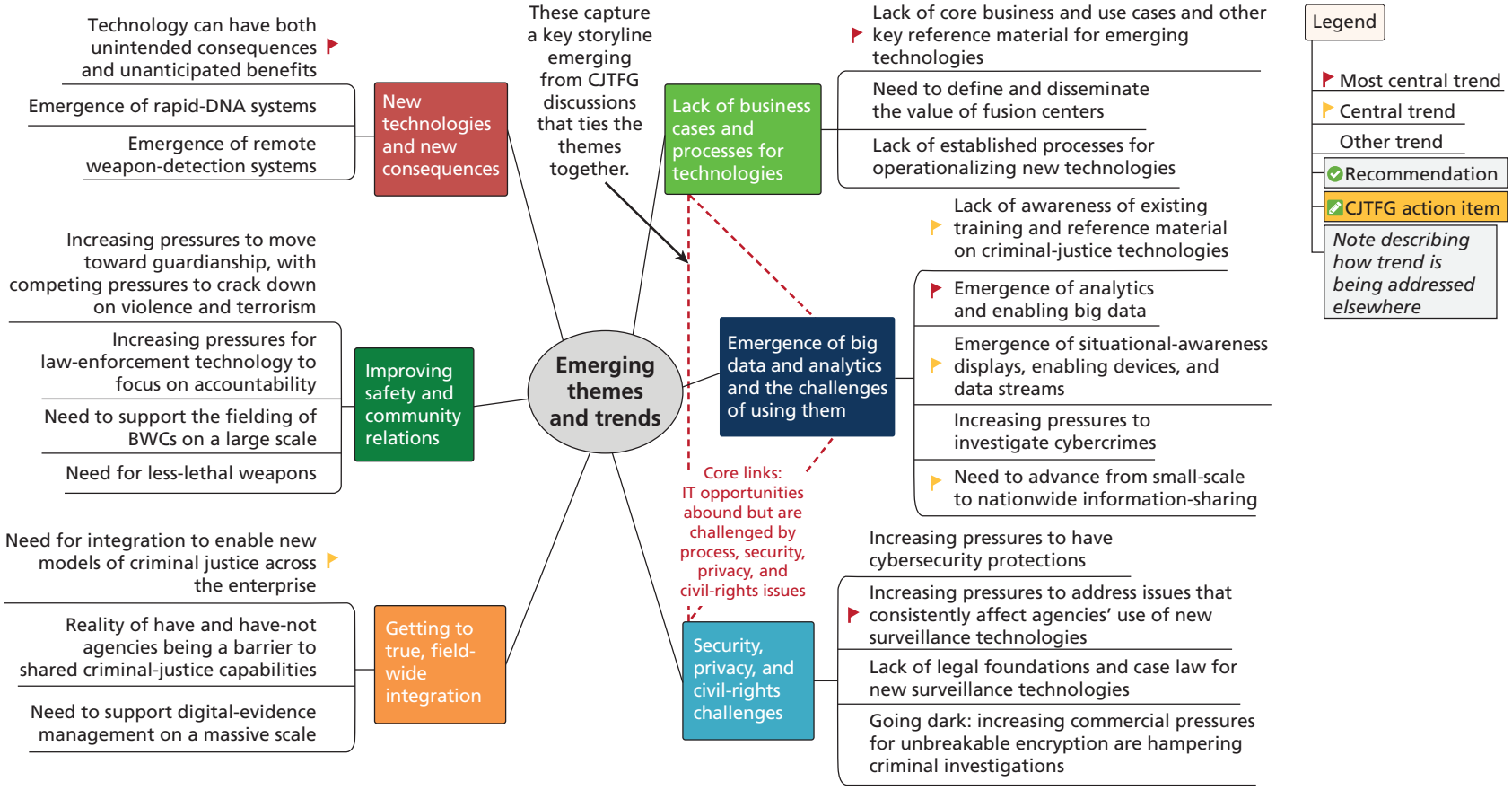
The emerging storyline from CJTFG discussions is that many of the largest technology opportunities and challenges today involve IT ranging from data collection (including surveillance systems, such as cameras and LPRs) to data management (including cloud installations) to analytics for processing all of those data to new tools and devices (e.g., smartphones, tablets, future virtual-reality goggles) for making that information available to personnel at all levels. However, exploiting these opportunities faces substantial challenges. The first can be summarized as a lack of knowledge about how to use and acquire the new technologies efficiently and effectively, as shown by the links to the general lack of core business cases and processes. The second is a lack of knowledge of the security, privacy, and civil-rights protections needed to employ this new IT safely.

This same narrative extends to other themes as well. Getting to true, field-wide systems integration is, in part, an IT challenge that faces significant process, security, privacy, and civil-rights challenges. Technologies for safety and community relations right now are focused heavily on BWCs and other technologies for accountability, which raise security, privacy, and civil-rights issues. Finally, new technologies include strong IT components (i.e., the information generated by touch DNA and weapon-detection sensors)—but new and unintended consequences are especially prevalent along security, privacy, and civil-rights lines as a result, especially for surveillance-related technologies.

A Lack of Business Cases and Business Processes for Technologies

Core business cases and use cases needed to inform criminal-justice technology investments are consistently lacking. Panelists noted that a perpetual problem is letting technology and unrealistic expectations about it drive technology adoption, rather than considering what practitioners really need. *Panelists asked whether one can develop mechanisms to help assess practitioners' true requirements for new technologies, starting with business-value propositions and*

Figure D.1
Emerging Themes and Constituent Trends from the Criminal Justice Technology Forecasting Group



NOTE: Colored rectangles are themes. Outlined items are trends. A red flag indicates a most central trend. A yellow flag indicates a second-tier (central but not most central) trend.

RAND *RR1987-D.1*

use cases. This idea was discussed most notably with regard to information-sharing but applied to other technologies as well. These cases need to identify the operational value for specified technologies. If possible, the cases should include what benefits agencies can expect to get in terms of law-enforcement outcomes, with references to the supporting evidence.

The cases need to be specific, providing checklists for agencies on what to get and how to use it in order to get the expected benefits. In developing the core business cases, stakeholders both inside and outside of agencies need to be involved to get their buy-in.

These core cases are a key necessary condition to deal with the increasing civil-rights, privacy, and other policy challenges to technologies, especially those that can be labeled *surveillance*. Challenges have been most acute when technologies have been fielded without a thorough understanding of how they will be used.

As one example of a place in which business cases are especially in demand, **the value of fusion centers needs to be defined and disseminated across the range of political and community stakeholders**. Although there are clear successes, privacy groups remain wary of fusion centers, and the public has become increasingly concerned; meanwhile, fusion-center advocates have often been accused as a group of failing to demonstrate their value consistently to funders in Congress and to local law enforcement (U.S. Senate, Committee on Homeland Security and Government Affairs, Permanent Subcommittee on Investigations, 2012, is perhaps the best-known example). Panelists noted that individual fusion centers need to become known for providing a specific product or service that has real operational value. Fusion centers need more-open functions to support stakeholder involvement and auditing. Examples include going beyond being reactive (outside of "wait mode") and training others on analyses. Panelists noted that, typically, not much funding has been available for using fusion-center staff time and expertise to train others despite a substantial need. As an example, during the East Coast rapist cases (Zapotosky, 2013), the panel discussed, many participating agencies did not have the necessary experience to work with crime data to recognize a crime cluster and identify suspects.

- *Is a fusion center a location that can consistently train people to access and use key data for crime and counterterrorism analysis, especially for agencies that cannot afford professional crime analysts?*

Another major value-add of real-time crime centers and fusion centers was described as being able to query lots of databases and combine the results into a useful product for the field quickly. As an example, panelists mentioned that, in Chicago, the major role of the city's fusion center is to support the immediate investigation by querying databases following shootings.

Established business processes for operationalizing new technologies are lacking. Successfully leveraging new technology is (at least) as much about changing business processes as it is about anything else. Although the group is nominally titled "technology forecasting," the group described a rich vein of governance, business-process reengineering, standardization, and silo-breaking that must be addressed. These findings are unsurprising. Regardless of the specific topic of discussion, traditional problems and concerns (such as governance, work flows, and improving or developing interagency relationships) routinely surfaced. There is an underlying layer of often very difficult issues that are either entrenched (e.g., lack of communication and trust between agencies) or are agnostic to the specific change in technology (e.g., institutional resistance to change).

Core business cases are an important necessary but far from sufficient component of larger operationalization processes. Panelists noted common challenges with technology implementation that are emerging, combined with requirements for dealing with them, including cost assessments, requirement management, governance mechanisms, and security, privacy, and civil-rights protections. Panelists asked whether *they could develop approaches to identify common requirements and best practices for implementing model emerging technologies.*

Emergence of Big Data and Analytics and Challenges Using Them

Awareness of existing training and reference material on criminal-justice technologies is lacking. The panel discussed numerous examples of many resources and trainings out there, including federally sponsored and association-sponsored material, but that are not widely known outside of a specific community. We also discussed that many resources are difficult to locate and understand, especially for newcomers to a specific technology. Examples specifically included information-sharing (with lack of awareness of how to share information being a barrier to nationwide information-sharing) and cybersecurity and cybercrime training and references. Panelists asked three questions:

- *Can we improve the marketing and dissemination of technology resources?*
- *Can we improve the organization and presentation of on-site materials?*
- *Can we improve the coordination across sites and resources?*

The emergence of analytics and big data offers substantial opportunities for criminal justice but also substantial barriers and risks to implementing them. It is worth noting that analytics and big data were the trend receiving the most discussion at the third CJTFG meeting. There is a range of potential applications, including predictive policing to identify locations, times, and people at increased risk of crime; risk-based bail, sentencing, and early-release decision support; and risk assessments to identify those on community supervision who are at higher (or lower) risk of reoffending. Panelists noted, for example, that a smart integration of technology, data, analytics, and good, community-based practices could provide a key example of what good policing looks like. Panelists also discussed the idea of integrating criminal-justice interventions with other, social-service interventions to generate holistic effects that would better protect communities and reduce individuals' risk. Examples included parenting improvement interventions, substance abuse treatment, and mental-health interventions. Panelists asked three questions:

- *What are the specific purposes (core business and use cases) for analytics needed for "good criminal-justice practice" that we want to put forward?*
- *What are the specific social interventions that should be integrated with criminal-justice activities to achieve the holistic effects?*
- *What are the best approaches and best practices for applications and corresponding interventions? Here,* best *is measured in terms of improving criminal-justice outcomes, community buy-in, and addressing privacy and civil-rights concerns.*

However, there is a great deal of variation in what is being done, with little consensus on what "good policing" driven by analytics and data is, much less what best practices are. (This is a specific example of the larger lack of core business cases for technology, discussed previously.)

Further, there are consistent concerns related to privacy, civil rights, and community buy-in when employing analytics and big data for criminal-justice applications. It does appear that preventive interventions on those labeled *high risk* are much more acceptable than punitive interventions, but much research needs to be done. Panelists asked four questions:

- *What are standards and approaches for ensuring that predictive policing and risk instruments do not contain biases, privacy violations, or security risks?*
- *What are the best approaches to involving the full range of stakeholders in design and oversight?*
- *How do we avoid slippery slopes of ever more surveillance data being used in analytics with less and less operational value?*
- *What are real use cases and mechanisms for using social media in ways that have both substantial operational and policy value?*

Panelists also noted substantial barriers to being able to use data and analytics for criminal-justice purposes. First, panelists noted a general lack of knowledge of crime analysis (an example of the general lack of technological knowledge, discussed earlier) and its value in general (both traditional and newer, computer-assisted forms) and cultural resistance toward computerized, quantitative decision support. Panelists noted that some very good explanatory papers and training sessions are out there (from the Vera Institute of Justice, Matthies and Chiu, 2014, and from some of the fusion centers), but dissemination to date has been limited. They noted Detroit, Michigan, and potentially Flint, Michigan, as examples of jurisdictions with agencies largely sold on crime analytics and its potential value. From a resource perspective, it currently requires substantial investments to set up and staff dedicated to analytics capabilities. Agencies also have to make substantial investments in the technology (tools and data management) and building up the necessary technical expertise. Panelists noted a perceived lack of analytics tools that are free (or very inexpensive) and easy to set up and use; they also noted that there are some legacy concerns about the security of open-source systems. Further, panelists noted that, even for agencies aware of free tools, training to use those tools and integrating them with existing systems are not. Getting and formatting the data needed are another major challenge, perhaps much larger than using the tools themselves. Panelists asked four questions:

- *Can we develop models to train and develop officers who can do part-time crime analysis, as opposed to traditional requirements for full-time, entirely technical analysts?*
- *Can we develop on-demand or outsourcing virtual models of crime analysis?*
- *Can we leverage new, open-source cloud and information integration tools, starting with basic crime mapping for both police and the public, to provide a simple-to-use environment (multi-standard and multijurisdiction) that can provide many of the key crime-analysis outputs very easily?* This capability might combine N-DEx (FBI, undated [a]), LInX (Northrop Grumman, undated), and COPLINK (IBM, undated), with major NIBRS incident reports being the major input. This approach has the compounding advantage of incentivizing agencies to adopt NIBRS reporting. The capability could be built as a mash-up of existing core open-source tools, including the statistical system R (R Foundation, undated), OpenStreetMap (OpenStreetMap, undated), and the high-level general programming language Python (Python Software Foundation, undated). On this topic, panelists asked whether, *as an alternative to a federal crime-analysis capability, they could fund development*

of common business and technical requirements for crime analysis, under the hypothesis that vendors would come forward to satisfy well-written requirements.

For agencies that do have analytics capabilities, panelists expressed concerns about duplication of effort, with agencies potentially having multiple analytics functions and analysts, each potentially with their own isolated data sets, and a larger lack of sharing and normalizing data. Here, panelists asked two questions:

- *Is it possible to use increasing political and public demands for data, as well as grant conditions, to drive vendor adaptation of National Information Exchange Model (NIEM), relevant Information Exchange Package Documentation, and so on?*
- *Can we ensure that NIEM includes crime-analysis standards?* It should be possible to reach out to the NIEM Justice domain, NIEM Business Architecture Committee, and IJIS Springboard, with the latter running compliance testing (IJIS Institute, undated).

The emergence of situational-awareness displays, along with enabling devices and data streams, similarly offers substantial opportunities for criminal justice but also substantial barriers and risks to implementing them. Indeed, panelists noted that predictive-policing vendors, for example, are increasingly selling situational-awareness systems that provide near-real-time monitoring and analysis of incoming incidents, with the "predictions" constituting just a single layer of the larger awareness displays. Panelists noted that the field is seeing novel form factors for display devices beyond smartphones and tablets, including improved display eyeglasses and improved voice-activated systems. Beyond the devices themselves is the software needed to do real-time monitoring and analysis of data that the devices are generating. Panelists also discussed leveraging new technologies to assist officers with filling out reports (autopopulating fields, for example), to save time and reduce error.

Panelists also noted that they expected agencies to heavily leverage upcoming commercial devices for officers in the field, much as they leverage commercial smartphones and tablets now. In addition to providing devices, panelists wondered, could commercial equipment mitigate certain interoperability and standard problems by default (note the need to migrate to nationwide data sharing below)? Certain communication and data standards would be used by default simply because most of industry uses them. On this, panelists asked three questions:

- *Leveraging improvements in voice-activated commercial devices, can we develop "Ask Siri" (iPhone) or "Ask Alexa" ("Amazon Echo," undated) for police officers?*
- *Can we develop automated or voice-directed reporting tools as well?*
- *Can future commercial equipment mitigate ongoing standard problems by default?*

Panelists also discussed displays and supporting data analysis for operations centers and command posts. They discussed two potential applications: real-time monitoring of the stress levels of voice communications (both into 911 call centers and over in-field networks) and real-time monitoring and control of video feeds. Panelists asked two questions about this:

- *Can analytics be used to do voice stress and attitude analytics beyond BWCs to 911 call centers?*
- *What would the command display for groups of BWCs and related sensors look like?*

For the former, the thought was that such real-time analytics could alert agencies to situations to which they most need to pay attention. For the latter, panelists asked whether such displays might look something like out of the movie *Aliens* (1986), which shows banks of camera feeds plus officers' health telemetry information. An alternative model would be the app Periscope (Periscope, undated), which shows mostly live video feeds on a map, with some additional indicators for the feeds at which one should look right now because they are actively broadcasting.

Panelists noted two major types of risks with situational-awareness feeds. The first had to do with human factors, including the physical burden of carrying too many devices and the cognitive burden of being overloaded with too much information. Here, panelists asked three questions:

- *Can these data and awareness displays be extended to decision agents that inform officers on how they should make tactical decisions?*
- *How do we avoid information overload and preserve physical space for pieces of equipment?*
- *How do we integrate officers' systems and software so that they need to carry only one device rather than many?*

The second had to do with the communication and IT resources needed to share, process, and integrate all the data being generated to populate situational-awareness devices. Panelists noted a lack of capabilities and resources to integrate all the different systems that might be used in the field. Panelists also asked how data coming off in-field devices could be integrated into court systems; court systems have their own specific data schemes. On this subject, panelists asked two questions:

- *The physical infrastructure to handle all of those data likely far outstrips existing wireless capabilities. Can we obtain the bandwidth and have it be affordable?*
- *How do we integrate device data with courts, given that new court systems have their own proprietary data?*

There are needs to advance from small-scale to nationwide information-sharing. Substantial progress on information-sharing has been made. As a recent example, panelists noted seeing increasing migration to regionalization, shared services, and cloud models for record-management systems, CAD systems, and other key data systems, which contribute to both interoperability (multiple agencies use the same services) and affordability. Here, panelists had one question: *What guidance should be provided for agencies on migration to regionalization, shared services, and cloud approaches for key IT?*

However, panelists expressed concerns about making only limited progress on information-sharing after decades of effort. They expressed concerns about repeatedly hearing the same problems with achieving information-sharing, including government, policy, cultural, and other barriers, along with the same generic solutions ("calls for better leadership"). They noted that there have been many pilots, experiments, summits, and so on, but there has only been limited progress outside of small-scale interagency sharing and a few nationwide systems and initiatives.

Panelists noted that it continues to be difficult to get people in the same room to share information because of a combination of inertia and unwillingness to share for a variety of

reasons. The lack of disseminated use cases describing the value of shared information and awareness of how to share are two contributing factors. As an example, discussion specifically on law-enforcement information-sharing noted that sharing among agencies remains a problem; sharing law-enforcement information outside the law-enforcement community is even more problematic. There is a need to demonstrate to law enforcement that the risk of sharing information is not as high as the law-enforcement community generally believes. It is clear that, in general, the law-enforcement community is reluctant to share with others, regardless of whether this attitude is acknowledged. This has an adversely limiting effect on the opportunity to appropriately and legally leverage data in ways that would ultimately return value to the originating agency. On this subject, panelists had two questions:

- *What can be done to change the culture to support the sharing of information needed for criminal-justice purposes?*
- *Can the culture and dialogue be changed to support presumptive data sharing (i.e., from needing to justify reasons to share data to one of needing to validate exceptions to the presumption (or replacing "need to know" with "right to know" as the default presumption)?*

Security, Privacy, and Civil-Rights Challenges from New Technologies

Pressure to have cybersecurity protections is increasing, and closely related is the fact that **pressure to conduct cybercrime investigations is increasing**. The CJTFG devoted substantial time to cybersecurity in its meetings. On the positive side, it was reported at the CJTFG meetings that there was

- more federal funding for the Multi-State Information Sharing and Analysis Center (see Center for Internet Security, undated)
- increased FBI support for states' cyber investigations
- the creation of a new NIEM cyber domain on cyberthreat and risk modeling (NIEM, undated)
- more progress on the Global Federated Identity and Privilege Management architecture (Justice Information Sharing, undated)
- the holding of a summit on identity, credential, and access management, which supports getting a single sign-on to secure systems, that led to a report recommending principles and actions to develop a future strategy for identity, credential, and access management (McEwen, 2015)
- the establishment of small-scale pilot efforts to help agencies improve their cybersecurity efforts
- the launch of the BJA-sponsored Law Enforcement Cyber Center, which provides numerous resources to help agencies build and enhance cyber prevention, investigation, prosecution, and response policies and protocols (Law Enforcement Cyber Center, undated [a]). The center's strategy is to provide basic information and strategies to chiefs, then have them reach out to county and vendor providers. There is also an increasing availability of training and reference material, in general. That said, dissemination of cybersecurity and cybercrime material is a major challenge. On this issue, panelists had two questions:
  - *What are ways to improve cybersecurity dissemination and training, both over the near term, for the IACP Cyber Center and related initiatives, and over the longer term?*
  - *Where are additional resources about which we need to know now?*

- a rise of promising cybertechnologies and practices, including shared-service and cloud security models, as well as offensive, counterhacking strategies. Panelists had two questions about this:
  - *Migration to hack-back or offensive attacks as best-practice defensive mitigations—what does that mean? How do we train on it?*
  - *What additional information needs to be provided on regionalization, shared services, and cloud security?*

On the negative side, panelists noted the following:

- In general, there is a need to frame the cybersecurity discussion and, likely, to break it into several different discussions more reflective of what is truly at issue. There appears to be broad agreement that cybersecurity is important but little actual agreement on what the term means or entails, other than that it covers a wide range of issues. CJTFG discussions, for example, ranged from security of new systems to defining cybercrimes to staffing and resources. The lack of focus in cyber discussions leads to limited progress. Panelists here asked whether they could *establish a finite set of lanes and frames to focus cyber discussions and subsequent efforts, including unanswered questions.*
- There is no unity of effort on cyber efforts. A 2014 flyer said to report cyberattacks to eight different places, for example, with those eight seen as far from a complete list. (That said, substantial effort in this area is in progress—notably, because of the core cyberthreat sharing portal being established by DHS as part of the Cybersecurity Information Sharing Act (CISA) (Public Law 114-113, 2015). The Law Enforcement Cyber Center's web page on incident reporting (Law Enforcement Cyber Center, undated [b]) now guides the respondent to report to one of five portals depending on whether the respondent is a law-enforcement agency, private organization, or individual, as well as urgency of need).
- As noted, many cyber efforts to date are pilot initiatives on a very small scale; others are useful only if an agency has computer security personnel.
- Developers often do not include sufficient security for their products; security has to be added on at a later stage by agency personnel or via third-party products.
- There is a lack of knowledgeable people on cyber in general, which is especially acute for criminal-justice agencies ("can't afford them, and when we do get some they tend to leave quickly" was one theme of discussion).
- Data on cyberattacks and crimes are lacking. Panelists noted that there could be billions in fraudulent social-service payments as a result of successful cyberattacks, but the lack of systematically collected, quality data means that we do not really know. There is no consistent nationwide tracking and reporting system for cyberattacks and crimes, not even having consistent definitions and metrics (how we compute damages in the event of a cyberattack), much less, for example, cyberincident codes in NIBRS (FBI, undated [b]). Different agencies collect small pieces of cyberdata at most. Panelists asked two questions:
  - *What needs to be done to provide such a system?*
  - *Will the new CISA portal, DHS's Automated Indicator Sharing (U.S. Computer Emergency Readiness Team [US-CERT], undated), fill this role, at least partially?*
- In general, there is a need to overcome both denial of the threat and a sense that nothing can be done. Panelists asked two questions:
  - *What are promising approaches for overcoming cultural barriers?*

  - *What are the compelling business and actual cases to get agencies to focus on cybersecurity?*
- About a different form of security, group members raised concerns that new wearable devices (e.g., smart watches) could kick off a new wave of robberies.
- Specifically on cybercrime, there is a lack of tools, procedures, and knowledge of existing resources to deal with this threat. Panelists identified three needs:
  - compelling business cases (including actual cases) to get agencies interested in cybercrimes
  - to provide and disseminate educational materials and training on how to investigate cybercrimes, for both law enforcement and prosecutors
  - more insight on how to build solicitations and funding opportunities, given existing resources (mostly technical) already out there.

Pressure is increasing to address issues that consistently affect agencies' use of emerging surveillance technologies. Discussions of new technology (such as BWCs) will probably ultimately be less about the technology than about the standard operating procedures, law, policy, ethics, and other rules that should surround it. The CJTFG's discussion in meeting 2 about recent experiences by jurisdictions that have implemented BWCs are likely in no way novel to BWCs or to any single jurisdiction. Inevitably, implementation of new technology—particularly technologies that allow access to information that might not have previously been available—will create a long tail of related policy, legal, and ethical issues that are potentially far more difficult to solve than the technology itself is to implement.

Thus, a family of related challenges to using technology is emerging, not just for BWCs but for any technology with a surveillance aspect. These currently include automated LPRs, cell site simulators, touch DNA systems, field DNA-collection systems, facial recognition, health telemetry sensors, vehicle telemetry tracking, persistent IoT sensors, and social-media monitoring and analytics used by criminal-justice agencies. This list likely is far from complete. Specific technologies identified right now as raising the most concerns include cell site simulators, LPRs, and BWCs. Panelists asked whether they could *characterize which technologies are likely to be widely disseminated, as well as which ones will substantially affect practice, thus triggering this family of related challenges.*

The common challenges involved with surveillance-technology implementation include demands for, and disputes over, specific use cases for the technologies, information-assurance policies (note the link to increasing pressures for cyber protections, discussed below), usage policies, and community and external expert participation and oversight. Panelists asked whether they could *identify common requirements and best practices for implementing surveillance technologies.* This includes asking what they can learn from current efforts, such as IACP's Technology Policy Framework efforts (IACP, 2014).

Note that these can be seen as special case subsets of the general need to improve and standardize requirements and other business processes for fielding new technologies, discussed previously.

Another, somewhat competing aspect of dealing with the emerging surveillance technologies relates to public expectations. Panelists noted that the public expects commercial and TV show levels of performance resulting from new technologies: "Why couldn't you see the criminal commit the shooting, track him, and verify his identity over the satellite? I saw it on TV!" Panelists asked whether any standard approaches exist *for dealing with unrealistic expecta-*

tions of new technologies. Describing service expectation data like one would see from Amazon was one possibility.

Finally, panelists discussed the 2015 Data and Civil Rights conference on criminal justice and policing in Washington, D.C., which brought together a large number of legal and political science experts, civil-rights experts, privacy-rights experts, and community development experts. They noted that the presentations and discussion made outstanding points that would be very useful in early-stage technology-usage considerations but that participants at that meeting typically did not attend criminal-justice technology workshops and conferences. Panelists asked how they could *bring outside privacy, civil-rights, and community development expertise into the CJTFG and other criminal-justice technology forums.*

Legal foundations and case law for emerging surveillance technologies are lacking. Supreme Court justices are on record stating that addressing emerging technologies will likely be the biggest legal challenge of the next few decades (Tolson, 2012). There is a great deal of new and unsettled law, reflecting the ongoing rapid changes to technology and society. Panelists suggested two questions that judges and legislatures will face:

- *Can video be used to better identify people, as opposed to or in addition to static mug shots and lineups? How would we account for implicit biases?*
- *How can courts address (the often naturally occurring) discrepancies between peoples' statements and testimony and video and other sensors?*

Panelists noted that there are some cases of agencies deliberately attempting to avoid BWCs and other monitoring technologies and dashboards so that they can avoid having to be accountable and take corrective actions. They asked how to *incentivize agencies to adopt key technologies to avoid having to take corrections.*

Panelists noted that what constitutes "gold standards" of evidentiary technology changes over time. With that comes changes in how both court officers and the public treat evidence that is consistent with older standards. Panelists asked what the impact of BWCs and other emerging technologies becoming gold standards would be, especially with respect to what status quo types of evidence would become unacceptable. With respect to proliferation of cameras in general, they asked how they address the refrain, "If it's not on video, how do we really know it happened?" They also asked whether *court officers and the public could be better educated as to what even older forms of evidence mean and how they should respond to those older forms of evidence.*

Given that BWCs are among the most preeminently discussed technologies of the past year, many discussions of technology issues were specific to cameras. Panelists discussed controversies over officer and citizen privacy, such as when a camera should be turned on, and how to deal with cameras not showing full scenes, such as lead-ups to uses of force, in court (and the court of public opinion).

The increasing commercial pressures that going dark puts on unbreakable encryption is hampering criminal investigations. This refers to the trending issue of agencies not being able to get data from electronic devices if those devices have strong encryption that source vendors cannot override. Recent Apple mobile operating systems, notably, incorporate strong encryption that Apple itself cannot decrypt (for example, "Our Approach to Privacy," undated). The rise of strong encryption is being driven in part by growing cybersecurity pressures, as well as social pressures against governmental surveillance. The lack of existing legal

foundations and case law on strong encryption is furthering court disputes about it. Analyzing data from devices has been a key mechanism of investigating violent crime and other organized-crime cases. There was substantial discussion on how much of a challenge this poses to criminal-justice agencies outside of anecdotal reports about specific investigations being hampered. Panelists asked two questions:

- *What are the hard data on the extent of this problem and its impact on criminal-justice outcomes, efficiencies, and cost–benefit calculations?*
- *Are there work-arounds, especially for scenarios in which strong encryption becomes ubiquitous?*

Getting to True, Community-Wide Integration

There are needs for information integration to enable new models of criminal justice across the enterprise. To maximize the potential from emerging technologies that provide more-rapid in-the-field access to information, law-enforcement agencies need to view themselves as one component of a connected criminal-justice enterprise and their role as one part of a larger criminal-justice cycle.

The principal example panelists mentioned was rapid sharing of law-enforcement contact, arrest, location tracking, and substance-testing information to support the "swift and certain sanctions" intervention model for corrections (National Network for Safe Communities at John Jay College, undated). In this model, those under community supervision receive rapid, near-certain, but limited penalties for violating supervision terms, a system that requires rapid recognition and sharing of information regarding term violations. However, that was just the beginning. Other information-sharing needs in support of new models of criminal justice include the following:

- *improving visibility on corrections:* Data on those under community supervision, as well as coming out of jails and prisons in general, are a major demand for information-led policing models. It is a current major information gap, with no guidance to date on probation and parole information-sharing. Despite the lack of guidance, panelists noted that community supervision data is the "most pinged" data in ARJIS (ARJIS, undated).
- *improving incident command:* There is a need for clear organizational structure, processes, and information dissemination to prevent overload of communication and personnel during major incidents. One key role of the LAPD's operations center is to provide for clear command and information dissemination during major incidents.
- *predictive analytics to support focused deterrence:* The Cambridge, Massachusetts, police discussed prioritizing the risk of hundreds of thousands of offenders to determine which ones should receive focused deterrence efforts.
- *improving entity resolution:* One large county noted that it had four to five people do nothing but verify identities for criminal-justice actions (e.g., warrants), an effort driven by the fact no identifiers go across the entire criminal-justice system. There were also calls for one state-level biometric identifier that could be shared across state lines where states permit it.
- *one kid, one record:* There is a desire to have a single, secure, high-quality juvenile record per person.

- *police-car telematics for training purposes:* The LAPD reported using in-car telematics to see who needs to improve their driving skills.
- *monitors to protect officers' health:* This could help, for example, detect early signs of a heart attack, which is a major cause of death for officers in the line of duty. Panelists did, however, point out a counterrisk, which is what defense attorneys might do with officers' health telemetry data. Participants also noted that unions would object to these devices if there were any way they could be used to discipline practitioners or otherwise used adversely against practitioners.

Looking across all of these specific needs, we see that the most critical emerging need is to *identify the highest-value use cases for information-sharing and other technologies.* This need takes the general lack of core business cases for technology to the next level of detail for information-sharing. Although there is widespread support for the general idea of improving information-sharing, there has been little in the way of focused discussion around specific models and processes that, if followed, would drive specific, positive, high-impact outcomes. Indeed, a statement to the group that information-sharing is an imperative was challenged with "it's an imperative only when it's worth it" and we "need the information to make the decision at hand and no more." These problems manifest to an even greater extent with the emerging surveillance technologies that can generate very large amounts of data; as noted, these technologies are consistently raising policy issues, have expenses that rise with the volumes of data being stored and shared, and could be viewed by privacy advocates and even the general public as overly invasive—for example, LPRs, fixed and mobile cameras, and facial recognition in said cameras.

We have found few academic studies to date matching information-sharing to changes in criminal-justice outcomes. The major exceptions are hot spots and focused deterrence or "hot-person" policing, which inherently require data to identify places, times, and people at elevated risk. In an uncommon example of data from a surveillance system, ARJIS reported that employing LPR data to find stolen cars has resulted in vehicle-recovery rates improving from 57 percent to 83 percent and mean recovery times falling dramatically.

From an operational perspective, panelists described seeing issues with designing and implementing information-sharing and coordinated processes to support these sorts of interventions. A short document describing key information needs and requirements for these interventions is an important first step to addressing these issues.

That said, in tension with the need to establish use cases and focus on operational information-sharing is still a need to be willing to share data without knowing that they will be valuable or how they will be used. It is critical that criminal-justice agency executives recognize that sharing information outside of their agencies—and potentially outside of law enforcement and traditional networks—has value and might have value even if the outcome is not immediately clear.

From a policy and business-process perspective, panelists noted widely varying issues on whether states and localities support needed information-sharing. For swift-and-certain-sanctions models, in about half the states, agencies can just go to a state repository for information on offenders. For others, agencies need to get permission from whoever runs local parole and probation, which can be courts in some areas. As example, in Charlotte–Mecklenburg, North Carolina, the governor recently granted law enforcement access to probation and parole information. Conversely, in Massachusetts, probation and parole have robust electronic

monitoring of those under community supervision, but law enforcement is specifically excluded from access to that information.

More broadly, there is growing recognition that there is a great deal of compelling non–law enforcement (or nontraditional law enforcement) data that have value to the law-enforcement community, but accessing and using them appropriately is another matter. Social-service data were roundly cited as promising. However, it appears that the more useful the information could be, the more difficult it is likely to be to share appropriately (e.g., mental illness, gun registration or purchase). It would seem unreasonable to simply walk away from the possible benefits of making these types of information available in a very limited and restricted manner; there should be space for improvement while maintaining needed safeguards. Panelists asked whether they could *determine model information-sharing needs and policies to be able to share key data across sectors, both within and outside of criminal justice.*

The reality of have and have-not agencies is a barrier to information-sharing and other capabilities across the criminal-justice environment. Budgets, manpower, procurement processes, and other resources vary dramatically throughout the criminal-justice enterprise. Although there are obvious resource differences between small and large police agencies, even among large criminal-justice agencies, there is a wide variation in funding and resources for technology, as well as capability to employ it effectively. Outside of differences within a region, panelists noted, there are differences between agencies in different parts of the criminal-justice system. For example, a police department might be able to afford a new information system, but court and corrections agencies for the same jurisdiction might not, creating an inherent interoperability problem. Court officers reporting difficulties managing the increasing volumes of BWC footage is a concrete example of this. These gaps need to be bridged for the overall effectiveness and efficiency of the criminal-justice enterprise. *Panelists noted a strong need to develop systems and business models that permit "have" agencies to share information and capabilities with have-not agencies in the same region*.

Digital-evidence management needs to be enabled on a massive scale. Much of the discussion here concerned BWC footage, but it applies much more broadly to the rapidly emerging family of surveillance-related technologies. There is a broad range of issues that need to be addressed. The first concerns formats, standards, and data conversion. Video and other standards need to work now and in 15 or more years.

Data redaction of bystanders is a major challenge for video footage. Panelists noted that, with existing technologies, redacting video (to remove faces of bystanders, notably) is a manually intensive process, with some CJTFG attendees reporting their agencies having to redact frame by frame. This was a major driver as to why state agencies in Washington State were having such a hard time responding to requests for video. That said, this is an area being actively researched and developed (Kanowitz, 2016, discusses recent developments).

Data retention poses a major challenge to agencies. Consistently storing most BWC footage imposes costly and heavy storage burdens. Further, the technologies and applications are too new to be able to predict future requirements. In the future, the burden will grow to include DNA collection from crime scenes and suspects.

There are highly labor-intensive demands for supervisors to review footage of their officers. Panelists noted that addressing this issue is an active area of federally funded research, with universities funded to develop algorithms to flag just those clips in which something "interesting" (an actual encounter that turns into a dispute or emergency of some type) happens.

Court integration challenges are a major concern. In addition to interoperability, there is high concern about prosecutors and courts not being able to process large volumes of video data. One potential solution discussed is to give court attorneys and judges secure log-ins to police video–storage systems so they can stream the specific videos they need to examine, which does require police departments to have video storage solutions that offer secure accounts that can be associated with access to specific videos.

The CJTFG also discussed the potential major role of federal assistance in helping agencies with the data-management challenge. Potential questions included the following:

- *Should CJIS maintain a federal resource for video footage?*
- *Should CJIS provide security standards and certifications for camera devices and cloud infrastructure?*

For the latter question, panelists noted that CJIS appears to be moving in that direction. Agencies (and probably CJIS) assume that CJIS is going ahead to apply CJIS policy to BWC footage, starting with video on Microsoft Azure and Amazon Web Services clouds.

Improving Safety and Community Relations

Pressure is increasing to move from "militarized" to "community-based" or "guardianship" models of law enforcement. However, there are also competing pressures to crack down on violence and terrorism—and these pressures can vary enormously from day to day. In the post-Ferguson and -Baltimore environments, demands to demilitarize and "be less violent" appear persistent. Similarly, demands to be more community-centric appear persistent.

At the same time, agencies are facing conflicting pressures to crack down on criminal violence, domestic terrorism threats, and organized-crime threats. Media, political, and community pressures on community relations, civil rights, accountability, and concerns about terrorism and violent crime will compete and vary, not just over time but day to day, and sometimes even simultaneously, in response to specific (and often isolated) events that get wide media and public attention. As examples, a single video of an apparently unjustified police shooting can affect perceptions of every police officer in the country, while a single mass shooting can drive widespread fears of entire groups of people. The proverbial swinging pendulum of the public's attitudes on criminal justice is being replaced by a proverbial pachinko machine. In response, panelists asked these two questions:

- *Can any technology help agencies address all of these competing demands simultaneously?*
- *Can any corresponding model of criminal-justice practice help agencies do the same?*

Pressure is increasing for law-enforcement technology in the near future to focus on accountability of all types. This pressure come in large part from the trend just discussed—emerging demands to move toward guardianship models of criminal justice. The panel noted that, for example, U.S. discussions of BWCs have been almost entirely about holding police accountable. In contrast, discussions of BWCs in the UK have been more about filming to gather evidence. The assumption is that BWCs and other accountability-monitoring technologies are not going away. Further, panelists noted there that would be legal, political, and civil consequences if these accountability technologies are not present or are mishandled.

Accountability of all types was a major theme of the CJTFG's discussions. These included discussions of privacy protections, ensuring appropriate use of data, documentation of citizen interactions, and improving performance management and officer accountability through data. Examples of the latter included BWC footage, driving telemetry data, and biometric feedback. However, "officer situational awareness" through enhanced availability of data is a two-way street: Although data can be used to increase officer accountability, they can also be used to answer the question "who is this citizen?" during interactions with the public, through improved data sharing, data overlays, accessing certain mental-health data, and so on.

BWC fielding needs to be enabled on a large scale. This topic was a major focus of the second CJTFG meeting, with a focus on the LAPD's recent BWC acquisition and associated policies. It is clear that there are substantial issues involving camera fielding, including cost, training, and multiple policy issues. However, it was also reported that early fielding results are implying that cameras are game changers, with major reductions reported in uses of force and in assaults on officers.

Digital-evidence management issues for growing volumes of BWC footage have already been discussed. In terms of other issues, a first note is that testing candidate camera systems is extremely important before purchase. The LAPD noted that it based its vendor selection primarily on human-factor considerations that officers reported when field-testing cameras from different vendors.

Privacy policies with BWCs are a major consideration to be resolved. The issue is complicated by the fact that applicable privacy laws vary substantially by state and put at tension desires to keep sensitive law-enforcement information private (especially filming of bystanders uninvolved with the situation) and desires to make law-enforcement operations transparent. The aforementioned lack of settled law and case law on surveillance-related technologies is a major driver here. The LAPD noted that officers are to record all situations in which they are engaged in an enforcement activity, which notably does not include people asking officers for directions. In terms of privacy protections for officers, the LAPD noted that its police union required its vendors to provide it, in writing, with assurances that video recording cannot be triggered remotely. California departments noted disputes with various groups of advocates and attorneys over getting access to footage and that, under California law, if video is made available outside of law enforcement to one person, it becomes public information. Conversely, under Washington state law, panelists noted, video is generally considered to be public, and state agencies have had difficulty handling all the requests.

Finally, panelists noted that the UK has taken a very different approach to using BWCs. Whereas U.S. usage has been driven by transparency and accountability concerns, UK usage has been driven by using cameras for evidence-gathering purposes. Panelists discussed whether U.S. agencies might learn from the UK experience. They asked whether *U.S. agencies could learn from UK experiences about how to best use BWCs to gather evidence, in addition to ensuring accountability?*

Agencies need to take better advantage of less-lethal weapons. There do appear to be cases in which lethal outcomes could have been avoided with less-lethal weapons. As a result, Chicago, as one example, has set a policy that there will be at least one conducted-energy weapon in each patrol car. A potential alternative to conducted energy is a "grenade launcher"–appearing device that fires 40-mm rubber balls. The device itself appears to have substantial deterrent effects. That said, a drawback is that muscle-memory issues might have led to officers accidentally firing guns when they really meant to use conducted-energy weapons.

It is important to capture that these weapons are less lethal, not nonlethal.[1] The public and policymakers need to be educated to that fact. Departments (such as that in Chicago) have held many presentations about it. Panelists asked whether they could *determine what needs to be done to better educate agencies, police, and the public about less-lethal weapons.*

In general, the implementation of new technology can have serious and unintended consequences but also major and unanticipated benefits. As the CJTFG noted at multiple points, technology, whether employed by practitioners or the public, can have a range of unintended consequences. Developments in technology commonly outpace associated developments in law, regulations, policy, culture, and, perhaps most importantly, baseline knowledge of how to use the new technologies effectively in operations. Examples range from overreliance on technology-eroding skills (will officers forget how to do basic functions if the technology does it for them?) to outside parties potentially manipulating human telemetry and other data in a misleading or unethical manner. Technology can generate a huge volume of new data before criminal-justice agencies have the opportunity to develop baselines or to truly understand them, which can overwhelm practitioners. As an example, panelists noted, investigators can now check so many databases and services to solve crimes that they need checklists and guidance just to navigate them. Other key examples include agencies' challenges with handling large quantities of digital-evidence data, especially BWC video, as well as handling data-related legal requests and challenges. Another example is the increasing amount of information that device displays can show, with the potential for overload and missing important information related to a need for immediate action. In general, it will be worth considering unanticipated consequences of the emerging technology trends, which include the rise of big data and analytics, situational-awareness displays, rapid and touch DNA systems, and remote weapon-detection systems.

Developing and understanding the key business cases for new technology (next item) are one part of addressing this challenge, which is to reduce the risk of improper implementation. That said, codifying "the major use cases" for emerging technology is in tension with a need to let operators develop novel ways to use technology; as described in more detail below, previously unanticipated uses of information can have major operational benefits.

Touch and rapid-DNA systems that might offer substantial capabilities to law enforcement are emerging, although there are barriers to overcome. Rapid-DNA systems can get DNA typing down to an hour. However, it is very expensive (panelists estimated costs of $250,000 for the equipment) and has substantial facility requirements.

Touch DNA systems can type DNA with very small samples, such as skin cells that an offender leaves behind after touching an object at a crime scene. This fact has substantial implications for identifying offenders (Minor, 2013). However, the technology is young, with key algorithms still under development.

Finally, the new technology of DNA phenotyping can create an image of what a subject looks like based on the subject's DNA (see, for example, Pollack, 2015). That said, this technology is very early in its development.

Panelists did not have any specific responses to this trend, treating it as one to watch. Panelists noted that, in addition to costs, DNA technologies will require large amounts of data handling to manage all of the typing data. Further, panelists noted that DNA technologies

[1] A conducted-energy weapon can, for example, induce a heart attack. These occurrences are rare but possible.

will raise substantial privacy issues and legal challenges—notably, on conditions under which a person's DNA can be sampled and which typing databases are subject to search and when. Again, this is a specific example of the broader emergence of a family of common policy issues around emerging surveillance technologies.

Technologies to detect firearms and other weapons remotely might be emerging. Panelists noted pilots to use millimeter-wave technology to detect weapons from stand-off distances, although they noted that examples to date appear to be van-sized devices with uncertain accuracies. (See Andrews et al., 2013, for a recent paper on what appears to be a smaller system.) Panelists also noted significant challenges and variations in state and local law in the conditions under which such a device might be used; this is another example of common policy issues around emerging surveillance technologies. Panelists asked two questions:

- *Can we assess when remote weapon-detection systems can be used—and used to derive stops and potential arrests—from a legal perspective?*
- *Can we assess the success rate, form factor or practicality, and cost of equipment for detecting weapons remotely?*

Mind Map from Criminal Justice Technology Forecasting Group Meeting 3

Figure D.2 shows the mind map (generated in XMind 7) that was built to capture the discussion during CJTFG meeting 3, held in February 2016. Given the size of the original full map, we provide it as a poster downloadable from the product page for this report.

APPENDIX E

Charters for Global/Criminal Justice Technology Forecasting Group Task Teams on Key Information Exchanges to External Service Providers

From the May 2016 Global Executive Steering Committee Meeting, Washington, D.C.:
Proposed New Task Teams
for the
Global Justice Information Sharing Initiative (Global)
Advisory Committee (GAC, Committee)

New activities that will benefit from the expertise of the Global Justice Information Sharing Initiative (Global) Advisory Committee (GAC) membership include the following. These efforts and opportunities fit nicely into Global's operational process of employing task teams to achieve "quick wins" and "value-adds" for the justice community. Additionally, given Global's agile task team approach, support for development of these solutions can be achieved in a very cost-effective manner.

Task 1: Identify Critical Nontraditional Information Exchanges Needed

Over a decade ago, SEARCH, The National Consortium for Justice Information and Statistics, published a reference model for exchanges that every jurisdiction should have and the types of data each of those exchanges should contain. That model was based on input from hundreds of justice organizations.

Global should support an effort to conduct a similar exercise, this time focusing on the many exchanges that the justice community now needs to accomplish with nontraditional organizations to appropriately carry out its mission. While this task has been partially addressed in the context of supporting efforts—including justice reinvestment, reentry, problem-solving courts (other innovative diversion programs), pretrial reform, and fines and fees reform—those exchanges and associated data have not been systematically documented. Potential Deliverable: A Global task team would identify and document core business requirements to address this capability gap in a valuable white paper/deliverable.

- Status: New task. Proposed at the Spring 2016 Global Executive Steering Committee (GESC) Strategic Planning Session, held May 18–19, 2016
- Time Frame: 3–4 months
- Anticipated Meeting Requirements: 1 in-person meeting, 4 conference calls/Webinars

Task 2: Generalize Information Sharing Technical Solutions in the Context of Cloud Requirements

The desire to leverage cloud capabilities for storage and other tasks is ubiquitous throughout the justice community. The Federal Bureau of Investigation has taken first steps toward describing business standards for justice use of the cloud in the context of the Bureau's Criminal Justice Information Services (CJIS) policy. If information sharing technology standards are "baked into" justice cloud standards for vendors such as Amazon and Microsoft Azure, then the Bureau of Justice Assistance (BJA) and Global would see broad adoption almost overnight. Potential Deliverable: A Global task team would outline this strategy in a short white paper/recommendation for execution by an appropriate agency.

- Status: New task. Proposed at the Spring 2016 Global Executive Steering Committee (GESC) Strategic Planning Session, held May 18–19, 2016
- Time Frame: 3–4 months
- Anticipated Meeting Requirements: 1 in-person meeting, 4 conference calls/Webinars

Note: Task Team 2 was designated to the FBI.

Task 3: Solve Specific Justice/Health Exchanges Using Consistent Architectural Approaches to Minimize Costs and Increase Interoperability

Supported by BJA, the IJIS Institute, Georgia Tech Research Institute, and the National Center for State Courts have begun identifying consistent, repeatable architectural strategies for information sharing between justice and health organizations. Currently, the U.S. Department of Justice laboriously negotiates technical solutions for priorities such as Prescription Drug Monitoring Programs exchanges as one-off solutions. This strategy will not scale across the range of exchanges needed with health care and human services. Potential Deliverable: A Global task team would identify and recommend high-value projects to build on this initial work by addressing technical solutions gaps for prioritized justice/health use cases.

- Status: New task. Proposed at the Spring 2016 Global Executive Steering Committee (GESC) Strategic Planning Session, held May 18–19, 2016
- Time Frame: 3–4 months
- Anticipated Meeting Requirements: 1 in-person meeting, 4 conference calls/Webinars

APPENDIX F

Resolution Requiring the Exportability of Core Criminal-Justice Record–System Data

The following was first proposed by Scott Came, executive director, SEARCH, to the Global Advisory Committee in May 2016 and endorsed by the CJTFG at its fourth meeting on November 4, 2016, and the Global Advisory Council on November 29, 2016.

Proposed Recommendation
for the
Global Justice Information Sharing Initiative (Global)
Advisory Committee (GAC, Committee)
Addressing Barriers to Justice Information Sharing: A New Strategy
A Proposed Global Advisory Committee Recommendation

Problem Statement

At the November 2015 Global Advisory Committee meeting, a breakout session examined the 2015 report by the RAND Corporation (and funded by the National Institute of Justice) entitled Improving Information Sharing Across Law Enforcement: Why Can't We Know? (http://www.rand.org/pubs/research_reports/RR645.html). Among other findings, this report pointed out that despite some visible and prominent efforts in specific jurisdictions, there has not been nationwide widespread adoption of justice community standards such as the Global Information Sharing Toolkit (GIST) and the National Information Exchange Model (NIEM). In the report, RAND provides several reasons (based upon interviews and its own analysis) for this phenomenon. RAND suggests that many vendors see it as a competitive disadvantage to enable open/standard interfaces to their customers' data, because system integration work generates a significant amount of revenue and profit for them; providing open interfaces puts that revenue/profit at risk. In addition, many proprietary systems' architectures remain tied to technologies that predate wider industry's adoption of the open standards on which the GIST and NIEM are based, which would make it costly for those systems' vendors to conform to the standards, thus harming their competitiveness.

For some time, the GAC has pursued a strategy grounded in the expectation that justice system vendors would build support for the GIST and NIEM into their products, which would in turn result in conformant information exchanges as justice agencies purchased and implemented these products. After nearly a decade and with the findings of the RAND report, it is time to rethink this strategy. Industry has suggested that vendors will build standards-based exchanges into their products when doing so becomes a common (ideally, universal) requirement in requests for proposals (RFPs) issued by their government customers. However,

this argument rests on premises that have proved to be false in practice. Government agencies often believe—justifiably, in many cases—that procuring a system with standards-based exchanges built in will cost significantly more (due to the business model and architectural factors mentioned above). Given limited resources for procuring such systems and the understandable buyer's prioritization of core functionality over standards conformance, the result is often the "softening" of standards conformance requirements, either by making them optional in the RFP or by removing them in the final contract with the vendor.

At the meeting in November, neither the breakout session participants nor the full GAC took formal action in response to the report, despite a robust discussion of its findings. The recommendation below is for the GAC to take such action, with the long-term goal of increasing adoption of the GIST, NIEM, and justice community standards more broadly.

Recommended Solution

Rather than encouraging justice agencies to require standards-conformant exchanges in their RFPs and to be firm in awarding contracts only to vendors that fully implement those requirements despite the likely higher costs involved, it would be better for everyone—practitioners, industry, and the community collectively—to seek ways to lower those costs so that the desired outcome happens naturally through market forces.

The first step in finding a solution is to identify two groups of vendors in the justice systems market:

1. Vendors who view the data, collected and managed through the use of their software, to be wholly owned by their customer and who understand that along with this ownership comes the right to access the data, at no additional cost, for whatever purpose the customer wishes, and a resulting obligation on the vendor's part to be transparent as to how data are structured and accessed in the system.
2. Vendors who view the data, collected and managed through the use of their software, or the structure/design of the data as the vendor's intellectual property and who prohibit customers (through software licensing or contract language) from accessing it except through custom vendor-provided interfaces.

Note that the vendors in each segment may or may not have technical or architectural difficulties in providing standards-conformant interfaces, and these difficulties would still understandably drive up the costs of implementing such interfaces. But it is important to distinguish these groups, because strategies for overcoming barriers to information sharing should be different for each group, as seen below.

The second step to a solution is recognizing that there is a robust, largely commoditized market in interfacing technology that can provide low-cost, standards-conformant interfaces to practically any information source. This technology is available from a wide variety of software vendors and is also available in open source form. Typically, this technology relies on basic information technology industry techniques—such as structured query language (SQL) and Representational State Transfer (REST)—that are within the capabilities of most enterprise information technology departments and consultants. Because of the commoditization of

the interface technology itself and the wide array of options for obtaining developers to work with it, the costs of employing it tend to be very low.

Putting these two steps together, a recommended solution emerges. For vendors in the first segment, for whom the high costs of standards conformance are due solely to architectural or technical difficulties, all a solution requires is for them to be transparent about the structure and meaning of the data stored in their systems—but importantly, it does not require that they expose those data in any particular manner (standards-conformant or not). As long as the data are exposed in a well-defined way, using one of the dozens (if not hundreds) of methods accessible to commodity interface technology, customers will have a variety of low-cost options for implementing standards-conformant exchanges of the data. It is possible—even likely—that new business models will emerge, with vendor companies seeking competitive advantage by forming partnerships and evolving new architectures that optimize the union of their legacy technologies with various interfacing approaches. Importantly, vendors in this segment can go on doing what they do best—making products with core agency records management functionality that their customers want—while preserving their existing architecture and staff skill sets.

By definition, agencies that purchase systems from vendors in the second market segment will continue to experience difficulty (if not outright impossibility) in exchanging information in an open, standards-based way with their partners. Because these difficulties are due to licensing or contractual language, the only solution is to prohibit such language via the agencies' procurement process. Because of competitive pressure from the large number of vendors (presumably) in the first segment, the hope is that vendors in the second segment will adjust their business model to provide customers with access to their data.

The viability of this solution rests on an assumption that the first market segment is robust, with multiple vendors competing for agencies' business. Anecdotal evidence from BJA-funded technical assistance efforts and grant-funded information exchange projects demonstrates that prominent system vendors do indeed enable extraction of data from their systems, though most often not in a standards-based way. The release of open data sets through the Policing Data Initiative offers further evidence that agencies of all types have had success in extracting data from their computer-aided dispatch (CAD) and records management systems. In fact, anecdotal evidence indicates that the first market segment encompasses far more vendors than the second, though anecdotal evidence also indicates that the second segment is not empty.

Global Advisory Committee Action

As a first step in working towards this solution, the Global Advisory Committee should consider making the following recommendations to the U.S. Attorney General, in its role as a Federal Advisory Committee to her office:

The Global Advisory Committee acknowledges the findings, recently published by the National Institute of Justice and the RAND Corporation, that specific technology barriers are impairing the ability of justice agencies in sharing information.

The Global Advisory Committee recognizes, as a matter of principle, that data collected by justice agencies in the course of managing their operations belongs to those agencies and as such should be freely available for those agencies to use. Consistent with this data ownership

is an assumed right to have a means of accessing the data and documentation of the structure and meaning of the data, unencumbered by licensing or contract language that prohibits such access and the availability of such documentation.

Accordingly, the Committee, as a Federal Advisory Committee to the Attorney General of the United States, recommends:

1. That the Attorney General of the United States encourage vendors of information systems sold to justice agencies to:
   a. Make available to any customer using their product(s) a means of accessing the customer's data maintained in the software. This can consist of querying the application database, accessing an application programming interface (API), accessing a Web service, or other automated mechanism.
   b. Make such means of data access available to all customers of their product, as a standard feature of the product, without requiring a separate purchase.
   c. Publish publicly on the Internet:
      - Either: Documentation sufficient to enable customers to use the means of data access, including a list of all data objects/elements made available, a definition of each object/element, and technical protocols necessary to enable the access;
      - Or: An assertion (evidence) of the product's conformance with relevant specifications (e.g., service specification packages or information exchange package documentation), which may include a trustmark issued by an appropriate trustmark provider or a certificate issued by the IJIS Springboard initiative.
2. That the Attorney General of the United States designate an entity, such as the IJIS Institute, to maintain an online list of vendors that comply with the requests in (1) above, with appropriate link(s) to the documentation and/or assertions relevant to each vendor.
3. That the Attorney General of the United States, through the Office of Justice Programs (OJP), include special conditions in grants issued by OJP to require that any vendors being paid out of grant funds for purchase or upgrade of any justice information system appear on the list called for in (2) above.
4. That the Attorney General of the United States encourage practitioner associations represented on the Global Advisory Committee to raise the awareness of their membership as to the existence of the list of compliant vendors and encourage their members to purchase systems only from vendors on the list.
5. That the Attorney General of the United States, through the Office of Justice Programs, produce guidance, in the form of model request for proposal (RFP) language or equivalent documentation, that assists justice agencies in purchasing systems from vendors that conform to the requests in (1) above.
6. That the Attorney General of the United States, through the Office of Justice Programs (OJP), include in OJP's technical assistance services (such as those of the National Training and Technical Assistance Center) assistance with implementation of this recommendation.