Emerging Technology Trends and Their Impact on Criminal Justice

Anyone who uses a credit card and has recently been notified of a possible hack to his or her private information knows that technology is a blessing until it falls into the wrong hands and becomes a curse. The Bureau of Justice Assistance, an office of the U.S. Department of Justice, formed an expert advisory panel to assess the impacts that technology and related emerging social trends could have on criminal justice and to identify appropriate responses.

The RAND Justice Policy Program teamed with the panel, called the Criminal Justice Technology Forecasting Group (CJTFG), to (1) identify major, emerging social and technology trends likely in the next three to five years; (2) assess the impacts, both threats and opportunities, that these trends could have on criminal justice; and (3) identify promising responses to the trends, including recommendations that advise agencies on how to use key technologies more effectively, advise creators and funders on making technologies more useful and less risky to implement, and directly support the criminal justice field.

Through a series of workshops held from 2014 through 2016, the team identified nearly two dozen trends that coalesced around six themes. A new report, summarized here, discusses these themes and the recommendations that the team generated. The table on page 3 shows the trends and recommended action plans (“ways ahead”). The single biggest takeaway from the experts: Information technology (IT) opportunities (such as big data, analytics and artificial intelligence, and the Internet of Things) abound, but taking advantage of those opportunities is thwarted by the lack of clear business cases for them; a lack of business processes for implementing them; and a lack of knowledge of common security, privacy, and civil-rights protections to prevent their misuse.

A Lack of Business Cases and Processes Hampers Agencies’ Use of New Information Technologies

The experts emphasized that the lack of clear business cases and the lack of implementation business processes impede investing in and taking advantage of emerging information technologies. They also cited the importance of identifying stakeholders’ needs and getting their buy-in when developing business cases and implementing new technologies. One example of the need for business cases was a call to better establish the vital role of fusion centers in providing useful information, products, and services for law enforcement. As an example of how to develop business cases, the Global Justice Information Sharing Initiative has developed

Key findings:

- The criminal-justice arena faces an abundance of information technology opportunities. However, important barriers, including a lack of business cases; a lack of implementation plans and procedures; and a lack of security, privacy, and civil-rights protections, hinder its ability to take advantage of those opportunities.
- Agencies need to develop business cases and common processes for implementing new technologies.
- Research is needed to improve sharing of criminal-justice technology among practitioners and researchers.
- To prevent misuse of new technologies, security, privacy, and civil-rights protections need to be incorporated into common processes for implementing those technologies.
- Materials need to be developed to educate the public about emerging criminal-justice technologies.
- Research is needed on changing organizational cultures to better support field-wide information-sharing and safeguarding.
- The technologies and practices with the most potential for improving both public safety and community relations need to be identified.
- Unintended consequences of new technologies must be assessed.
information exchanges between agencies that service offenders and the rest of the criminal justice system.

**RECOMMENDATION 1:** Develop business cases for key technologies and common process templates for implementing new technologies.

**Big Data and Analytics Provide Opportunities and Challenges**

Data and analytics are already playing a role in predictive policing (pinpointing people, places, and times at increased risk for crimes), as well as in risk-based bail setting and sentencing. Yet potential users lack awareness of existing training opportunities, references, and other resources on cybersecurity. The experts called for research into expanding the availability of training and reference materials and improving information-sharing and for pilot projects that would integrate data, analytics, and IT into community-based practices.

One priority is the pressing need for improved situational-awareness displays to identify, communicate, and respond quickly to threats; the technology for providing these displays is rapidly emerging, so improving them is a matter of leveraging that technology. Another priority is for the federal government to support crime-analysis capabilities for state and local agencies; the CJTFG developed a white paper on how such support might work (an appendix to the report).

**RECOMMENDATION 2:** Conduct research to improve how criminal justice technology information is made available to both practitioners and researchers.

**Ensuring Security and Privacy and Protecting Civil Rights Present Additional Challenges**

Despite increasing pressure to employ cybersecurity and protect the public’s privacy and civil rights when using the new big data, analytics, and surveillance technologies, guidelines remain inconsistent, legal precedent is often lacking (resulting in security and privacy concerns), and the public’s expectations, shaped by television shows and advertising, often fail to be met. On top of those issues is the fact that greater encryption of electronic devices is increasingly hampering law enforcement agencies from obtaining needed evidence (“going dark”).

**RECOMMENDATION 3:** Integrate security, privacy, and civil-rights protections into the common business process (from Recommendation 1) for adapting new technologies.

**RECOMMENDATION 4:** Educate the public on how criminal justice technologies work (or do not work) in the real world.

**RECOMMENDATION 5:** Collect data on the extent and severity of the going-dark problem.

**Getting to True Community-Wide Integration of Justice**

To realize the true benefits of emerging technologies, agencies must integrate information on a national scale, and managing growing floods of digital evidence is a key part of this imperative and a rapidly emerging trend. However, small, resource-poor agencies lack the needed capabilities. Organizational cultures can resist information-sharing. Further, some brands of record-management and other IT systems that criminal justice systems use frequently do not support data interoperability and sometimes even exclude information-sharing in their licensing provisions; the CJTFG cosponsored a resolution to require making record-management system data exportable for sharing with other systems.

**RECOMMENDATION 6:** Research changing cultures to support information-sharing and safeguarding.

**RECOMMENDATION 7:** Develop regional models for information-sharing capabilities.

**Improving Safety and Community Relations**

Agencies face conflicting pressures to minimize use of force while cracking down on violence and terrorism. Missteps can quickly affect police–community relations and alienate groups of people from each other. Body-worn cameras are a promising tool for accountability of both police and the public; the experts suggested examining their use for investigative purposes as well. CJTFG experts also expressed a strong need for less-lethal weapons capable of subduing and restraining violent attackers, in order to provide alternatives to lethal force or grappling.1

**RECOMMENDATION 8:** Identify practices and technologies that can both reduce crime and improve community relations.

**RECOMMENDATION 9:** Explore international exchanges on using cameras for investigative and accountability purposes.

**RECOMMENDATION 10:** Develop new immobilization and restraint devices to provide alternatives to lethal uses of force.

**New Technologies and New Challenges**

Implementing new technologies can have both unintended consequences and major, sometimes unanticipated, benefits. Technological developments often outpace associated devel-

---

1 Less-lethal has a specific meaning in law enforcement and refers to the fact that the use of less-lethal weapons, such as conducted-energy weapons (tasers), can sometimes result in death.
opments in law, regulations, policy, culture, and knowledge regarding effective use. In addition, many of the technologies are young, and costs might remain prohibitive. In the business cases (recommendation 1), including the need for security, privacy, and civil-rights protections (recommendation 3) can help protect against unintended drawbacks, although care must be taken to avoid stifling the emergence of unanticipated benefits.

Two emerging technologies appear worth following. The first is rapid deoxyribonucleic acid (DNA) typing coupled with use of DNA to create profiles, and the second is technologies to detect guns, knives, and other weapons at a distance.

Themes, Trends, and Ways Ahead

<table>
<thead>
<tr>
<th>Theme</th>
<th>Trend</th>
<th>Way Ahead</th>
</tr>
</thead>
</table>
| Lack of business cases and processes for new technologies* | • Lack of core business cases and other key reference material for new technologies  
• Need to define and disseminate the value of fusion centers  
• Lack of established business processes for operationalizing new technologies                                                          | • Develop business cases for key technologies.  
• The CJTFG cosponsored a resolution specifying data exchanges to providers of services to offenders.  
• Develop common business processes for operationalizing key technologies.                                                             |
| Emergence of big data, analytics, and challenges of using them* | • Lack of awareness of existing training and reference material on criminal justice technologies  
• Emergence of analytics and enabling big data  
• Emergence of situational-awareness displays, enabling devices, and data streams  
• Increasing pressures to investigate cybercrime  
• Need to advance from small-scale information-sharing to nationwide information-sharing                                          | • Conduct research and experimentation on improving how technology resource materials are made available to both practitioners and researchers.  
• Through site visits and interviews, learn from agencies how they are using emerging data technologies.  
• The CJTFG recommended that the Bureau of Justice Assistance directly sponsor a learning tour.  
• Develop a federally sponsored crime-analysis capability.  
• The CJTFG authored a white paper on this topic.                                                                                   |
| Security, privacy, and civil-rights challenges* | • Increasing pressure to have cybersecurity protections  
• Increasing pressure to address issues that consistently affect agencies’ use of new surveillance technologies  
• Lack of legal foundations and case law for new surveillance technologies  
• Going dark: unbreakable commercial encryption hampering criminal investigations                                             | • Incorporate security, privacy, and civil-rights protections throughout the previously recommended common business processes.  
• Develop materials to educate the public on how criminal justice technologies work (or do not work) in the real world.  
• Collect hard data on the extent of the going-dark problem and investigate work-arounds.                                                |
| Getting to true field-wide information integration | • Need for integration to enable new models of criminal justice across the enterprise  
• Reality of “have and have-not” agencies being a barrier to shared criminal-justice capabilities  
• Need to support to digital evidence management on a massive scale                                                                      | • Research methods to change cultures to support information-sharing and safeguarding.  
• Require the exportability of core criminal-justice record-system data.  
• The CJTFG cosponsored a resolution on this topic.  
• Develop regional models for information-sharing capabilities.                                                                             |
| Improving safety and community relations | • Increasing pressure to move toward guardianship, with competing pressure to crack down on violence and terrorism  
• Increasing pressure for law enforcement to focus on accountability  
• Need to support fielding of body-worn cameras on a large scale  
• Need for less-lethal weapons to reduce the number of lethal use-of-force incidents                                                      | • Identify combinations of practices and technologies that offer the greatest potential in reducing crime and improving community relations.  
• Facilitate exchanges between the United States and the United Kingdom on lessons learned on using cameras for both investigative and accountability purposes.  
• Develop new immobilization and restraint technologies.                                                                                 |
| New technologies and new consequences | • Possibility of both unintended consequences and unanticipated benefits  
• Emergence of touch and rapid-DNA systemsb  
• Emergence of remote weapon-detection capabilities                                                                 | • Have the core business cases and processes include risk-assessment elements to mitigate unanticipated consequences.  
• Assess the potential of remote weapon-detection capabilities.                                                                       |

* This theme is part of an overall narrative that IT opportunities are being hampered by business process obstacles and challenges in ensuring security and civil liberties.

b 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.

RECOMMENDATION 11: Assess the potential of remote weapon-detection capabilities.

Moving Forward

Going forward, the initial priorities are to establish the business cases for the new technologies; develop the work processes needed to implement them; and integrate them with the core security, privacy, and civil-rights protections needed for successful implementation. Better ways of informing and educating practitioners and technologists will then help get the word out about why and how to use the new technologies.
Criminal Justice Technology Forecasting Group Members

- Peggy Bell, Executive Director, Delaware Criminal Justice Information System
- Jean Bousquet, Director and Chief Information Officer, Wisconsin State Courts Office
- Ronald Brothers, Chief Information Officer, Information Technology and Communications Division, Maryland Department of Transportation
- Scott Came, Executive Director, SEARCH Group
- Thomas Clarke, Vice President, Research and Technology Services, National Center for State Courts
- Mitch Cunningham, Deputy Chief, Investigative Bureau, Wilmington (N.C.) Police Department
- Phillip Goff, President, Center for Policing Equity, John Jay College of Criminal Justice
- Maggie Goodrich, Chief Information Officer, Los Angeles Police Department
- John Hollywood, Ph.D., Director, Information and Geospatial Technologies Center of Excellence, National Law Enforcement and Corrections Technology Center
- Jonathan Lewin, Commander and Managing Deputy Director, Chicago Office of Emergency Management and Communications, Chicago Police Department
- Cherie Lingelbach, Policy and Implementation Manager, juvenile justice information system, Oregon Youth Authority
- Mike Overton, Chief, Information Services Division, Nebraska Crime Commission
- Jerry Ratcliffe, Ph.D., Director, Center for Security and Crime Science, Department of Criminal Justice, Temple University
- David Roberts, Senior Program Manager, programs, International Association of Chiefs of Police
- Anne Roest, Commissioner, New York City Department of Information Technology and Telecommunications
- Cynthia Rudin, Associate Professor, Sloan School of Management, Massachusetts Institute of Technology
- Pam Scanlon, Executive Director, Automated Regional Justice Information System
- Teresa Takai, Chief Information Officer, U.S. Department of Defense
- Sean Thakkar, Executive Director, Connecticut Criminal Justice Information System Governing Board
- Joseph Wassel, U.S. Department of Defense
- Harlan Yu, Principal, Upturn.

NOTE: These are the positions the members held when they served on the CJTFG.