PRIORITY
Criminal Justice
NEEDS INITIATIVE
A project of the RAND Corporation, the Police Executive Research Forum, RTI International, and the University of Denver

Using Future Internet Technologies to Strengthen Criminal Justice

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

Key findings

- Panelists saw the need to leverage web technologies to improve information-sharing and protection across the criminal justice enterprise.
- In addition to leveraging web technologies for information-sharing in general, top priorities included developing a common criminal history record and cataloging scheme, developing real-time language translation capabilities, and developing displays or "dashboards" to meet officers' tailored, dynamic information needs.
- Priorities included general education on key web technologies, and model policies and procedures for using them.
- Panelists called for procurement checklists and cost-benefit tools for systems acquisition, and for policies and procedures to address the anticipated rise of unmanned vehicles.
- Panelists agreed that the networking infrastructure needs improvement to support web technologies (and other applications), especially for courts and corrections.
- Several needs were expressed related to leveraging wearable and embedded sensors (part of the Internet of Things), with an emphasis on using sensors to improve officer health and safety.
- Panelists frequently noted the importance of civil rights, privacy rights, and cybersecurity protections.

SUMMARY Web technologies just over the horizon, including semantic tagging, intelligent agents, and the Internet of Things (IoT), could dramatically change how the criminal justice enterprise operates. In September 2014, the RAND Corporation convened an expert panel for the National Institute of Justice to discuss how the criminal justice community can take advantage of (and reduce the risks from) these emerging web technologies.

The panel assembled 16 experts on both web technologies and criminal justice, and collectively identified 45 technology needs. After the conference, the panelists assessed the expected value derived from each need by rating each need's potential importance to criminal justice (law enforcement, courts, or corrections), the technical feasibility of meeting the need, and the operational feasibility of meeting the need. Top needs from the workshop are displayed in sidebars. Major themes that cut across groups of needs are described below.

Improving Information Sharing

The top theme from the panel was to leverage web technologies to improve information sharing and protection across the criminal justice enterprise. In addition to leveraging web technologies for information-sharing in general, top priorities included developing a common criminal history record and cataloging scheme, developing real-time language translation capabilities, and developing displays or "dashboards" to meet officers' tailored, dynamic information needs.

Educating Practitioners

Another major theme was improving practitioners' knowledge of web technologies. Priorities included general education on key web technologies, and model policies and procedures for using them. Panelists also called for procurement checklists and cost-benefit tools for systems acquisition, and policies and for procedures to address the anticipated rise of unmanned vehicles.

Top Five Needs Overall

- Video links to correctional facilities, so inmates can meet with community corrections officers and others prior to release
- Educational materials on key web technologies (sensors, video conferencing, tele-education, data translation)
- Real-time language interpretation
- Virtual criminal record catalog
- Technological infrastructure for criminal justice interfaces

Improving Infrastructure

A third theme was to improve the networking infrastructure needed to support web technologies (and other applications), especially for courts and corrections.

Exploring the Use of Emerging Internet of Things (IoT) Sensors in Criminal Justice

Several needs were expressed related to leveraging wearable and embedded sensors (part of the IoT), with an emphasis on using sensors to improve officer health and safety.

Civil Rights, Privacy Rights and Cybersecurity Concerns

Panelists frequently noted the importance of civil rights, privacy rights, and cybersecurity protections. While there were few needs about these topics specifically, panelists noted that more than half of the needs either raised security, privacy, or civil rights concerns or had implied requirements on these topics.

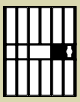
Top 5 Needs of Law Enforcement

- Policies and procedures for unmanned and automated vehicles
- Virtual criminal record catalog
- Better access to data for facial recognition identification
- Biomedical sensors for officers
- Identification of officers in close proximity

Top 5 Needs of Courts

- Video links to correctional facilities
- Procurement checklist for courts' information technology
- High-speed Internet connections for courts
- Virtual courtrooms
- Educational materials on key web technologies

Top 5 Needs of Corrections



- Video links to correctional facilities
- Better access to data for facial recognition identification
- Biomedical sensors for officers
- Internet of Things–enabled models for house arrest
- Educational materials on key web technologies

Conclusions and Recommendations

Information sharing: Partner with the Standards Coordinating Council and constituent information-sharing development efforts to explore how semantic tags and intelligent agents might be leveraged to expedite information sharing, with criminal history data as a starting point. Experiment with real-time language technologies.

Practitioners' knowledge: Focus education efforts on semantic technologies that support finding, accessing, and translating key information; sensor systems for monitoring officer health and officer safety, and maintaining community supervision; video conferencing; and civil rights, privacy rights, and cybersecurity protections.

Designate a group to develop law enforcement requirements, policies, and procedures, for interfacing with self-driving cars.

Infrastructure: Develop field experiments with video teleconferencing links for inmate communications and remote education. Pursue novel business models and support to make Internet links more affordable in rural areas.

IoT sensors: Experiment with health and safety sensor feeds, both wearable and embedded. Experiment with Internet-connected sensor systems to support maintaining the location and tracking of offenders under community corrections supervision.

Civil rights, privacy rights, and cybersecurity: At a strategic level, seek to ensure that civil rights, privacy rights, and cybersecurity provisions are built into technology developments, standards, policies, and procedures from the beginning. For intelligent agents that support decisionmaking, research how to ensure the quality of data used to make the decision, and how decisionmakers should use the agents' recommendations. For IoT sensors, conduct research to advise on common attributes for policies, procedures, and required protective technologies for sensors related to the IoT.

INTRODUCTION

The police officer directing traffic in the intersection could see the car barreling toward him and the occupant looking down at his smartphone. Officer Rodriguez gestured for the car to stop, and the self-driving vehicle rolled to a halt behind the crosswalk.

The officer waved the car on as the oblivious passenger continued checking his email. But he wasn't oblivious for long. A very human-driven sport-utility vehicle (SUV) barreled through the intersection, forcing the officer to dive for safety and the automated car to brake hard and swerve to avoid a collision.

While Officer Rodriguez called for assistance, an unmanned aerial vehicle on patrol recognized the speeding SUV and gave chase while it transmitted the vehicle's location to police cruisers. A police cruiser precision immobilization technique (PIT) maneuver forced the SUV off the road minutes later.[1] *As officers prepared to swarm the vehicle, one took the man's photo from a distance, uploaded it to compare against a national repository of mug shots, and quickly produced a high-probability match. The photo, combined with the license plate and vehicle description, helped the system identify an ex-convict who was related to the SUV's owner, and who had a lengthy rap sheet of armed robbery and reckless driving.*

A few moments later, an armed robbery at a nearby gas station crackled over the officers' radios. Surveillance photos from the scene, showing the SUV driver pointing a weapon at the gas station attendant, arrived shortly after the suspect had been safely taken into custody—where he would remain for a very long time.

How we use information technology (IT) is on the verge of dramatic change. In the past, the World Wide Web and the Internet largely have involved passive activities: reading or watching multimedia on a computer screen or typing in search requests on a keyboard or touch screen. Over time, we have migrated from personal computers to laptops to tablets and smartphones, but the basic interactions with the web have been the same. In the future, however, the web will be embedded in our surroundings—in clothes, cars, appliances, flying unmanned vehicles, and utility grids themselves. Rather than typing in search requests, information services will be delivered to us somewhat automatically, depending on context. Criminal justice agencies must prepare to make the most of this transition while protecting civilians from the threats these new technologies may present.

The web as we have known it—mostly web pages and social media—has had a significant impact on criminal justice. For example, the massive-scale "crowdsourcing" of pictures and video from the Boston Marathon bombing generated a great deal of useful intelligence for investigators (Wadwha, 2013). However, the criminal justice community often is perceived as largely reacting to new web technologies (and other technologies; see, for example, Smith, 2013) rather than anticipating them. In addition, not every innovation is perfect or always useful to criminal justice. The same crowdsourcing that produced useful intelligence after the Boston Marathon bombing also resulted in a number of innocent people being wrongly accused (Wadwha [2013] notes that the crowdsourcing was a great success at gathering information but a failure at investigating it).

To help the criminal justice community learn about upcoming web technologies, and to start informing developers and policymakers about what criminal justice practitioners will need to use new technologies effectively, the RAND Corporation and the National Institute of Justice (NIJ) brought together an expert panel of 16 practitioners and technology experts. Collectively, they discussed what upcoming web technologies are valuable and what they likely will mean for criminal justice. Then they identified and prioritized 45 needs for both technology and policy development that would allow usage of new technologies

successfully while mitigating the technologies' risks. This report summarizes the panel's discussion, first describing what the new technologies are and how they might be used, then covering the specific needs for technology and policy development.

EMERGING WEB TECHNOLOGIES AND CRIMINAL JUSTICE

The current web technologies that we regularly use are commonly referred to as *Web 2.0 technologies*. These include basic web pages that look like documents, searches based on keywords and phrases, online mapping and navigation, and social media. Table 1 adapts Kevin Kelly's perspective on the history of the web and associated information technologies (2007). While there are no canonical definitions of web generations, Kelly's descriptions are some of the most widely disseminated. Kelly characterizes the linking of documents, individuals, and data as generations 1.0, 2.0, and 3.0 of the web. In the table, we extend his characterization into the past and future by examining the IT linkages that came before and the ones that are just over the horizon. As noted, Web 2.0 can be thought of as today's web, as social media and crowdsourcing technologies (along with the Web 1.0 baseline technologies of document browsing and searching) are ubiquitous. Web 3.0 and 4.0 technologies are emerging now.

The key technologies for Web 3.0 (predominantly Semantic Web–related) tend to be foundational in nature: They support the information management and sharing needed to enable the more immediately visible technologies (intelligent agents and Internet of Things [IoT]) of Web 4.0.

Web 3.0 and 4.0 technologies will have a variety of potential applications and effects on the criminal justice system. As a whole, these technologies will change the way citizens obtain and synthesize information. They will offer cheaper and more accessible methods for physically monitoring our personal environments or any other environment of interest. In addition, they will offer the ability to intelligently and remotely react to changes in those environments.

> These technologies will improve the ability of average citizens and criminal justice practitioners to "see" around corners.

Imagining the Technological Future of Criminal Justice

These technologies will improve the ability of average citizens and criminal justice practitioners to "see" around corners. This improved sight will be physical in terms of remote monitoring, and informational in terms of having access to (or being intelligently supplied with) highly relevant, just-in-time information about individuals' identities, connections, reputations, histories (including criminal), past and present whereabouts, etc.

Imagine a law enforcement officer interacting with a vehicle that has sensors connected to the Internet. With the appropriate judicial clearances, an officer could ask the vehicle to identify its occupants and location histories. The officer then could use Semantic Web technologies to review the criminal histories and search for any outstanding warrants of the occupants across dozens or even hundreds of local, state, and federal repositories—even repositories that do not contain data in a traditional "compatible data format" (but that are semantically tagged). Or, if the vehicle is unmanned but capable of autonomous movement and in an undesirable location (for example, parked illegally or in the immediate vicinity of an emergency), an officer could direct the vehicle to move to a new location (with the vehicle's intelligent agents recognizing "officer" and "directions to move") and automatically notify its owner and occupants.

Individuals on pretrial or postconviction supervision are already being fitted with location monitoring devices. As the communication and processing capabilities of these devices improve, they also might monitor these individuals' stress levels, drug use, or states of arousal (for sex offenders). They could allow for video or telephonic connections to monitored individuals and provide the monitoring officer with clues about the truthfulness of verbal responses. More broadly, suppose that an offender disables a tracking bracelet before leaving his or her home to commit a crime. Other sensors in the home could notify police of the offender's departure.

Of course, all of this "vision," monitoring, and sensitive information sharing raises substantial security, privacy, and

Table 1. Generations of Linkages in Information Technology

Generation	What Was Linked?	Characteristics
0.0	Nothing (stand-alone personal computers)	Vast computational power becomes accessible to the masses.
0.5	Computers were linked in local networks, which were further linked into *Inter-net*works.	The capability was developed to share such resources as files, printing, processing, and storage.
1.0	Documents were linked to create the World Wide Web. Search engines helped users discover these documents through keyword searches.	Initial use was an extension of existing content and information sources (broadcast, publishing, etc.), with institutions making online content available to users.
2.0	Individuals and groups are linked to form social networks. Networks of individuals are able to collaborate en masse to intelligently achieve objectives (crowdsourcing).	Information flow becomes much more collaborative and bidirectional with sharing of text, images, video, etc. Users become content creators, not just readers of institutionally published information. Crowdsourcing is used to identify and locate suspects, identify crime hotspots, and address other problems in emergency response and beyond.
3.0	**Semantic Web:** Data are semantically tagged and linked. Information searches use context and natural language instead of just keywords. Researchers have access to datasets that are linked together through formal, structured relationships.	Computers are better able to "understand" the content of the information processed and "communicate" with humans using spoken and written language. Difficult analytic problems can be solved using data that was previously difficult to integrate (such as medical records and medical research). With semantic tagging and linking, one can "ask" the following types of requests: • "Find scientific publications like those written by these specified authors" • "Find pictures of Georgian chests of drawers for sale near my house" • "Find other employees whose backgrounds make them a good fit for my project" • "Display a network chart of all technical design documents for this wing assembly and the relationships between the documents" • "Show me points of interest around me as I walk down this street" (also relevant to the IoT, below).[a]
4.0	**Intelligent agents:** Intelligent software agents learn and perform rudimentary tasks.	Software tools learn what sorts of information and analysis a user wants, and delivers it to him or her regularly. Some of these tools are embedded in devices (see IoT, below). Two key types of intelligent agents are especially relevant to criminal justice: • search agents that scan a range of media (social media postings, video, photos, etc.) to find events "of interest." In the criminal justice context, these tend to relate to suspicious activity or a possible connection to a crime. • decision agents that take in a range of data and use statistical algorithms to advise someone on how to make a decision. In the criminal justice context, these might include judgments on bail or sentencing.
	Internet of Things: Previously unlinked everyday objects are now linked to the Internet: automobile, refrigerator, watch, smoke detector, thermostat, airline seat, etc.	The services provided by these objects are enhanced. Connected cars can improve traffic flow. Things become sensors that can collaborate to improve life. One example is buildings that adapt to weather, warn/defend against external emergencies (earthquake, tornado, fire, flood, etc.), or report the number of building occupants, their locations, and vital signs. Autonomous vehicles can be thought of as part of both intelligent agents and the IoT.

[a] These questions are adapted in part from examples taken from the World Wide Web Consortium's draft requirements for an initial web ontology language (Heflin, Volz, and Dale, 2002).

> Interagency communication has been a perennial problem for all organizations, and criminal justice organizations are no different.

civil rights questions; we discuss these issues further below. In the worst case, individuals' private behavior and personal data could be stolen and exploited, either by criminal hackers or corrupt government officials.

Interagency communication has been a perennial problem for all organizations, and criminal justice organizations are no different. Lawyers and courts have a constant need to schedule appearances efficiently, and law enforcement agencies need up-to-date information on the status of parolees when they encounter them. Many agencies currently rely on Web 1.0 technologies to address this need. Community corrections officers (whom courts often employ), periodically export lists of parolees by email or host them on secure file transfer protocol sites, transferring files from one host to another for law enforcement use. These are transmitted in "standard" formats, such as extensible markup language (XML) or Excel worksheets. Web 3.0 technologies, such as linked data, will facilitate on-demand access to this information and make it available to a larger number of agencies. Semantic Web and linked data techniques can facilitate the interconnection of documents, social networks, and databases, without regard to the structure of the underlying data source (provided the data are tagged and stored in a core format that can be searched, retrieved, and displayed readily). When fully realized in this context, linked data techniques will provide law enforcement with the most accurate and timely information while providing parole officers with important details about parolees' contact with law enforcement.

The scheduling of courtrooms, judges, lawyers, and others in the criminal justice system was noted as a problem during the workshop. In the future, a court system could use intelligent software agents working on behalf of their human and physical (courtroom) counterparts to automatically and intelligently examine and prioritize individual schedules and dynamically assemble a court docket. Once assembled, the individual agents could push updated information to other interested parties and the public.

It is important to address another technology that is not actually new: cheap and portable personal video teleconference equipment (on smartphones, computers, and other devices), which is nearly ubiquitous. The expert panel discussed this at length due to its potential uses in the law enforcement, court, and prison systems. What is new is the growing accessibility-on-demand and interconnection of all these systems, made possible by emerging Web 3.0 and 4.0 standards. Consequently, judges might be able to set up court nearly anywhere ("courtroom in a box") or receive remote testimony from anywhere. Prisoners might be able to better maintain family connections, build connections with their parole officer and social service providers, and generally improve their transition to civilian life through easy and inexpensive videoconferencing—all while intelligent agents monitor their communications to flag any discussions that appear to reference criminal activity.

However, the dark side to all of the emerging access and interconnectivity is the risk to the public's civil rights, privacy rights, and security. One can readily imagine abuses that might occur if, for example, capabilities to control automated vehicles and the disclosure of detailed personal information about their occupants were not tightly controlled and secured. Intelligent agents monitoring social media feeds might wrongly flag certain people as potential suspects—notwithstanding larger issues of the circumstances under which such monitoring is justified. Policies, procedures, and technologies to help ensure that new technologies are not abused were a major discussion throughout the workshop.

Methodology

To consider the implications of these rapidly emerging technologies for criminal justice—as well as how the criminal justice community might get ahead of the curve in using them—NIJ asked RAND to assemble an expert panel of both criminal justice practitioners and technologists. In all, 16 panelists participated; see the appendix for the complete list. On the practitioner side, we asked the major practitioner associations in law enforcement, courts, and corrections to send representatives to serve as the practitioner experts. Six associations sent representatives: the International Association of Crime Analysts, the International Association of Chiefs of Police, the American

Jail Association, the American Probation and Parole Association, the American Correctional Association, and the National Center for State Courts.

On the technologist side, RAND identified a list of experts with substantial backgrounds in the key web technologies under consideration (intelligent agents, Semantic Web, and sensors/IoT), as well as general expertise with IT in the public sector. RAND Knowledge Services, in particular, conducted a detailed search of experts' online information to prepare brief profiles of candidates, with those who had some experience working in the public sector (especially security and/or criminal justice) given priority for potential participation. Ten of these technical experts agreed to attend the workshop.

In hosting the panel, we recognized that since Web 3.0+ technologies are new to criminal justice, few attendees would have experience both with the new technologies and with criminal justice technologies and practices. Thus, our concept was to bring together those with both web technology expertise and criminal justice expertise and provide orientation materials and sessions to share information about both web technologies trends and criminal justice technology perspectives. We then had the panelists work together in small breakout groups to jointly discuss pressing problems in criminal justice and how the new technologies might help or hinder solutions, as well as general opportunities and challenges the new web technologies might raise for criminal justice. We then had the panelists use these issues to generate specific needs to leverage the opportunities and mitigate the challenges posed by Web 3.0+ technologies; those needs could include technical development, policy changes, practices changes, and training changes.

After departing the workshop, the panel convened electronically in multiple rounds to consolidate, edit, categorize, and prioritize the needs. The technical details are described in the appendix to this report. In brief, panelists rated how valuable a solution to each need might be to each community of practice (law enforcement, courts, and corrections). They then assessed how technically feasible and operationally feasible it would be to develop and field those solutions. (Here, panelists were asked to explicitly include affordability, civil rights, privacy rights, and security concerns in making operational feasibility ratings.) We then combined these ratings to produce *expected value* (EV) scores—how much value a solution might provide multiplied by the likelihood a solution actually could be produced and fielded.

To provide rough assessments of the needs priorities, we used a clustering tool to divide the needs into three tiers: Tier 1 (high priority), Tier 2 (medium priority), and Tier 3 (low priority). The tool was used to find the "best overall" splits to divide the needs into tiers, with "best" measured in a mathematical sense.

The panelists frequently flagged particular needs as raising civil rights, privacy rights, or cybersecurity issues. We tracked which needs were flagged as raising one or more of these issues as well.

We believe that we assembled an experienced group of panelists who produced a well-founded set of technology needs. The final panel was split roughly 50–50 between those who had web technologies expertise and those who had expertise on criminal justice IT and practices. Panel members' specific areas of expertise included

- criminal justice technologies, standards, and practices, focusing on IT for institutional corrections, community corrections, courts, crime analysis, and law enforcement
- Semantic Web technology, to include providing education about Semantic Web technology in general and using semantic links to improve what is known about the provenance and trustworthiness of data

Our concept was to bring together those with both web technology expertise and criminal justice expertise and provide orientation materials and sessions to share information about both web technologies trends and criminal justice technology perspectives.

- the IoT, including developing both hardware and software (on-device and backend processing)
- public sector IT, including experience with eGovernment and Open Government initiatives, serving as a state and agency chief information officer, and expertise in communications and computing infrastructure providing high-bandwidth data and video
- technologies related to Web 3.0+, including IT security, civil rights, and digital privacy issues and solutions; security and management controls and audits specifically for government agencies; XML and transaction processing; and geospatial analysis, including recognizing, geocoding, and visualizing event location data with assorted details.

However, we recognize that these results reflect their subjective assessments, and as with any panel exercise involving a limited number of participants, a different group may well have produced a different set of results. That said, our findings are consistent with our prior studies on criminal justice technology needs (Hollywood et al., 2015, Jackson et al., 2015, Silberglitt et al., 2015) and with findings from earlier studies on law enforcement technology needs (Koper, Taylor, and Kubu, 2009; International Association of Chiefs of Police, 2005), and we believe they will provide a useful guide to both practitioners and developers in considering how to leverage Web 3.0+ technologies.

Top Technology Needs from the Workshop for Each Community of Practice

Table 2 summarizes the Tier 1 needs overall and for each criminal justice community of practice. The needs are shown in order of their expected value for that community of practice, with the need with the highest score shown first.

One need has a single star—providing video links to correctional facilities had scores noticeably higher than the scores for all other needs. Two needs at the bottom of the corrections list are double-starred. These are needs that were initially assigned to Tier 2 by the predictive analytics tool but had noticeably higher scores than other Tier 2 needs. They are included in Table 2 because there are comparatively few Tier 1 needs for corrections as a percentage of all corrections needs (there are fewer Tier 1 needs for courts, but there also were fewer courts needs overall).

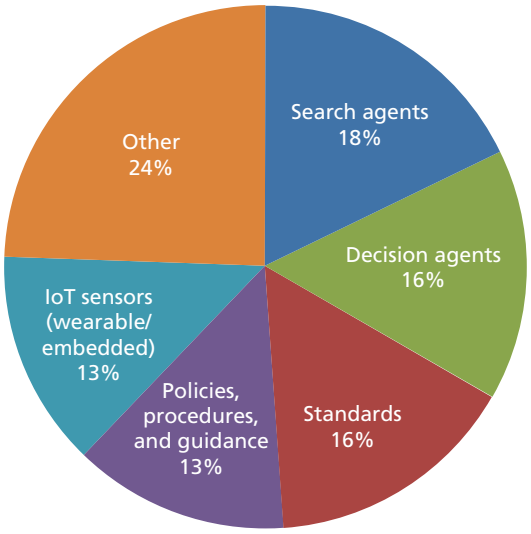
Figure 1 summarizes the needs by technology area. As shown, three-quarters of the needs are related to intelligent agents (both to search for suspicious activity and to help personnel make decisions in the field), standards leveraging the Semantic Web, policies and procedures for using the emerging technologies, and sensors in the IoT. The remaining quarter of the needs under "Other" covers a wide range of technical topics. These included improving networking infrastructure, research on displaying information, real-time language interpretation, real-time decryption of criminals' codes, facial recognition, identifying structured data in free text, and interfaces with unmanned vehicles.

On average, the scores for search agents were on the low side, whereas the scores for standards and policies, procedures, and guidance were on the high side. The lower scores for search agents appear due in part to feasibility issues (such as whether search agents can really find genuinely worrisome activity going on while avoiding "finding" huge numbers of innocent activities). The lower scores also were due in part to concerns about civil and privacy rights (since, depending on the application, many agents would be searching through large amounts of public data). The higher scores for standards and policies, procedures, and guidance appear to be due to (1) being seen as necessary to the use of web technologies across the criminal justice community and (2) being comparatively easy to develop and implement.

DISCUSSION

In prior research on priority criminal justice technology needs (International Association of Chiefs of Police, 2005, Koper, Taylor, and Kubu, 2009, and Hollywood et al., 2015, on needs

Figure 1. Needs by Technology Category



RAND *RR928-1*

Table 2. Top Needs Overall and for Each Community of Practice

Overall
Video links to correctional facilities*
Educational materials on key web technologies
Real-time language interpretation
Virtual criminal record catalog
Technological infrastructure for criminal justice interfaces (elements needed for information sharing)
Funding high-speed Internet connections for courts
Tools to improve data quality and integrity
Cost-benefit tools for technology acquisition
Policies and procedures for emerging IoT and Semantic Web technologies
Improved sharing of information about offenders with third parties (treatment providers and other stakeholders)
Better access to data for facial recognition identification
Biomedical sensors for officers
Research on information overload
Intelligent agents to help protect digital evidence chain of custody
Situational awareness/mapping displays tailored to individual officers
Improved tracking of officers within buildings
Procurement checklist for courts IT
Law Enforcement
Policies and procedures for unmanned and automated vehicles
Virtual criminal record catalog
Better access to data for facial recognition identification
Biomedical sensors for officers
Identification of officers in close proximity
Educational materials on key web technologies
Research on information overload
Video links to facilities
Real-time language interpretation
Situational awareness/mapping displays tailored to individual officers
Analytics for social media and community feedback
Improved tracking of officers within buildings
Tool to assess skills of individuals at an incident
Policies and procedures for emerging IoT and Semantic Web technologies
Corrections
Video links to correctional facilities*
Better access to data for facial recognition identification
Biomedical sensors for officers
IoT-enabled models for house arrest
Educational materials on key web technologies
High-speed Internet connections for courts
Situational awareness/mapping displays tailored to individual officers**
Improved tracking of officers within buildings**
Courts
Video links to correctional facilities
Procurement checklist for courts IT
High-speed Internet connections for courts
Virtual courtrooms
Educational materials on key web technologies
Real-time language interpretation

* Scores noticeably higher than scores for all other needs.

** Initially assigned to Tier 2 by the predictive analytics tool but had noticeably higher scores than other Tier 2 needs

The call for "technological infrastructure" closely matches the general desire to improve criminal justice information sharing, in a single need.

for law enforcement; Jackson et al., 2015, on needs for corrections; and Silberglitt et al., 2015, on future needs for law enforcement), top needs could be grouped into three overarching themes. The first reflects a general demand for greater knowledge and educational development about technologies as well as how to apply them effectively. The second reflects a general demand to improve the sharing and display of information as needed across the criminal justice enterprise. The third comprises "everything else." That same pattern applies to the results from the Web 3.0+ technologies workshop, with a few additional themes emerging: a need to improve networking infrastructure; a need to develop IoT sensors for criminal justice; and a need to ensure protections of civil rights, privacy right, and cybersecurity around the use of web technologies in criminal justice. The specifics are discussed below.

Theme 1: Improving Information Sharing

The driver stopped by Officer Nguyen appeared to be completely confused by the officer's request to produce his license and registration. "No entiendo," he said. "No hablo Inglés." The officer's earpiece immediately translated: "I don't understand. I don't speak English."

Officer Nguyen held out a small speaker and spoke quietly into a microphone. In Spanish, the man heard the officer's words: "That's okay, I just need your license and registration."

The cluster of demands for improved information sharing had the highest number of top-tier needs (eight). These are, in order of overall expected value (with the most needed at the top),

- real-time language interpretation (ranked third overall)
- virtual criminal record catalog (ranked second for law enforcement and fourth overall)
- technological infrastructure for criminal justice interfaces (ranked fifth overall)
- tools to improve data quality and integrity
- improved sharing of information about offenders with third parties (treatment providers and other stakeholders)
- better access to data for facial recognition identification (ranked second for corrections)
- research on information overload
- situational awareness/mapping displays tailored to individual officers.

All of these demands were discussed in the context of leveraging web technologies, especially Semantic Web (3.0 technologies), to support meeting them. We discuss how web technologies might be leveraged to improve information sharing and security below, first in the general sense, and then with regard to the specific needs under this theme.

Web Technologies to Improve Information Sharing and Safeguarding in General

Panelists thought it would be useful to explore whether semantic tagging might help facilitate data sharing in general, along with a range of data safeguards (on data provenance, privacy, and data access) and whether intelligent agents might be used to monitor and enforce access control and usage policies. As an initial focus, panelists thought it would be useful to develop standards for criminal history data, to include sharing specifications, cataloging specifications, and common policies.

The call for "technological infrastructure" closely matches the general desire to improve criminal justice information sharing, in a single need. Hollywood et al. (2015) touch on the substantial difficulties and complexities involved in developing all the components needed for genuine, seamless information sharing, while acknowledging the substantial progress made to date. During the workshop, there were discussions on how web technologies, especially semantic tagging, with some assistance from intelligent agents, might facilitate sharing and safeguarding information, in general. (Here, "safeguarding" includes both cybersecurity and protecting the quality and integrity of the information.)

To get a sense of how semantic and agent technologies might help, we discuss the major advance between Web 1.0/2.0

and Web 3.0 in more detail. Coding (tagging) of web pages in Web 1.0 and 2.0 was primarily about formatting how the pages would appear—where to make text appear in bold or in italics, what color to make the page, where and how to put content in tables, and so on. Relationships were included, but just on the level of "click here to go this other web page." While one certainly could—and did—support searching for information across pages, the searching was based on matching key words and terms, with Google and others adding methods for guessing which pages a user would likely want, based on which pages had the most inbound links, where they were searching from, and so on (Page et al., 1998, provides an early discussion of Google's algorithms, for example).

We also note, today, that most criminal justice data are stored in *relational databases*. This means data are stored in large structured tables, with records as the rows of the table and fields as the columns. Importantly, each table entry typically is a small piece of structured data, such as a number or a small text string ("street name, no more than 80 characters"). Each record has a unique identifier, called a key. In a records management system, for example, one typically has data tables describing basic facts about persons, a second describing locations, a third describing tables, and other tables describing facts about incidents. (See, for example, Law Enforcement Information Technology Standard Council, 2008). Pulling a person's criminal history involves querying and joining information both about the person (from a "names table") and about the past crimes they committed (from the incidents table). The difficulty is compounded if one wants to pull a person's criminal history across multiple jurisdictions where he or she committed crimes—one has to put in very specific queries to a whole range of disjointed databases in different agencies, and then be able to properly interpret and assemble the results. Consider how different agencies' databases might treat "name" differently: Is it first name/last name? Is it all one string? Are the middle initial or full middle name included, and if so, where? What if someone is a Sr., Jr., or III? And these questions are just for a person's name. It is easy to see how databases are naturally non-interoperable with each other.

What the Semantic Web does is add codes (tags) that characterize the *content* of information in a web page, as well as *relationships* to related information, not just describe how to display the information. For example, a person can now have a page of machine-readable data about themselves that looks like:

```
<foaf:Person>
    <foaf:name>John Smith</foaf:name>
    <foaf:homepage rdf:resource=http://person.org/JohnSmith />
    <foaf:img rdf:resource=http://person.org/JohnSmith/picture_of_me />
</foaf:Person>
```

Despite the symbols (tags), it is clear that we have described a person named John Smith along with his homepage and a picture of him. The tags make it possible for computer software agents to determine that as well. It is similarly possible to add machine-readable fields describing organizations to which John Smith belongs, who his associates are (linking to their machine-readable profiles), and where he lives and works. The semantic tags shown are part of the Friend-of-a-Friend (FOAF) format (Foaf Project, undated).

New types of databases also are being deployed, with a key type being documented-oriented databases (Lerman, 2011). Rather than being a set of small-tightly-controlled fields in a table, each record is now a text document filled with data coded with tags such as the one shown above, as well as content-tagged links to other related information, which can be inside or outside of the database. The format makes it very easy to add new information—if a subject is convicted of another crime, for example, his or her criminal history document can be updated with that conviction event by adding a few lines of tagged text.

We can see how the use of these technologies might make sharing criminal justice information much easier. Suppose an officer needs to look up the criminal history of a suspect quickly:

- First, it will be much easier to search specifically for criminal history records across a range of systems, since they will be specifically tagged as criminal history records.
- Finding the right record will also be much easier, since the officer will be able to search specifically on what is known

New types of databases also are being deployed, with a key type being documented-oriented databases.

about the person—name, address, scars/marks/tattoos, or any other specific information known about the person.
- It will be much easier to put together the criminal history of the subject, as almost all of it will be part of one document record, perhaps with links to related information (photos, detailed reports about specific incidents, etc.). The history will not have to be assembled across multiple tables and databases.
- Finally, it will be much easier to look up and review the related, linked information, as the linked information itself will be expressed in terms of these tagged text documents. It is much easier and much more robust to interpret the tagged text than to have to deal with the very specific file and data formats used within traditional databases. For example, we will know a block of text in a document record is an <address> as opposed to having to interpret how an agency's internal database chops up and represents all of the different parts of an address.

Intelligent agents, especially search agents, hold the promise of leveraging these tags to simplify and automate the searching and retrieval described above.

New web technologies developments have promise for making information safeguarding much easier as well. The same sorts of tags described above can also be used to describe the security requirements to access a document (or a database of documents). Identity and access management systems for users similarly have tagged documents describing information about each user, so in principle, one can then match up the users' credentials with document access requirements to determine whether a given user can get a given document. The goal is to move toward "single sign-on" systems in which a user needs to log into only one portal to get access to all of the information needed to do his or her job, as opposed to having to log in to up to dozens of separate systems.

New web technologies developments have promise for making information safeguarding much easier as well.

Further, it is now becoming possible to largely automate one of the most painful parts of information sharing—negotiating memoranda of understanding between multiple agencies to share information. These depend in large part on all parties agreeing on whom (more specifically, which *roles*) will get access to the information and what security measures will be taken on both ends with the data. In an initiative called Trustmarks, both those seeking information and those providing information can get certified tags (the trustmarks) describing their roles and the security measures with which they comply (as well as the auditing mechanisms checking compliance), making it possible to automatically identify whether two agencies can share based on matching roles and trustmarks (GTRI NSTIC Trustmark Pilot, undated). As with searching, intelligent agents can simplify and automate the process of interpreting trustmarks and other security tags to get access to needed information.

Opportunities for and Obstacles to Improving Information Sharing in General

Both the biggest opportunity for and obstacle to information sharing is the large number of information-sharing initiatives under way. A top finding from Hollywood et al. (2015) was that integration and dissemination of existing information-sharing efforts were needed far more than new starts. To incorporate Semantic Web and other technologies into criminal justice information sharing would involve coordinating Global Justice Information Sharing Initiative (GLOBAL), National Information Exchange Model (NIEM), and other key developers (Federal Bureau of Investigation Criminal Justice Information Systems, IJIS Institute standards and testing development,[2] and International Association of Chiefs of Police Model Policies are a few key examples) to determine whether web technologies might help expedite building information exchange and information assurance standards. The recently formed Standards Coordination Council, an advisory working group to the White House on information sharing and safeguarding standards, includes 14 different organizations (Standards Coordinating Council, undated).

The number of different standards themselves is far larger. For example, NIEM information exchange package documents (IEPDs) are key tools for supporting information sharing across multiple systems. However, there are hundreds

of such IEPDs, and they overlap and can be inconsistent.[3] A search for "criminal history" on the IEPD Clearinghouse (undated) alone found 91 relevant IEPDs. Coordination and integration will be one of the biggest challenges. Policies and procedures for sharing this information with third-party providers such as treatment providers would address an additional top-priority need. Similarly, developing policies and procedures for emerging IoT might be folded into existing efforts toward developing model IT policy.

Specific Needs Related to Information Sharing

Here we discuss top-rated information sharing needs that were highly specific.

Better access to facial data addresses the specific problem of not being able to query the full range of federal, state, and local databases containing mug shots. It was seen as a policy problem as much as a technical data-exchange problem. This need did raise substantial concerns about civil rights and privacy rights that included ensuring proper access to sensitive information and the risk of false matches (for example, identifying someone as a criminal based solely on his or her appearance). Panelists also noted that addressing this need would have to be consistent with the Federal Bureau of Investigation's (FBI's) new Interstate Photo System (part of the FBI's larger Next Generation Identification system).

The call for "situational awareness displays" to use the shared information effectively closely parallels a similar need for law enforcement IT (Hollywood et al., 2015). Also related is a call for human factors research on averting information overload from all the incoming data.

As with information-sharing infrastructure, ongoing research and development is related to developing situational awareness displays, or "dashboards," for staff at different levels. Semantic tags and intelligent agents might contribute to these research and development (R&D) efforts. For example, semantic tags might lead to better ways to display what is most relevant in various situations while hiding what is not. Similarly, intelligent agents populating the dashboards offer the possibility of addressing information overloads—assuming that the intelligent agents can be readily trained to give users the types of information they need when they need it.

The highest-ranking machine-to-user need—and the highest-ranking information-sharing need overall—was to *develop real-time language interpretation services*. There does appear to be substantial commercial development in this area that could be leveraged; for example, Microsoft in December 2014 released a real-time English-to-Spanish translation service for Skype (Warren, 2014).

Theme 2: Improving Practitioners' Knowledge of Web Technologies and Their Uses

Chief Holmes had just suffered through an hourlong presentation on the ever-worsening cyber threat. He knew about hijacked and defaced websites, but that was just the very tip of the iceberg. Stolen case investigation records. Names, photos, and addresses of undercover officers posted online. Overseas crime syndicates holding departments' entire computer systems for ransom. That part was terrifying, but at least it was understandable. Then came half an hour of numbing acronym soup about dozens of places to report attacks, dozens of development tools, government standards, references that presumably were great if you were a computer security expert, and something about improved tags that would help protect data and intelligent agents that would help figure out who was a real user and who was a hacker. When question time finally came about, he raised his hand.

"Excuse me, but like most of us, all I know about security is to install antivirus and not use the return key for my password. You've done a great job telling us about the threat, but for those of us who aren't security experts, what are we supposed to do? How do we get started?"

"Well . . . um . . . maybe you could go to . . . um . . . ?"

The highest-ranking machine-to-user need—and the highest-ranking information-sharing need overall—was to develop real-time language interpretation services.

This theme comprises methods to help practitioners learn more about technologies, use them properly and effectively, and acquire them. Improving practitioners' knowledge had the second-highest number of top-tier needs (five)

- educational materials on key web technologies (ranked second overall)
- cost-benefit tools for technology acquisition
- policies and procedures for emerging IoT and Semantic Web technologies
- procurement checklist for courts IT (ranked second for courts)
- policies and procedures for unmanned, automated vehicles (top-ranked need for law enforcement).

Education on Web Technologies, in General

The second-ranked need overall was to provide the criminal justice community with educational materials on the core Web 3.0+ technologies. This need is broadly in keeping with the findings from prior research into improving practitioners' knowledge of key technologies in general. Panelists discussed providing education and training, model policies and procedures, and/or acquisition checklists for

- Semantic Web technologies (and related developments, such as document databases) that specifically support finding criminal justice information (such as criminal histories), getting access to information, and translating and using information. An example is the discussion in the previous section of how to use semantic tags combined with document databases to share criminal justice histories.
- IoT sensors and actuators, especially those related to top needs for monitoring officer health and officer safety, as well as maintaining house arrest conditions (as described under Theme 4, below)
- entity analytics, which are tools that can take plain text and parse them into structured data. Key examples include tools that can pull names, addresses, phone numbers, license plate tags, and email addresses out of plain text, as well as generate relationships between them (such as details about people who live at the same address).
- video conferencing/tele-education technologies and services, to include both the tools themselves and the infrastructure and information access policies needed to support them
- civil rights, privacy rights, and cybersecurity technology issues and solutions (see Theme 5, below)
- emerging real-time language systems, as discussed above.

The principal opportunity in web technologies education is that a great deal is known about these technologies, especially in the commercial and academic sectors. However, there are two principal barriers. The first is that these technologies are largely new and unfamiliar to criminal justice, and it will take time and effort to introduce them.

The second is that technology education material is very widely distributed, with the Department of Justice (DoJ), practitioner associations, and some commercial associations all maintaining a wide range of web portals on criminal justice technology with varying degrees of awareness by the criminal justice communities of practice (see Gordon et al., 2012, for a larger discussion of this issue, focusing on the DoJ side). Even within portals, material is commonly presented as lists or databases of disjointed documents. At the 2015 Workshop on Information Sharing and Safeguarding, for example, it was noted that two key portals on information sharing tools, standards, and methods—the Standards Coordinating Council (SCC) portal (2015) and the Project Interoperability (undated) portals—are new and can thus be reasonably described as "grab-bags of stuff," with sponsors planning to integrate the materials and their presentation over time. These and other portals work for technical experts seeking a specific reference or two but do not work well for those seeking to develop technical expertise in the area or, more broadly, for agencies looking to acquire new technologies without much prior background.

Specific Needs Related to Technology Knowledge

On the specific needs side, the *procurement checklist for courts' IT* scored highly; it has been mentioned that the National Center for State Courts and others are preparing procurement guidance. That guidance may end up largely meeting this need.

The top law enforcement priority was *developing policies and procedures for self-driving unmanned and automated vehicles*. In addition to being the top-ranked need for law enforcement, it was the most "futuristic" of the needs considered. However, this area is developing rapidly; for example, California in 2014 issued to Audi the state's first permit allowing autonomous vehicles on public roads (Franzen, 2014). Panelists noted that law enforcement work in this area should coordinate closely with major existing policy efforts under way by the National Highway Traffic Safety Administration (NHTSA), state departments of transportation (especially the California Department of Motor

The breakout need from the workshop was to provide video links to corrections facilities so that community corrections officers could meet with inmates prior to their release.

Vehicles [DMV], given the amount of self-driving car activity centered there; see Madrigal, 2014), top self-driving car developers, and others. Panelists also advised prudence: The lowest-ranking need overall was to develop an interface for officers to directly take control of unmanned vehicles.

Theme 3: Improve Infrastructure

"And that about does it for me. Mr. Smith. Big thing is, our first phone call meeting at 2 p.m. next Thursday. You're going to call in from the warehouse lounge, right?"

"Yes."

Another voice and face chimed in on the screen. "And I'll expect you bright and early for your first day on the job on Thursday at 8:30 a.m., right? You know how to get here? If not, just call and we'll answer any questions you have."

"Yes, I won't have any problem."

A third person spoke. "And on Friday, you need to come to your initial counseling appointment at the Center after work. I know you know where that is."

"Yes, Dr. Nassar, looking forward to it."

"Okay, sounds like we're done here. Good luck and congratulations on getting early parole. Don't blow it. See you next week."

With that, the screen on Mr. Smith's tablet went blank. He leaned back on his cell cot, and pressed another tablet button to bring up the day's sports scores.

The common element in this theme is that leveraging web technologies in criminal justice requires the networking infrastructure to support them. This theme includes only three top-tier needs, but these were some of the highest-ranking needs. They include

- video links to correctional facilities (top need overall, for corrections and for courts)
- high-speed Internet connections for courts
- virtual courtrooms.

We talk below about each of these needs individually.

The breakout need from the workshop was to provide video links to correctional facilities so that community corrections officers (and other stakeholders, such as service providers) could meet with inmates prior to their release. We are aware of existing videoconferencing links and supporting technologies (secure tablets, for instance) to support remote education for prisoners; it may be possible to leverage some these systems for meetings with community corrections officers and other service providers. Notably, in 2014, the White House Office of Science and Technology Policy held a workshop on using technology to improve inmate re-entry. One of the major discussion topics at the workshop was the use of remote learning technologies (including video teleconferencing) to provide educational services to inmates; the technologies and infrastructure discussed there might be expanded to include teleconferences with external probation and parole officers and service providers.

The other two needs concerned high-speed Internet build-outs to courts. The first involved providing high-speed connections to existing courthouses in rural areas; the second (slightly lower-ranked) involved creating mobile communications packages to courtrooms that can be set up in other locations as needed. One panelist noted that the virtual courtrooms could be lower-ranked if high-speed Internet were provided to existing rural courthouses, because much of the need for virtual courtrooms and their associated expenses would disappear. These needs were primarily about obtaining funding for technology improvements; not much R&D is needed here. The principal barrier is obtaining funding.

Theme 4: Exploring the Use of Emerging IoT Sensors in Criminal Justice

Officer Jackson thought she smelled something—kind of like rancid cigarette smoke—but didn't think much of it as she searched the suspected drug house for stacks of small bills. She reached out to open a door that led down a hall to the kitchen.

> Three of the four needs concerned furthering officer health and safety.

The door felt warm, but not enough to really ring any alarm bells in her head. Suddenly, an alarm sounded in her ear, and a voice shouted over her earpiece, "Don't open that door! The house's alarm system says there's a fire in the kitchen!"

Of the three major Web 3.0+ technology areas (IoT, intelligent agents, and Semantic Web), IoT proved to be the one with its own cluster of needs. In comparison, Semantic Web technologies were subsumed into information sharing, and needs related to intelligent agents (search agents and decision agents) tended not to rank highly.

This theme includes four top-tier needs and has the fourth-greatest sum of overall expected value across its needs. Needs in this cluster constituted 8.7 percent of all needs' overall expected value scores. Top needs are

- Internet-enabled biomedical sensors for officers. A great deal of academic and commercial development has gone on this area; Steele and Clarke (2013) provide a reference.
- improving the tracking of officers within buildings. A great deal of academic and commercial development has gone on in this area, too; Schutzberg (2013) provides a quick reference.
- IoT-enabled models for house arrest
- identify officers in close proximity. The panelists noted that the human factors issues would require special attention—for example, one does not want loud buzzing to identify that an undercover agent is present.

Of interest, three of the four needs concerned furthering officer health and safety, which were similar to clusters of IT needs for law enforcement. Thus, protecting the health and safety of officers appears to be the principal topic of interest in this area. The final need involved the use of further sensors to supplement body-worn Global Positioning System (GPS) devices to locate and track offenders who are under community corrections supervision.

The use of IoT sensors in criminal justice involves two principal barriers. The first is the comparative newness of the technologies, with the exception of early body-worn GPS tracking devices. A great deal would need to be done to introduce and experiment with the technologies, and we reiterate that the challenge includes not just the devices themselves but also the large IT back-end needed to get data from the devices and use those data effectively.

The second comprises the risks to civil rights, privacy rights, and cybersecurity raised by the widespread use of deployable sensors. As noted below, IoT sensors received focused attention for raising these risks, and special attention will need to be paid to mitigating those risks.

Theme 5: Civil Rights, Privacy Rights, and Cybersecurity Concerns

The hacker grinned at his monitor. A few more commands and all of the supposedly secret names, addresses, and photos of the city's undercover officers and informants would be his. The initial plan was to dump all that information online. But then he wondered how much he could get by selling it to the local crime syndicates. Very tempting.

At last he was in. He eagerly downloaded the file and laughed as he brought it up. What? Big Bird? Bozo the Clown? Was this someone's idea of a joke? If so, he'd show them what a joke was when he made them pay—after a good night's sleep.

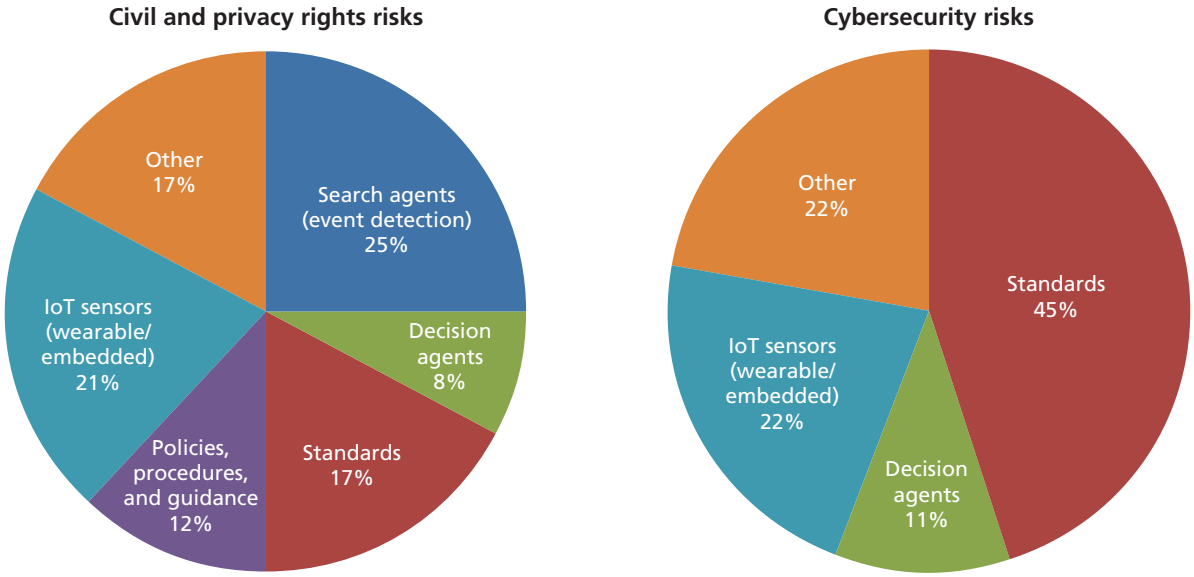
In the middle of the night, he awoke to what he wished was simply a nightmare: a group of officers who had been given his identity and location by the city's cybercrime unit.

Two overarching concerns were frequently discussed at the workshop, although they did not make their way into many needs. The first involved cybersecurity concerns arising from the new technologies, and the second involved privacy rights and civil rights.

Figure 2 shows the proportions of needs that panelists flagged as having potential civil rights, privacy rights, or cybersecurity risks. Twenty-four needs (53 percent) were flagged for potential civil rights or privacy rights implications; nine (20 percent) were flagged for potential security implications.

From a civil and privacy rights perspective, search agents were called out as potentially problematic due to their analyzing large amounts of public data (public surveillance cameras and social media feeds, for example) and generating large num-

Figure 2. Civil and Privacy Rights Risks and Cybersecurity Risks



RAND *RR928-2*

bers of false positives (such as subjects being incorrectly flagged as likely engaged in criminal behavior).

Decision agents, such as those related to recommending bail/bond or sentencing judgments, were seen as potentially raising civil rights concerns for computing decisions based on inadequate or biased data.

IoT sensors were seen as raising potential privacy issues from generating substantial data on persons either wearing sensors or those who are nearby. For example, one panelist noted, "We may need to monitor someone under community supervision, but we should not end up monitoring the others at the group counseling session with them."

From a security perspective, IoT sensors and other devices were seen as potentially vulnerable. By definition, they transmit and receive a great deal of data, providing access for hackers, and their small, lightweight, and inexpensive nature implies that the devices will not have a great deal of computing power to run security software. Beyond cybersecurity, operational security for sensor data was raised as well. For example, the top-tier need for sensors that can detect when other officers are nearby was seen as being a potentially critical tool for crisis response and operational deconfliction but also as a threat if criminals could recognize an undercover agent's sensor during an operation.

Standards were not seen as posing inherent risks to civil rights, privacy rights, or security. Rather, the concern was that because standards are inherently about enabling the sharing of sensitive criminal justice information, strong security measures and strong civil and privacy rights protections should be built into the standards to avoid opening vulnerabilities. Similarly, policies and procedures for using information resulting from Web 3.0+ technology applications were seen as needing strong protections for civil rights, privacy rights, and cybersecurity to defend against misuse of sensitive information.

Civil rights, privacy rights, and cybersecurity protections are major pain points across criminal justice technologies in general. They are repeatedly described at criminal justice workshops and conferences as areas in which agencies lack expertise. The White House Cybersecurity Coordinator, for example, described information security in general (not just for criminal justice) as widely seen as too hard and too expensive, and as something that still has to be added on by experts rather than being designed in and turned on in hardware and software systems by default (Daniel, 2015).

Comprehensive List of Key Criminal Justice Needs

Table 3 presents the needs from the Web 3.0+ Technologies Workshop by their technology category. Within tables, needs are presented in order of their overall expected value score, with highest score first. We also show what tier the need is in with respect to overall expected value. The last two columns show whether panelists flagged the need as having civil rights, privacy rights, or security issues.

Table 3. Needs from the Web 3.0+ Technologies Workshop

Legend			
Community of Practice key:	Law enforcement	Courts	Corrections
Tier key:	1: Top priority	2: Medium priority	3: Low priority
Privacy Rights/Civil Issue and Security key:	✓ Concern identified by panelists		

Community of Practice in Need	Description	Tier	Privacy Rights/ Civil Issue?	Security Issue?
Part 1: Decision Agents				
Law enforcement	*Digital evidence chain of custody* Need intelligent agents to help protect the chain of custody as digital evidence receives metadata markups for semantic search and analysis	1		
Law enforcement	*Skills assessment* Need to develop tools to help incident commanders/managers quickly identify or assemble teams with specific skills (such as language, hazardous materials, or hostage negotiation skills)	2		✓
Law enforcement, Courts	*Managing court workload* Need cognitive/artificial intelligence systems that use a range of data, including real-time data feeds, to inform day-to-day workloads of criminal justice staff ranging from law enforcement officers to judges	2		
Law enforcement	*Interviews and report writing* Need intelligent agents to assist with field interviews and writing incident reports, along with the controlled vocabularies required to develop them. The agents should make it easy to enter data, structure the data as they are entered to support later queries, and help enforce completeness (for example, "This is a burglary and you haven't entered a mode of entry. If you know the mode of entry, enter it now.")	2		
Law enforcement	*Digital evidence gathering* Need intelligent agents that can guide patrol officers to identify and recover digital evidence	2		
Courts	*Offender risk assessment* Need new risk assessment tools to inform court decisions and evaluate existing ones. These include tools informing pretrial bail setting and post-trial sentencing. Should include defining metrics and best practices for risk assessment tools	2	✓	
Courts	*Support for specialized courts* Need intelligent agents as "expert systems" to support decision-making for specific courts (drug courts, veteran courts, etc.)	2	✓	

Table 3—Continued

Community of Practice in Need	Description	Tier	Privacy Rights/ Civil Issue?	Security Issue?
Part 2: Internet-of-Things Sensors				
	*Biomedical sensors for officers* Need to develop and/or assess wearable biomedical sensors to monitor officer health and safety. Sensors should monitor stress levels, fatigue, and injuries. Data could be used to dynamically shorten work shifts if fatigue levels are excessive	1	✓	
	*Tracking officers inside buildings* Need to study using IoT sensors to better track officers inside buildings. Sensors should be both officer-worn sensors and within the building (for example, proximity sensors). Tracking would help improve officer safety and could be used for opening doors and other applications	1		✓
	*Monitoring alcohol/drug use* Need to develop and/or assess wearable sensors for monitoring offender use of alcohol or drugs as well as procedures for employing them effectively. Research should include authentication (ensuring the right individual is wearing the device) and integration of data into dashboards	2	✓	
	*Monitoring house arrest* Need to experiment with using IoT sensors to better enforce house arrest and noninstitutionalized corrections options	2	✓	✓
	*Identify nearby officers* Need to develop and/or assess wearable proximity sensors (such as automated virtual badges) to improve officers' situational awareness of each others' locations. Could be used for task forces; high-density, poor visibility, operational deconfliction; and undercover work	2	✓	
	*Emergency help for at-risk civilians* Need sensors to detect when someone needs emergency help at home (for people with disabilities or disease, or individuals at risk of domestic violence)	3	✓	
Part 3: Miscellaneous Technologies				
	*Video links to correctional facilities* Need to develop and/or assess video teleconferencing tools to allow incarcerated offenders to establish relationships and build rapport with community corrections officers before release	1		
	*Real-time translation* Need the capability to translate languages in real time. If not stand-alone, the capability should include connections so that remote officers and courts can access translation services	1		

Table 3—Continued

Community of Practice in Need	Description	Tier	Privacy Rights/ Civil Issue?	Security Issue?
Part 3: Miscellaneous Technologies (continued)				
	*High-speed Internet* Need to fund high-speed Internet for courts to enable web technologies and other tools	1		
	*Facial recognition search across databases* Need to develop a system to search across multiple mug shot databases and other photo databases at the federal, state, and local levels	1	✓	
	*Information overload research* Need research on the impact of information overload on law enforcement, courts, and corrections personnel, as well as the causes of distractions and potential solutions	1		
	*Situational awareness tools* Need to develop technologies to provide situational awareness displays (annotated maps, "data mashups," and customized alerts) dynamically tailored to individual officers both in the field and at headquarters. Should automatically generate alerts when people of interest (such as parolees) have made contact with police. Technologies will include developing better data models	1		
	*Extracting data from reports* Need tools to extract structured data (names, addresses, phone numbers, vehicle plates, etc.) from narrative descriptions about incidents and people (such as incident descriptions in the FBI's National Data Exchange [N-DEx] program, a repository of criminal justice records)	2	✓	
	*Virtual courtrooms* Need to develop and/or assess portable courtroom video teleconferencing "kits" that judges can set up nearly anywhere (such as a public library) to alleviate travel burdens in small and rural settings	2		✓
	*Court case management* Need to further develop and evaluate integrated court case management systems (CMS) that provide case information across a large set of courtrooms (such as statewide systems). Development might be done through entirely new builds, rehabbing existing CMS, or adopting and integrating law enforcement and corrections records systems. Evaluation should include defining metrics and best practices for emerging CMS	2	✓	✓
	*Code-breaking tools* Need tools to decipher codes used by gang members and other offenders to conceal their communications. One approach might be to use natural language models	2	✓	
	*Controlling automated vehicles* Need methods for control and manipulation of automated vehicles (when warranted). For example, law enforcement may want to direct a parked vehicle to move	3		

Table 3—Continued

Community of Practice in Need	Description	Tier	Privacy Rights/ Civil Issue?	Security Issue?
Part 4: Policies, Procedures, and Guidance				
	*Technology training* Need educational materials for key web technologies, including Internet-enabled sensors and actuators, entity analytics, data life-cycle management, video conferencing, translation, and tele-education. Materials might include training, trade show presentations, and workshops	1		
	*Cost-benefit tool for technology acquisition* Need cost-benefit research to assess the return on investment on technology-related acquisitions/programs. The research should produce not only general guidance on which investments are valuable but also tools to assess specific investment options, as both are needed to help determine and communicate the value of possible technology investments	1	✓	
	*Policies and procedures for emerging technologies* Need policies, tactics, rules of engagement, and best practices for responding to emerging technologies such as IoT and Semantic Web technologies. Should address policies around the collection, storage, and transfer of data from IoT-enabled objects (cars, appliances, etc.)	1		
	*Procurement checklist for courts' IT* Need to develop procurement checklists for courts' IT, including: (1) discouraging vendor lock-in resulting from acquiring proprietary systems, (2) advance documentation of data formats and software interfaces, and (3) benchmark and performance assessments to help ensure that systems perform as expected	1		
	*Aerial drones and driverless vehicles* Need policies, tactics, rules of engagement, and best practices for responding to emerging technologies such as aerial and terrestrial automated and unmanned vehicles. This includes methods to extract data from IoT-enabled vehicles for improved accident investigation and reporting, educating practitioners on the capabilities of new technologies, friend or foe identification, locating the owner/ operator, and techniques for safe neutralization.	2	✓	
	*Security of IoT sensors* Need to examine security implications and countermeasures against the use of IoT sensors by criminals and the public to collect and publicize information on criminal justice operations (for example, tracking officer locations, identifying undercover officers)	2	✓	

Table 3—Continued

Community of Practice in Need	Description	Tier	Privacy Rights/ Civil Issue?	Security Issue?
	Part 5: Search Agents			
	*Monitoring criminals' associations* Need intelligent agents to detect criminal activity by monitoring offenders' activities and social connections (such as social network analysis)	2	✓	
	*Detecting patterns of criminal activity* Need intelligent agents to search online data for activity patterns worthy of additional attention (for example, human trafficking and money laundering)	2	✓	
	*Video analytics* Need to improve the accuracy of existing video analytic tools, to include integrating the tools with other types of sensor data to improve detection of serious events	2	✓	
	*Semantic search assessment* Need to assess existing digital evidence toolkits to determine whether semantic search tools could substantially speed up searching and analyzing digital evidence	2		
	*Analytics for social media and community feedback* Need automated analytics of social media and community board postings to assess public feedback and ambient community safety ("the community as an intelligent sensor")	2		
	*Sensor-detected crime* Need to develop and/or integrate data from audio, video, and other sensors carried by civil servants, civil fleet vehicles, and/or volunteers to identify incidents worthy of additional investigation (such as gunshots)	3	✓	
	*Sharing offender tracking data* Need research on detecting and sharing events of interest in offender tracking data. Examples include meeting with treatment providers, associating with other offenders, and being near a probation or law enforcement officer. Research should include methods for improving tracking accuracy	3	✓	
	*Semantic analysis of inmates' phone calls* Need automated audio analytics to assist with monitoring inmate communications	3	✓	

Table 3—Continued

Community of Practice in Need	Description	Tier	Privacy Rights/ Civil Issue?	Security Issue?
	Part 6: Standards			
	*Virtual criminal record catalog* Need a common criminal history record, a common catalog for storing the records, policies governing access to the records, and business processes for ensuring the records are up to date, correct, and consistent.	1	✓	✓
	*Technological infrastructure* Need technologies to support data exchange across the criminal justice enterprise. These include agreed-to data formats and Application Protocol Interfaces (APIs), a set of routines and tools for building software applications; authentication/identity management; access control mechanisms; cloud; and accessible-anywhere tools	1		
	*Tools to improve data quality and integrity* Need research on methods to enhance data quality and integrity, including provenance markings (PROV standard; integrated into NIEM), collection criteria, privacy attributes and other self-enforcing data-usage policies, use of intelligent agents for continuous data validation, and metadata matching	1	✓	✓
	*Information sharing* Need methods to better share information about offenders between corrections agencies and third parties (e.g., treatment providers and other stakeholders)	1	✓	✓
	*Common technology vocabulary and use cases* Need a core set of use cases that describes where and how criminal justice activities should be supported with IT, along with ontologies providing the "grammar" for doing so. (Here, an ontology is a formal vocabulary that describes the types, properties, and interrelationships of criminal justice concepts)	2		
	*Emergency data sharing* Need common data models and data access mechanisms that will support integrating data feeds from multiple sources (including IoT sensors from the public and private sectors) and providing the data to multiple types of stakeholders (Red Cross, etc.) in response to unanticipated needs. Should begin by considering what semantic extensions NIEM needs	2	✓	✓
	*Metadata standards for video to support semantic search* Need to determine standards ("ideals") for labeling video with metadata tags to support semantic search and analysis	2		

CONCLUSIONS: SETTING THE TECHNOLOGY AGENDA

In this concluding section, we present ways to take action on the themes and needs that can help criminal justice leverage the new web technologies.

Leveraging the New Web Technologies to Improve Information Sharing

Improving information sharing in general. As noted, both the major opportunity and major challenge is the large number of existing efforts by a variety of organizations to improve criminal justice information. The SCC has been established to

As with information sharing, a number of ongoing efforts are disseminating knowledge about technology, technology acquisition, and technology policy education and guidance efforts.

integrate the work of standards-making organizations. Indeed, one purpose of the council is to "identify high-priority standards activities that can be coordinated across standards development organizations (SDOs) for greater return on resources" (Information Sharing Environment, undated). The next step, then, would be to request that the council and its members explore how semantic technologies, as well as intelligent agents that exploit semantic tags, might be leveraged to make it much easier for developers to make criminal justice information searchable and available, while also ensuring its safeguarding (to include data quality, integrity, and security).

The top-ranked need, developing a virtual criminal history, would be a good place to start. In addition to being a highly ranked need in its own right, criminal history information frequently is used in many applications across the criminal justice enterprise, ranging from an officer in the field querying for data about a stopped driver, to a judge looking up a defendant's prior criminal history prior to a bail or bond decision, to institutional and community corrections officers using criminal history background to make risk prioritization decisions.

Better access to mug shots and other facial data. The next step here is to work with the FBI to develop standards and common policies for sharing mug-shot photos in response to queries, consistent with the FBI's larger Next Generation Identification system. A key aspect will be policies and procedures to protect against abuses, as well as to mitigate the risks of false positive identifications. The new Trustmarks (GTRI NSTIC Trustmark Pilot, undated) and other security tagging technology might be leveraged here to expedite setting up memoranda of understanding for sharing mug shots and other facial data.

Tailored situational awareness displays and reducing information overload. The next step for these needs is to explore folding web semantic tagging and intelligent agents that populate displays into existing R&D. As noted, semantic tags and intelligent agents might lead to better ways to find and display what is most relevant in various situations while hiding what is irrelevant. One way is to have a subsidiary effort, under the larger proposed SCC initiative, explore using tagged data and agents to populate situational awareness displays (also known as *dashboards* or *common operational pictures*) at multiple levels.

Developing real-time language interpretation services. The next step here is to experiment with the new commercially available services, such as Microsoft's new English-to-Spanish translation service (Warren, 2014).

Improving Practitioners' Knowledge of New Web Technologies and Their Uses

Education on web technologies in general. As with information sharing, a number of ongoing efforts are disseminating knowledge about technology, technology acquisition, and technology policy education and guidance efforts. The natural next step here is to determine which organizations (or individuals) might be called upon to develop educational material, along with model policies and checklists. As with information sharing technologies, it would be useful to start with the SCC to assess who is coordinating policy and educational efforts for these technologies. Specific technologies to focus education efforts on include

- Semantic Web technologies (and related developments, such as document databases) that specifically support finding criminal justice information (such as criminal histories), getting access to information, and translating and using information
- IoT sensor systems related to monitoring officer health and officer safety
- IoT sensor systems that could be used to maintain house arrest and other community supervision conditions

- entity analytics, which are tools that can take plain text and parse it into structured (tagged) data. This includes tools that can pull names, addresses, phone numbers, license plate tags, and email addresses out of plain text, as well as generate relationships between them (for example, details about people who live at the same address).
- video conferencing/tele-education technologies and services, to include both the tools themselves and the infrastructure and information access policies needed to support them
- civil rights, privacy rights, and cybersecurity technology issues and solutions (discussed further below)
- emerging real-time language systems (as discussed above).

The more general next step is to begin converting key technology portals from lists of disjointed materials to *learning portals*, which provide both technical developers and agencies seeking to acquire technologies with a logical series of instructional materials to get the knowledge they need. As discussed in the previous section, this process is just starting in the criminal justice information sharing area.

Policies and procedures for self-driving cars. The top-ranked need in this category—policies and procedures for self-driving cars—will need close coordination with the existing policy efforts under way by NHTSA, state departments of transportation, and others. The next step here is to designate a group from the law enforcement community to take the lead in partnering with the key stakeholders (NHTSA, California DMV, industry) to (1) develop law enforcement requirements for self-driving vehicles, (2) ensure law enforcement requirements are included both in regulations and in technical design specifications, and (3) develop policies and procedures for law enforcement personnel in dealing with self-driving cars.

Improving Infrastructure

The breakout need of the workshop was video teleconferencing with prisoners soon to be released. Related technologies supporting remote education for prisoners are sufficiently advanced to support developing and conducting field experiments on video teleconferencing links. The next step here is to designate a group from the criminal justice community to

- identify use cases and requirements for video teleconference (VTC) technology between inmates and officers and external service providers
- develop standard policies and procedures for using VTC, leveraging the information sharing safeguarding policies discussed previously
- identify and contact technology providers and funders about what might be possible to provide at what cost, and disseminate the results to the larger criminal justice community, including practitioners, developers, and funders.

The other two top needs in this area are largely technologically solved. The next step is to designate a group to identify a standard set of requirements for high-speed Internet to rural courthouses, along with standard estimated costs, which agencies then could use agencies for both planning purposes and to seek funding. The group should also pursue novel business models and support to make Internet links more affordable in rural areas.

Using IoT Sensors in Criminal Justice

Two directions of applied development and experimentation are recommended. The first is experimenting with health and safety sensor feeds—both wearable sensors and those embedded in buildings. The second is experimenting with Internet-connected sensors (and supporting Semantic Web and intelligent agents for sharing and analyzing the data feeds) to support the location and tracking of offenders under community corrections supervision. Technologically, this means experimenting in two directions. The first is on tracking systems, both wearable and contained in infrastructure, that can leverage the substantial technologies already developed. The second is on biomedical sensors, again experimenting with the substantial technologies already developed.

The breakout need of the workshop was video teleconferencing with prisoners soon to be released.

Addressing Civil Rights, Privacy Rights, and Cybersecurity Concerns

Finally, given the high concern about civil rights, privacy rights, and cybersecurity risks, there are next steps to be taken.Most important is ensuring that civil rights, privacy rights, and cybersecurity provisions are incorporated into emerging information-sharing standards, policies, and procedures that deal with the emerging web technologies. At their core, these are strategic, national-level issues that need to be inculcated throughout criminal justice development efforts. Developing a full civil rights, privacy rights, and cybersecurity strategy is well beyond the scope of this report. However, there are a few initial points:

- Note White House guidance that cybersecurity (and IT privacy rights and civil rights protections, relatedly) needs to move from being too difficult and too expensive for agencies (and other organizations) to add to their systems—they need to be built in and turned on by default (Daniel, 2015).
- The International Association of Chiefs of Police has created a general Technology Policy Framework that describes common provisions that should be part of any policies and operating procedures for new technology acquisition and use, including civil rights, privacy rights, and security protections (International Association of Chiefs of Police, 2014). This framework can be built upon for future technology development, experimentation, and fielding efforts.

Regarding intelligent agents and IoT sensors, two web technologies that were repeatedly flagged as raising special civil rights, privacy rights, and cybersecurity concerns:

- For intelligent agents supporting criminal justice decision-making about people (who should be the focus of law enforcement or community corrections scrutiny, bail/bond decisions, sentencing decisions, etc.), we recommend a study on how to ensure the quality of data used to make the decision, as well as how decisionmakers should use the agents' recommendations given realistic uncertainties and potential biases.
- For IoT sensors and search agents retrieving data across both sensor feeds and data stores, the next step is a study to develop common attributes for criminal justice policies, procedures, and required protective technologies for both sensor feed access control and cybersecurity.

For both studies, criminal justice technology experts and experts on civil rights, privacy rights, and information security should be participants.

Notes

[1] A precision immobilization technique (PIT) is a driving maneuver designed to cause a suspect's vehicle to spin out and stop.

[2] IJIS formerly stood for "Integrated Justice Information Systems." It now simply stands for IJIS.

[3] This has to do with many IEPDs being from small information-sharing efforts, in which a few agencies document the specific standards they are using to share information with each other.

Bibliography

Ahmed, Alijah, "K-Means Clustering Calculator," *SciStat Calc*, January 24, 2014. As of June 12, 2015:
http://scistatcalc.blogspot.com/2014/01/k-means-clustering-calculator.html

Bir, C., J. Cecconi, A. Dennis, M. McMullen, and C. Sloane, *Behind the Badge: Management Guidelines for Impacts to Body Armor*, National Institute of Justice, Award Number 2004-IJ-CX-K040, 2011. As of June 12, 2015:
https://www.ncjrs.gov/pdffiles1/nij/grants/233645.pdf

Braga, Anthony A., Andrew V. Papachristos, and David M. Hureau, "The Effects of Hot Spots Policing on Crime: An Updated Systematic Review and Meta-Analysis," *Justice Quarterly*, iFirst, 2012, pp. 1–31.

Contchart Software, "Outlier Tests for the Normal Distribution," ControlFreak: Control Charts for Individual Data Points, 2014. As of June 12, 2015:
http://contchart.com/outliers.aspx

Daniel, J. Michael, presentation to the 2015 Workshop on Information Sharing and Safeguarding, Reston, Va., March 26, 2015.

Foaf Project, homepage, undated. As of June 12, 2015:
http://www.foaf-project.org/

Franzen, Carl, "Google's Self-Driving Cars and Others Get Permits to Drive in California," *The Verge*, September 22, 2014. As of July 8, 2015:
http://www.theverge.com/2014/9/22/6828161/california-permits-self-driving-cars-google-audi-mercedes-benz

Gordon, John, IV, Brett Andrew Wallace, Daniel Tremblay, and John S. Hollywood, *Keeping Law Enforcement Connected: Information Technology Needs from State and Local Agencies*, Santa Monica, Calif.: RAND Corporation, TR-1165-NIJ, 2012. As of July 7, 2015:
http://www.rand.org/pubs/technical_reports/TR1165.html

GTRI NSTIC Trustmark Pilot, homepage, undated. As of June 12, 2015:
https://trustmark.gtri.gatech.edu/

Heflin, Jeff, Raphael Volz, and Jonathan Dale, eds., "Requirements for a Web Ontology Language" (working draft), World Wide Web Consortium, March 7, 2002. As of June 12, 2015:
http://www.w3.org/TR/2002/WD-webont-req-20020307/

Hollywood, John S., John E. Boon, Jr., Richard Silberglitt, Brian G. Chow, and Brian A. Jackson, *High-Priority Information Technology Needs for Law Enforcement*, Santa Monica, Calif.: RAND Corporation, RR-737-NIJ, 2015. As of June 12, 2015:
http://www.rand.org/pubs/research_reports/RR737.html

IEPD Clearinghouse, homepage, undated. As of July 7, 2015:
http://iepd.custhelp.com/

Information Sharing Environment, *Standards Coordinating Council*, undated. As of June 12, 2015:
http://www.ise.gov/standards-coordinating-council

International Association of Chiefs of Police, *Law Enforcement Priorities for Public Safety: Identifying Critical Technology Needs*, Alexandria, Va., 2005.

———, *IACP Technology Policy Framework*, January 2014. As of June 12, 2015:
http://www.theiacp.org/Portals/0/documents/pdfs/IACP%20Technology%20Policy%20Framework%20January%202014%20Final.pdf

Jackson, Brian A., Joe Russo, John S. Hollywood, Dulani Woods, Richard Silberglitt, George B. Drake, John S. Shaffer, Mikhail Zaydman, and Brian G. Chow, *Fostering Innovation in Community and Institutional Corrections: Identifying High Priority Technology and Related Needs for the United States Corrections Sector*, Santa Monica, Calif.: RAND Corporation RR-820-NIJ, 2015. As of June 12, 2015:
http://www.rand.org/pubs/research_reports/RR820.html

Kelly, Kevin, "The Next 5,000 Days of the Web," TED.com, December 2007. As of June 12, 2015:
http://www.ted.com/talks/kevin_kelly_on_the_next_5_000_days_of_the_web

Koper, Christopher S., Bruce G. Taylor, and Bruce E. Kubu, *Law Enforcement Technology Needs Assessment: Future Technologies to Address the Operational Needs of Law Enforcement*, Washington, D.C.: Police Executive Research Forum and Lockheed Martin Corporation, 2009. As of July 8, 2015:
http://www.policeforum.org/assets/docs/Free_Online_Documents/Technology/law%20enforcement%20technology%20needs%20assessment%202009.pdf

Law Enforcement Information Technology Standards Council, *Standard Functional Specifications for Law Enforcement Records Management Systems Version II*, Washington, D.C.: Bureau of Justice Assistance, 2008.

Lerman, Julie, "What the Heck Are Document Databases?" *MSDN Magazine*, November 2011. As of June 12, 2015:
https://msdn.microsoft.com/en-us/magazine/hh547103.aspx

Madrigal, Alexis C., "Meet the Regulators Trying to Make Sure Self-Driving Cars Are Safe," *The Atlantic*, May 22, 2014. As of July 8, 2015:
http://www.theatlantic.com/technology/archive/2014/05/meet-the-regulators-tasked-with-making-sure-self-driving-cars-are-safe/371352/

National Institute of Standards and Technology, "Grubbs' Test for Outliers," *e-Handbook of Statistical Methods*, 2013. As of June 12, 2015:
http://www.itl.nist.gov/div898/handbook/eda/section3/eda35h1.htm

Page, Lawrence, Sergey Brin, Rajeev Motwani, and Terry Winograd, *The PageRank Citation Ranking: Bringing Order to the Web* (working paper), Stanford InfoLab Publication Server, January 29, 1998. As of June 12, 2015:
http://ilpubs.stanford.edu:8090/422/

Project Interoperability, homepage, undated. As of June 12, 2015:
http://project-interoperability.github.io/

Schutzberg, Adena, "Ten Things You Need to Know About Indoor Positioning," *Directions Magazine*, May 6, 2013. As of June 12, 2015:
http://www.directionsmag.com/entry/10-things-you-need-to-know-about-indoor-positioning/324602

Silberglitt, Richard, Brian G. Chow, John S. Hollywood, Dulani Woods, Mikhail Zaydman, and Brian A. Jackson, *Visions of Law Enforcement Technology in the Period 2024–2034: Report of the Law Enforcement Futuring Workshop*, Santa Monica, Calif.: RAND Corporation, RR-908-NIJ, 2015. As of June 12, 2015:
http://www.rand.org/pubs/research_reports/RR908.html

Smith, Rick, "Why Is Public Safety Behind the Tech Curve?" *Police*, April 9, 2013. As of June 12, 2015:
http://www.policemag.com/blog/technology/story/2013/04/why-is-public-safety-behind-the-tech-curve.aspx

Standards Coordinating Council, *SCC Member Organizations*, undated. As of June 12, 2015:
http://www.standardscoordination.org/scc-member-organizations

Steele, Robert, and Andrew Clarke, "The Internet of Things and Next-Generation Public Health Information Systems," *Communications and Networks*, Vol. 5, No. 3B, 2013, pp. 4–9.

U.S. Department of Justice, *NIEM IEPD Clearinghouse*, 2014. As of June 12, 2015:
https://it.ojp.gov/framesets/iepd-clearinghouse-noClose.htm

Wadwha, Tarun, "Lessons from Crowdsourcing the Boston Bombing Investigation," *Forbes*, April 22, 2013. As of June 12, 2015:
http://www.forbes.com/sites/tarunwadhwa/2013/04/22/lessons-from-crowdsourcing-the-boston-marathon-bombings-investigation/

Warren, Tom, "Skype's Newest App Will Translate Your Speech in Real Time," *The Verge*, December 15, 2014. As of June 12, 2015:
http://www.theverge.com/2014/12/15/7393665/skype-translator-features

Wu, Xindong, Vipin Kumar, J. Ross Quinlan, Joydeep Ghosh, Qiang Yang, Hiroshi Motoda, Geoffrey J. McLachlan, Angus Ng, Bing Liu, Philip S. Yu, Zhi-Hua Zhou, Michael Steinbach, David J. Hand, and Dan Steinberg, "Top 10 Algorithms in Data Mining," *Knowledge and Information Systems*, Volume 14, No. 1, December 2007, pp. 1–37.

Acknowledgments

The authors would like to acknowledge the participation and assistance of the panelists of the Web 3.0+ Criminal Justice Workshop. We would also like to acknowledge the contributions of William Ford and Steve Schuetz of the National Institute of Justice. The authors also acknowledge the valuable contributions of the two peer reviewers of the report, Edward Balkovich and John Davis, both of RAND.

The RAND Safety and Justice Program

The research reported here was conducted in the RAND Safety and Justice Program, which addresses all aspects of public safety and the criminal justice system, including violence, policing, corrections, courts and criminal law, substance abuse, occupational safety, and public integrity. Program research is supported by government agencies, foundations, and the private sector. This program is part of RAND Justice, Infrastructure, and Environment, a division of the RAND Corporation dedicated to improving policy and decisionmaking in a wide range of policy domains, including civil and criminal justice, infrastructure protection and homeland security, transportation and energy policy, and environmental and natural resource policy. Questions or comments about this report should be sent to the project leader, Brian A. Jackson (Brian_Jackson@rand.org). For more information about the Safety and Justice Program, see www.rand.org/safety-justice or contact the director at sj@rand.org.

About the Authors

John S. Hollywood is a senior operations researcher at the RAND Corporation and a professor of policy analysis at Pardee RAND Graduate School. His principal focus is information systems research in support of improving security, ranging from crime prevention to terrorism prevention to improving combat effectiveness. His recent research projects have included examinations of predictive policing, high priority information technology needs for law enforcement, and U.S. effectiveness at foiling terror plots.

Dulani Woods is a data science practitioner adept at data acquisition, transformation, visualization, and analysis. He has a master's degree in agricultural economics (applied economics) from Purdue University. His master's thesis was an economic analysis of organic and conventional agriculture using the Rodale Institute's Farming Systems Trial. He began his career as a Coast Guard Officer on afloat and ashore assignments in Miami, Fla.; New London, Conn.; and Baltimore, Md.

Richard Silberglitt, senior physical scientist at the RAND Corporation, has worked in academia, government, and private industry for more than 40 years, performing, evaluating, and managing research in materials, energy, nanotechnology, and other advanced technology areas. He has lectured widely on emerging technologies in the United States and Asia, and he served as chairman of the International Advisory Board of the APEC Center for Technology Foresight, in Bangkok, Thailand.

Brian A. Jackson is a senior physical scientist at the RAND Corporation and director of the RAND Safety and Justice Program. His research focuses on criminal justice, homeland security, and terrorism preparedness. His areas of examination have included safety management in large-scale emergency response operations, the equipment and technology needs of criminal justice agencies and emergency responders, and the design of preparedness exercises.

About This Report

On behalf of the U.S. Department of Justice, National Institute of Justice (NIJ), the RAND Corporation, in partnership with the Police Executive Research Forum (PERF), RTI International, and the University of Denver, is carrying out a research effort to assess and prioritize technology and related needs across the criminal justice community. This initiative is a component of the National Law Enforcement and Corrections Technology Center (NLECTC) System and is intended to support innovation within the criminal justice enterprise.

This report is one product of that effort. It presents the results of the Web 3.0+ Criminal Justice Needs Workshop, a group convened in September 2014 as part of the NIJ/NLECTC Priority Criminal Justice Needs Initiative to identify and prioritize future criminal justice technology needs on emerging Internet technologies such as linked data, Semantic Web, intelligent agents, and the Internet of Things. This report and the results it presents should be of interest to planners from law enforcement departments, corrections agencies, and courts; research and operational criminal justice agencies at the federal level; private-sector technology providers; and policymakers active in the criminal justice field.

NIJ | National Institute of Justice
STRENGTHEN SCIENCE. ADVANCE JUSTICE.

This publication was made possible by Award Number 2013-MU-CX-K003, awarded by the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, and conclusions or recommendations expressed in this publication are those of the author(s) and do not necessarily reflect those of the Department of Justice.

Limited Print and Electronic Distribution Rights

www.rand.org

RAND CORPORATION

The RAND Corporation is a research organization that develops solutions to public policy challenges to help make communities throughout the world safer and more secure, healthier and more prosperous. RAND is nonprofit, nonpartisan, and committed to the public interest.

RAND's publications do not necessarily reflect the opinions of its research clients and sponsors. **RAND**® is a registered trademark.

RR-928-NIJ