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

Future-Proofing Justice

Building a Research Agenda to Address the Effects of Technological Change on the Protection of Constitutional Rights

Brian A. Jackson, Duren Banks, Dulani Woods, Justin C. Dawson

Key Findings

- Panelists convened to craft a research agenda to ensure that advances in technology inside and outside the criminal justice system do not adversely affect the protection of individuals' constitutional rights and identified a variety of needs for the near and longer terms.
- Shifts in technology and in how individuals integrate devices into their lives—and, in some cases, into their bodies for medical or human-augmenting technologies—call into question traditional ways of viewing data collected and used in criminal justice processes.
- The largest number of needs identified by the panel focused on educating participants in the criminal justice system on the implications of technological change and how to enable the adversarial process to better take on complex technical questions.
- The top priorities of the panel included requirements for best practice and training development, addressing such issues as criminal justice data quality and its implications for individuals' rights; evaluation work to better understand how analytic tools (such as risk assessment instruments) perform; and fundamental research on such topics as how the exploding volume of electronic data could affect the protection of rights.

As changes occur in society, fitting the effects of those changes into existing legal structures and practices is not always smooth. When changes are gradual, law and precedent have time to react, using analogies to earlier situations or cases to build and understand how today's world might differ from the world in which those precedents were set. When changes are sudden, however, thinking through how to address them can be tougher, and large-scale shifts can make it difficult to navigate the present based solely on analogies to the past. Shifts in technology—in which new innovations can produce rapid differences in what is possible—can create these types of challenges.

As part of a multiyear research effort sponsored by and supporting the National Institute of Justice, the Priority Criminal Justice Needs Initiative has focused on identifying innovations in technology, policy, and practice that would be beneficial to the U.S. criminal justice sector. To do so, we convened expert panels and held other structured discussions with practitioners from law enforcement, courts, and corrections. During these discussions, practitioners identified changes in technology or new ways of doing things that might save money or enhance performance but also flagged innovations that might threaten the ideals that the criminal justice system is charged with protecting.

An example that arose more than once in discussions with court practitioners was virtual presence. Teleconferencing has evolved from an expensive technology transmitting low-quality images to a technology so cheap that it is included as a standard feature in most new mobile communication devices. Today, on higher-end professional systems, a person can appear life size and at high enough resolution that a viewer can read facial expressions and body language. In the future, virtual reality

> "In some cases, virtual confrontations fall short of face-to-face confrontation because of limitations on the ability to gauge the witness's demeanor. This is a key fact to determining a witness's credibility."
>
> – Panel Member

devices likely will make it possible for someone who is hundreds of miles away to seem within arm's reach, an illusion of proximity so good that both people might forget that what is being whispered between them privately is not traveling the virtual inch between their mouths and ears but actually is being carried through miles of cables or fiber optic lines. Virtual presence can save money—by limiting transportation of the accused between jail and court, allowing more-efficient use of time by expert witnesses, or cutting visits to jails by lawyers to speak with their clients. But is virtual "good enough?" Can the face-to-face confrontation guaranteed by the Sixth Amendment be fulfilled when the witness is on a computer monitor rather than in the witness chair? Can a public defender build the relationship she needs to effectively represent her client if the first time they physically sit next to each other or shake hands is at the defense table in court? Will a defendant get a fair hearing when he appears on screen in front of a jail camera rather than neatly dressed next to his lawyer?

Even for a technology as seemingly simple as videoconferencing, the answers to these questions are not obvious. And today's technology environment is replete with other examples that are even more complicated. Today, citizens commit a seemingly ever-expanding volume of data to their mobile devices and smartphones, some knowingly and some captured without their knowledge. Events entangling smartphones and crime have already raised questions about appropriate surveillance and reasonable search and seizure, and the questions could become more complex as citizens entrust more of their lives to the technologies they use. And it is unlikely that future technologies will be simpler. As technologies become more integrated into people physically—from implanted medical devices that record and transmit data to human-augmenting technologies surgically implanted to provide capabilities we lack on our own—the line between a technology and a person will continue to blur. If a citizen cannot be forced to testify against herself, it follows that information to support her prosecution could not be involuntarily read directly from her brain—should technology allow such a capability in the future. But if technologies are sufficiently integrated into a person, at what point does it become compelled self-incrimination or an unreasonable search to extract data from those devices? The correct answer to such questions is not obvious, but what is clear is that simple analogies between new and old technologies are likely not enough to understand their implications. For example, it might be easy to make an analogy between an electronic calendar on a smartphone and a desk datebook, but when that smartphone records more and more data or is an integral part of a system of medical devices that the person cannot set aside, thinking of it as a diary or telephone seems a weak analogy at best.

To help inform thinking by government, technology developers and innovators, the legal profession and courts, and citizens at large about how technological change could affect the rights of individuals in the criminal justice system, we wanted to explore the breadth of this issue in an effort to get in front of these challenges. In the process, we identified technologies that are already outpacing the simple analogies we use to understand the implications for protecting individuals' constitutional rights.

A FOCUS ON PROTECTING INDIVIDUALS' RIGHTS IN THE CRIMINAL JUSTICE SYSTEM

Our initial focus for this report was on how technology affected the fairness and justice of the criminal justice system, with a particular focus on the courts. Procedural due process within the court system is aimed at ensuring that the law is administered fairly and uniformly. Procedural due process places restrictions on and requirements for government power over individuals during criminal proceedings. Such restrictions and requirements reflect constitutional principles limiting the government's exercise of power and are designed to protect the rights of all participants in the legal process by requiring all levels of government to apply uniform rules of practice and procedure.

In all elements of due process is the underlying tenet of fairness—that the application of law to individual cases must be consistent and not biased by extra-legal factors, such as a defendant's race or income. Additional elements of procedural due process (originating in the Fourth, Fifth, Sixth, Eighth, and 14th Amendments of the Constitution) include the presumption of innocence—which usually means the right to be free, pending the outcome of the charges (i.e., be offered reasonable bail)—and the rights against self-incrimination and compelled testimony.

Although we initially focused on the processes that happen once a citizen is formally charged, we found it difficult to maintain that narrow scope. Given the role of the courts in regulating the actions of other arms of the justice system—for example, balancing the powers of law enforcement through the issuance of warrants and determining the length and nature of punishment for an individual in the correctional system—our focus broadened to explore questions of how technological change might affect the protection of individuals' rights in the larger criminal justice context. This required a significant expansion to address concepts of privacy, surveillance, search, and seizure. As a result, the effort presented in this report sought to explore this wider landscape, looking at the effects of technologies that are emerging today and that are on the horizon and asking what we need to know to either address the technologies' negative effects or capture their potential benefits for protecting individuals' rights in the criminal justice system.

VARIED NEW TECHNOLOGIES, VARIED POTENTIAL EFFECTS

Technological changes, both inside and outside the courtroom, have the potential to affect individuals' constitutional rights and the protection of those rights via due process, and technologies that are available now are already raising important questions. Given current trends, technological changes in communication and information technology in particular have produced devices with capabilities to collect, record, store, transmit, and display data in a variety of ways.

Inside the courtroom, technological advancements could both hinder and support procedural due process and rights protection. Technology is available now to facilitate communication between defendants and their attorneys, to allow remote interpretation for litigants that do not understand English, and to more quickly and securely access evidence (see, for example, Lederer, 2004a, 2004b; Jackson et al., 2016). And although discussion and consideration of these technologies often focuses on how they can save tax dollars by making the court system more efficient, they may also reduce citizens' legal costs and lower the practical barrier that socioeconomic status can represent. Furthermore, electronic record systems allow for a more complete record of court proceedings that are backed up and therefore less susceptible to loss. These systems can also make public access to court proceedings easier. Furthermore, technology is available to provide legal support and other resources to assist pro se litigants (those choosing to represent themselves). But technology may make it more difficult to protect defendants' rights as well (National Center for State Courts [NCSC], undated-b). Already, courts have seen problems with jurors using their mobile electronic devices to do their own legal or case research during trials, potentially introducing biases and defeating the protections put in place for introducing evidence in legal proceedings (e.g., Brayer, 2016). Mobile devices have been used to photograph witnesses and, through social media systems, intimidate individuals to shape trial outcomes (Davis, 2013).

As discussed earlier in the context of virtual presence, when it comes to protecting individuals' rights, a single technology may produce positive effects, negative effects, or both. For example, significant effort has been devoted to developing risk assessment models that seek to predict the likelihood that an individual will fail to appear at his or her trial or will commit crimes in the future (see Simon, 2005). In the pretrial context, tools that identify defendants who are very likely to appear could make it easier for judges to release them (including setting lower bail amounts), limiting the infringement of their freedom before trial—and saving the government the cost of holding them.[1] To the extent that such tools make decisions more consistent across different judges, they increase fairness and help ensure equal protection of all citizens under the law. However, because such tools generalize from the characteristics of groups to make their predictions about individuals, the nature of the predictive models and what characteristics are used can incorporate bias into decisions. And if that is the case, the consistency in decisionmaking does not increase fairness but instead results in systematic bias in the justice system. For example, if—as a result of bias—police officers are more likely to arrest individuals from a minority group rather than release them with a warning, then predictions of future offenses that rely on past arrest may magnify that bias even if the model itself does not use race as a predictor (see, for example,

Data & Civil Rights, 2015; Angwin et al, 2016; and Barry-Jester, Casselman, and Goldstein, 2015).

Technological advancements outside the courtroom could affect individuals' rights and their interactions with the criminal justice system more broadly. For example, in recent years, there has been controversy over the collection of information on individuals' online activities and physical movements—via vehicle-tracking devices or databases that accumulate information on where and when a car with a specific license plate appears—and what legal requirements (e.g., probable cause, a warrant) should be met when gathering, storing, or using such data (see, for example, Hermann, 2015; Trottier, 2014). New technologies and encryption of personal devices have given rise to questions about whether law enforcement can access such information and compel third parties to assist in investigations. These issues raise substantive rights questions, including the line between public safety and private interest and how the capabilities that new technologies provide government might begin to affect individual behavior and infringe on freedoms protecting expression, association, and political action (see Kaminski and Witnov, 2015).

To move beyond these contemporary examples, we developed a framework for thinking through the implications of technology for protecting individuals' rights in their interactions with the criminal justice system. We defined categories of technologies that appeared to be useful for considering the implications of the data they produce and capabilities they might provide to the justice system. Our considerations included both how voluntary an individual's interaction with the technology might be and how much knowledge and control the person might have over the data or capability that the technology produced. We examined two sets of technologies—those potentially used inside the courtroom (a relatively well-defined class of technologies) and the much broader set of commercial and societal technologies whose proliferation and use could shape the data and information available to criminal justice processes.

> "Players within the criminal justice system must develop an understanding of the technologies, their use and misuse, and how to properly address them in order to ensure that defendants' rights are not violated."
>
> – Panel Member

Looking first at **courtroom technologies**, the areas of interest ranged from devices or techniques for accessing, analyzing, and presenting data (e.g., tools for processing "big data" data sets and, as we have already introduced, virtual reality tools for case presentation, prediction, and virtual presence) to technologies related to recording in the court (e.g., by citizens or court participants, as well as by court representatives capturing the official court record that is needed to support appeals and case review).

Looking at technological change more broadly, we started at the level of an individual person and examined **body-integrated technologies**, which include instances in which it is difficult or impossible for a technology to perform its functions if an individual puts it aside or separates from it. Such instances include tools that are used to track activity for health reasons, as well as technologies that are literally integrated into the human body, such as pacemakers and insulin-delivery devices. Today, such implanted technologies are used for medical reasons, but in the future, human-augmenting technologies for nonmedical purposes may become more widespread.

From there, we defined a class of **carried devices**. The current analog for this category is a smartphone, tablet, or other such device that individuals can separate themselves from at any time (even if they might not want to), and it is assumed that the owner can maintain more control over the data stored by such devices than by body-integrated devices. However, technology companies (e.g., smartphone or software developers) can adjust policies on how data are collected, used, and distributed, which could increasingly limit such personal control over data in the future. Indeed, some firms' entire business models rely on wresting data about individuals from their control in order to sell the information—for example, for delivering targeted advertising or building customer profiles for commercial purposes.

Next, we identified **personal computing devices**, defined to capture desktop and laptop computers, gaming consoles, and other systems that have greatly increased in storage capacity and, because of their connection to the Internet, can transmit data to others (e.g., cloud storage providers, gaming networks), potentially "leak" data if they are hacked, or host others' data (whether consensually through peer-to-peer sharing models or nonconsensually as a result of hacking).

The fifth category is **home-integrated and household technologies**, such as smart homes, smart televisions, and other Internet-of-Things devices. Such technologies have the potential to collect data within the most private of spaces and to do so with varying degrees of owner knowledge and consent. In a private home, it would be the owner's decision to install a smart security system that might capture video, activity, and other data within the home or to purchase a smart television whose voice activation features meant that the device's microphone was essentially always on and transmitting audio to distant servers for voice-recognition processing. In an apartment complex, however, the renter might have less control over whether or what types of devices are installed in the building.

Analogous to home-integrated technologies are **vehicle-integrated technologies**, incorporating the increasing levels of sensing and recording technology being built into modern automobiles. Although movement toward autonomous vehicles may greatly expand the number of sensors, computing power, and ability to record data built into each vehicle, vehicles already connect to networks via cellular infrastructure (e.g., assist systems that allow occupants to call for help), record driving behavior (e.g., on-board computers or devices added for insurance purposes), and sense the areas around them (e.g., vehicle-mounted cameras and sensors for assisted driving or parking). Individuals may have control over the technologies that are integrated into their own vehicles, but changes in the vehicle ecosystem (e.g., requirements associated with increasing numbers of autonomous vehicles on the road) may mean that some types of sensing and data recording become standard elements of all "road ready" vehicles. These devices create challenges for protecting rights because they touch on how an individual's movements could reveal sensitive personal information (e.g., visits to a medical clinic or political gathering), as well as how such rights as free assembly might be affected if all vehicles other than the most basic (e.g., bicycles, feet) record data on where the vehicle went and when.

Finally, we defined a class of the wider **societal technology ecosystem** to capture the fact that sensors are being installed

> "[Inappropriate use of social media is] a true problem that strikes at the heart of our justice process. I fear education and harsh penalties may be the only means to address the issue."
>
> – Panel Member

in a wide variety of public places—not just by government but by private property owners—for security and other purposes. The more common such devices become, the more difficult it becomes to move about and interact in the public sphere without being—at least in theory—monitored and recorded. As such technologies are applied in commercial spaces, individuals may also have little choice but to interact with them in the course of work activities. Although practical concerns (such as the limits on how much video can be stored and the labor involved in actually watching it) may constrain such monitoring now, advances in video analytics and falling storage costs might mean that more video data will be catalogued and stored in the future. Although broad recording might negatively affect individuals' rights, the proliferation of cameras could mean that there are always many "technological witnesses" to individual events (e.g., a shooting incident captured from multiple angles by security cameras nearby), which could help to protect individuals' rights by better informing court processes—as long as citizens have the same access to such footage to inform their defense as police and prosecutors have when building a case. While individuals can control whether they purchase a smartphone, citizens have little or no control over the societal technology ecosystem, and they must accept this facet of technological change if they wish to continue to move and interact within the changing society.

Table 1 summarizes these seven technology categories with examples and key issues posed.

Table 1. Technology Classes, Examples, and Issues

Category	Examples	Key Issues

Courtroom technologies	• Devices to access, analyze, and present data
	  ○ Capability of counsel to analyze large volumes of case-relevant data
	  ○ Connectivity, communication, and data access from mobile devices during court proceedings
	  ○ Presentation technologies, including simulations, holographic reconstructions of crime scenes, and virtual reality tools
	• Forecasting and prediction tools, including pretrial and sentencing risk assessments
	• Virtual presence
	  ○ Teleconferencing for lawyer-client discussion or depositions
	  ○ Virtual presence in court proceedings (from today's screen-based tools to future holographic videoconferencing)
	• Recording in the court
	  ○ Cameras used by citizens
	  ○ Body-worn cameras on court personnel
	  ○ Preparation of the court record for technology-heavy cases, evidence, and in-court argument
		• Technologies in the courtroom already raise concerns about the following:
		  ○ fairness (e.g., in analytic tools)
		  ○ influence (e.g., whether virtual simulations might influence juries beyond the facts of the case)
		  ○ effectiveness (e.g., whether virtual presence meets justice objectives as well as face-to-face interactions do)
		  ○ appropriateness (e.g., whether techniques for making a court record capture the proceedings well enough when visual and other tools are used in hearings that may be hard to capture in a written transcript).

Body-integrated technologies	• Fitness trackers (e.g., smart watches) • Medical devices (e.g., network-connected pacemakers and insulin pumps) • Future implanted human-augmentation technologies	• Such technologies collect data on individuals' locations, activities, and environments, potentially without their awareness. • An individual may not have the option of deactivating or removing an implanted device.
Carried devices	• Mobile phones, smartphones, and tablet devices • Body-worn cameras (by both citizens and criminal justice practitioners)	• Individual apps on carried devices use cameras, microphones, positioning, and other capabilities to collect a wide variety of data on individuals' location, activities, communications, associates, data access, and so on, often without their knowledge and sometimes without their consent. Such features as voice command may mean that audio monitoring is always active. • Integration of carried devices into basic processes—payments, work processes, etc.—may limit the feasibility of individuals to not carry such devices. • Ubiquity of cameras may mean that video of an incident is available from many points of view. • Business models of technology companies may make data difficult to access in criminal justice processes, and access may differ for government (e.g., prosecution) and criminal defense entities.

Table 1—Continued

Category	Examples	Key Issues
Personal computing devices	• Desktop computers, laptop computers, gaming consoles, and other network-connected devices with increasing amounts of storage, including cloud-based storage and services	• Increasing volumes of data are stored on devices, where case-relevant data may be deeply intermingled with irrelevant data and information on other people. • The policies for some services and websites can involve individuals ceding some control of the functioning and content on their systems without full understanding of the implications of doing so. • Ensuring the integrity of data on electronic devices and systems in light of cyber and other threats is a concern.
Home-integrated and household technologies	• Web-enabled intelligent thermostats • Next-generation web-connected home security systems • "Smart" appliances (e.g., televisions and voice-controlled personal assistants)	• Devices integrate monitoring technology into intimate areas of the home, potentially without individuals' (e.g., purchasers, other occupants, and visitors) knowledge or understanding. • Technologies (e.g., voice-command systems) may monitor constantly and send data to external businesses' systems for analysis.
Vehicle-integrated technologies	• Connected car technologies (e.g., turn-by-turn navigation, remote diagnostics, in-vehicle security, emergency-contact systems) • Vehicle "black boxes" that capture driving behavior data (can be integrated into vehicle or added voluntarily for insurance purposes) • Future connectivity of vehicles to the Internet for access to data or capabilities	• Such technologies collect and record position, behavior, and other data—including audio for voice-activated devices—on vehicle use and occupants. • Connectivity of vehicles to external networks creates potential data integrity concerns. External hacking of the vehicle (or an allegation as such) could raise questions about driver responsibility.

Societal technology ecosystem	• Sensors and cameras being broadly installed in many locations for security and other purposes
	  ○ "Inward-looking sensors"—used in commercial or professional settings where only a subset of the population (e.g., employees, subcontractors, and customers) will be monitored as a result of access control, safety, or security technologies
	  ○ "Outward-looking sensors"—used in public settings where data may be collected on any member of the public that is nearby (e.g., traditional security cameras in commercial settings)
		• Technologies may collect data that are limited (e.g., access control logs) or expansive (e.g., real-time audio and video).
		• For any given incident, there may be tens or even hundreds of nearby data streams that could pose logistical challenges for evidence collection, analysis, and retention for both initial proceedings and appeals.

METHODOLOGY

To explore the intersection of emerging technologies and the protection of individual rights and due process in the criminal justice system, the National Institute of Justice asked the RAND Corporation and RTI International to assemble an expert panel of practitioners, legal scholars, and thinkers about technology and individual rights. The end goal is to frame a research agenda focused on getting ahead of related concerns or potential benefits—by shaping the development of technology (e.g., its features or applications), developing training or tools for criminal justice practitioners, educating the public, and exploring other approaches to use technology to advance the protection of individual rights and due process within the justice system. Through searches of published documents and recommendations from various organizations, we identified a set of candidates and convened a panel of 13 participants from those invitees. The list of participants and their organizations is included at right.

Before the meeting date, we sent panel members a background document and pre-workshop questionnaire that drew on the research team's review of published literature on these issues. The materials were structured using different categories of rights—the right against self-incrimination, to confront witnesses, to effective assistance of counsel, to a speedy trial, to presumption of innocence, and to an unbiased tribunal—with some additional issues related to evidence, the court record, and other technologies of interest to the panel. (The complete questionnaire is available in an electronic appendix to this report.) In each category, we asked whether specific technologies raised concerns and more-general questions about the implications—positive and negative—of emerging technologies (described earlier in Table 1) for the rights at issue.

The results from the questionnaire informed the agenda for the panel discussion; for example, we used specific points raised by the respondents to both kick off and inform discussion moderation. The discussion explored each category of rights and the implications of various emerging technologies. From this discussion, the moderating team identified individual *needs*—a term we have used in our related work to signify specific requirements tied to either solving a problem or taking advantage of an opportunity for better performance in the justice system. Because of the nature of the topic, much of the focus of this workshop was on basic research needs—including collection of data, analysis, and development of resources—rather than on the development of new technologies or practices.

From the discussion, the panel identified 37 needs, each related to a specific challenge or opportunity that new tech-

Panel Members

Ahunanya U. Anga
Associate Professor
Thurgood Marshall School of Law, Texas Southern University

Justin Fitzsimmons
Program Manager
SEARCH Group

David Gray
Professor
Francis King Carey School of Law, University of Maryland

Greg Hurley, Esq.
Senior Knowledge Management Analyst
National Center for State Courts

Jennifer Lynch
Senior Staff Attorney
Electronic Frontier Foundation

Patrick Muscat
Assistant Prosecuting Attorney
Wayne County Prosecutor's Office

Paul Ohm
Professor
Georgetown College of Law, Georgetown University

Jill Paperno
Second Assistant Public Defender
Monroe County Public Defender's Office, Rochester, N.Y.

Anjanette Raymond
Assistant Professor
Kelley School of Business, Indiana University

David Robinson
Principal
Upturn

Scott Shackelford
Assistant Professor
Kelley School of Business, Indiana University

Mark Shlifka
Executive Assistant State's Attorney
Cook County State's Attorney's Office

Pedram Tabibi
Attorney, Meltzer, Lippe, Goldstein & Breitstone, LLP
Associate Professor, St. John's University School of Law

Michael Trickey
Judge
Court of Appeals, Washington State

nologies present for the protection of individuals' rights. To provide structure to the set of identified needs, we asked the panel members to rank each need based on its expected benefit (how important they thought it would be if the need was met) and the probability of success of actually meeting the need. We multiplied those two ratings to produce an *expected-value* score, reflecting the value of meeting the need weighted by the likelihood of success. We used these scores to cluster the needs into three tiers, from the highest scoring (Tier 1) to the lowest (Tier 3). The best thresholds to split the tiers were identified by a clustering algorithm that mathematically minimizes differences between different assignments of needs to the groups.

We showed the panel the distributions of the initial scores that each need received for importance and probability of success to highlight areas of consensus and disagreement, and panel members then had the opportunity to re-score the needs based on the discussion, if desired. These second-round results were used to raise or lower the expected-value scores from the first round (weighted by the number of participants who had rated a need, because not all did so for each need). In some cases, the new scores changed what ranking tier the need was assigned. More-detailed discussion of the methodology—including contributors to the nonresponse in the second round of rankings and how we adapted the ranking method to address the nonresponse—is available in the electronic appendix to this document.

This process produced a prioritized list of needs for research in this area, broken into groups from high to low priority. We must acknowledge that—as with all subjective assessments involving a limited number of participants—the needs identified and the priorities assigned to them are reflective of the members of the panel. Although the panel process sought to ensure that discussion touched on issues related to each of the categories of rights that had been covered in the panel background document and questionnaire, the amount of discussion in each part of the workshop and the needs identified were determined by the panel participants. We sought to build a broad and representative group of panelists, but it is likely that a different group would produce somewhat different results.

KEY THEMES

The panel's deliberations and discussions identified a variety of issues and corresponding needs for research aimed at either better understanding the effects of current and emerging technologies on the protection of individuals' constitutional rights or preparing the criminal justice system to address the effects of those technologies going forward. As described previously, the panel identified 37 distinct needs, and we present the full, comprehensive list in the appendix at the end of this report. But to facilitate discussion on the range of needs that were identified, the research team also identified five key overarching themes.[2] Although the workshop was framed to explore both challenges and opportunities that new technologies present to the protection of individuals' rights, the greatest focus in our discussion related to concerns and new complexities raised for criminal justice. Here, we discuss each of the five themes and present the needs that the panel identified in each. We introduce each section with a fictitious vignette that illustrates how emerging technologies may complicate individuals' rights in the criminal justice process.

1. Are You *Really* Sure? Issues of Data and Analytic Quality for Just Decisions

Mr. Andrews has been charged with assault against Officer Franklin, and he does not dispute the assault. However, defense counsel questions the circumstances that led to the confrontation.

Defense attorney: *Your Honor, what precipitated this terrible situation was the assumption—the mistaken assumption—that my client was a gang member. Officer Franklin has testified that when he searched the police database for my client, a gang flag came up, so he responded to my client very aggressively.*

So, I went back to see where that gang flag came from. Three years ago, a patrol officer in another jurisdiction interviewed a man named Jonathan Jefferson. My client was with him. It turns out Mr. Jefferson was not a good guy—and was a gang member. But then the algorithms in that department's computers went to work, and my client first became tagged as a "known gang associate." And through a set of calculations that are honestly not entirely clear to me, at some point, "known associate" transformed into a "gang member flag" on my client's record. And because our department recently joined the Northern Law Enforcement Data Sharing System, when Officer Franklin searched my client's name, that department's flag popped up here.

Before so much data got entered into databases, the fact that Mr. Andrews was seen with Mr. Jefferson would have just been a note jotted in some officer's field notebook. When my client didn't have any contact with

police afterward, that notebook would have eventually gone into a desk drawer and been forgotten. But today, that note lived on in the police database and festered, transforming into the trigger for an incident that didn't need to happen at all. I am sorry that Officer Franklin got hurt, but blaming my client for an injury that occurred when the officer was tossing an innocent man to the ground doesn't seem like justice.

Using data and information to inform criminal justice decisionmaking and improve performance has become a central focus in contemporary justice policy for many years. For example, intelligence-led policing and the management process CompStat were developed to help make law enforcement more effective at addressing community problems and responding more effectively to deter and solve crimes when they occur, and these initiatives are now broadly accepted in many departments (Police Executive Research Forum, 2013; Ratcliffe, 2016). As alluded to in the introduction, the use of data about individuals to assess risk in court and corrections contexts—for example, the risk that an individual might not show up to his appointed court date before trial and the risk that he will reoffend after release from prison or during community supervision—is viewed as a promising practice to reduce the high costs of the justice system and potentially better serve the needs of individuals that come in contact with it (Simon, 2005).

Capturing such data in criminal justice information systems—to provide the foundation for such analytic strategies—has also been a policy priority for more than a decade. Transitioning to digital storage means the possibility of transitioning from a world in which "searching" meant a detective flipping through a notebook or a file clerk sorting through stacks of paper files to one in which an intelligent software agent can scour thousands of pages not just for the specific file sought but for other relevant data that might help crack a case or explain an offender's past behavior. As criminal justice data have been moved to electronic forms, sharing across jurisdictional boundaries has become more widespread (though is still challenging in some instances), which has further broadened the volume of data to support analysis (see Jackson, 2014, and references therein).

While applying data to help make better decisions seems simple enough, improvement only follows if the data being used are good. Concerns about the quality of data captured in criminal justice systems are not new. As far back as the 1980s—an era of information technology far less advanced than today—questions were raised about errors in the data recorded by justice agencies and the potential impact on individuals' rights (Laudon, 1986; Beskind, 1985). Such concerns have persisted, emphasizing that the advances in technology over the past three decades have not eliminated the problem (Pepper, Petrie, and Sullivan, 2010; Logan and Ferguson, 2016). While much of the concern in the literature is about data that are objectively wrong—for example, incorrect recording of crimes or charges ascribed to an individual—other concerns about the quality of data can arise that are less clear. For example, if an investigator records notes with uncertain judgments and that information then becomes codified as more-certain-seeming data points in a data system, that is a form of inaccuracy. This can occur as data are divorced from their original context—as in the vignette that introduced this theme, in which a person being seen with a gang member led to the conclusion that he was also a gang member.[3] With data-sharing, inaccuracy can travel—because of either objective inaccuracy from data-entry errors or more-subjective inaccuracy from how uncertain information is recorded.[4] And when data are copied and ingested into many separate data sets, inaccuracy can then multiply and become hard to fix.

Other trends in technology and society have further increased the volume of information available to the criminal justice system—sometimes so much that the volume becomes a burden. The amount of information stored on individual electronic devices means that investigation and prosecution teams may find themselves dealing with hundreds of gigabytes or even terabytes of data, particularly in complex cases involving many individuals or organizations. Although recording so much data may be useful for establishing guilt, innocence, liability, and so on, the processes for reviewing, understanding, processing, and presenting large volumes of information in investigations and court proceedings are time-consuming and expensive. And in a world in which information systems are vulnerable to hacking, establishing the quality and provenance of such data is necessary to ensure that the information used to inform decisionmaking is indeed what it appears to be.

The proliferation of new types of data and the rising volume of data have led to the development of analysis tools that seek to take advantage of the insights that data can provide and solve the practical challenge of managing and understanding large data sets. We have already mentioned risk assessment tools that seek to use available data to make predictions about an individual's future behavior to inform decisions (Simon, 2005). Tools for addressing data volume have been developed (e.g., predictive coding in electronic discovery) to help search through massive bodies of data and identify information related

to cases (Pace and Zakaras, 2012; Yablon and Landsman-Roos, 2013; Barry, 2013). In recent years, research efforts have been made to push these analytic and predictive capabilities further. Standing out in this field is the concept of predictive policing, which seeks to use data (about places, crimes, people, and others) to target policing activity in an effort to achieve better crime reduction (Perry et al., 2013).

Just as there are questions about *data quality*, concerns have been raised about *analytic quality* and the potential for these tools to shape decisions in ways that affect individuals' rights. Recent questions about potential racial and other biases in risk assessment tools were cited earlier (e.g., Angwin et al., 2016), but analogous questions were raised many years ago (e.g., D. Gottfredson, 1987; S. Gottfredson, 1987). Academic studies have shown that although some risk assessment tools have reasonable levels of predictive power, results from others are much less predictive, and some assessment tools show different rates of false positives and negatives for individuals of different races (see, in particular, Fass et al., 2008; Fazel et al., 2012). Analysts disagree about the implications of such different rates; some characterize the observation as a statistical inevitability given different observed recidivism rates across groups, while others suggest it demonstrates a more fundamental concern about using such tools to make decisions about individuals.[5] All analysis is tempered with the reality that such tools are intended to supplement individual human decisionmaking by judges or probation officers that could itself be affected by various biases, racial and otherwise, and that utilizes many of the same variables that provide the basis for the risk assessments (Bushway and Smith, 2007).

The main concerns regarding analytic tools, such as predictive search, focus on their accuracy—because relying on automated tools would not achieve the goals of justice if the algorithms missed key data in a case.[6] Covering a much wider range of analytic issues related to so-called big data, Joh (2016) flags concerns about how analysis of large data sets may shape the collection of additional data about individuals ("surveillance discretion," to use her term) with potentially both beneficial and troublesome effects for the protection of individuals' rights.[7]

Because applying analysis methods in criminal justice decisions can have serious consequences—potentially affecting whether individuals interact with the system at all and, if they do, shaping trial and sentencing decisions—it is essential to address the nature and accuracy of such methods. In an adversarial system, addressing these issues is partly about understanding the source of data that led to a judgment or action (as in the vignette at the opening of this section), but it is also about understanding the analytic methods that supported the judgments themselves. Just as the judgments of expert witnesses or officers of the justice system might be assessed in court proceedings by putting them on the witness stand and cross-examining them, putting an algorithm "on the witness stand" requires making data and information about how the algorithm works available to both the prosecution and defense to examine. Furthermore, issues of transparency have been raised regarding the use of new technologies and analytics by the criminal justice system and whether private proprietary concerns (i.e., a company wanting to protect the details of a tool it sells to criminal justice agencies) are getting in the way of the required transparency (Upturn, 2014). This issue has arisen not just for analytic tools (e.g., Joh, 2016, p. 40) but also for forensics techniques and data sets (e.g., National Research Council, 2009, pp. 273–274; Murphy, 2007), and even physical devices used by law enforcement for collecting data (e.g., Liebow, 2010).

During the panel's discussion related to this theme, concerns about data and analytic quality produced the largest number of needs, and all but one need fell in either the top or second tier for priority (see Box 1). Many of the needs were focused on developing better evidence to understand concerns in analytic and data-related areas, although others focused on new tools (e.g., to analyze large volumes of data) and policy or practice (e.g., to identify ways for citizens to review and correct data about themselves, to increase transparency, and to link data retention to the quality of the data). The requirements identified by the panel fell across the full life cycle of data in the criminal justice system, from collection and storage, through analysis and use, and ending with the decision to retain or not retain the data for other use.

> "There are often insufficient resources available to the defense to ensure that massive amounts of data can be fully reviewed and interpreted before trial."
> – Panel Member

Box 1. Needs Identified, Theme 1

Tier 1	• Research the implications of data volume on the ability (related to both time and resources) of the defense and prosecution to analyze and understand data so that rights are not affected simply by the scale of data produced in a case. • Assess the evidence and accuracy of risk assessment tools. • Develop best practices for assessing the quality and content of existing data sets in criminal justice agencies. • Develop best practices for data-retention policies that correspond to the importance and quality of the data. • Develop best practices for disclosing the types of data collected or used by law enforcement to support investigations and targeting. • Develop best practices for public examination and correction of risk assessment results when they are used in justice decisions and dispute errors in the source data used to perform them. • Develop semi-automated tools to tag, categorize, and analyze large volumes of data to shrink analysis timelines. • Examine how different jurisdictions are handling testimony and confrontation regarding different types of technology and the data streams they produce to move toward more-uniform treatment from court to court. Because it is not yet settled what confrontation means for data extracted from digital devices, research in this area can help clarify the issue.
Tier 2	• Develop best practices related to what level of certainty is necessary from automated algorithms for different justice system applications (e.g., probable cause, evidentiary purposes) and what confrontation means in such circumstances. • Develop best practices regarding the availability, accessibility, and timeliness of digital data to be used in proceedings. This can address concerns that data provided by third parties cannot be reviewed appropriately and that proprietary tools or algorithms are not disclosed to be challenged in court. • Develop a system for clearly communicating when a risk assessment tool is being used outside the scope of its validated purpose. This can enable review and challenge where relevant.
Tier 3	• Assess the implications of differing retention policies on digital data with respect to the statutes of limitations for different offenses.

2. My Technology, Myself: A Blurring Line Between Technology and the Person?

Police have arrested Mrs. Smith, and a detective has brought her into the police station for questioning.

Detective: *Mrs. Smith, where were you yesterday evening at 7 p.m.?*

Mrs. Smith remains silent.

Detective: *It is a shame you aren't willing to cooperate with us, but I see that you had a pacemaker implanted last year that is network-enabled so that it can send information to your doctor. We can't get the data from your doctor, but your pacemaker should tell us everything we need to know to reconstruct your location.*

A forensic specialist enters the room, carrying a device that can read the pacemaker's error codes, its maintenance data, and all of the networks it connected to for the past 96 hours.

Detective: *You may be interested in remaining silent, Mrs. Smith, but unless you left your heart at home last night, your pacemaker will tell us that you were indeed at the scene of the crime.*

Developments in modern technology, particularly the capabilities that have been built into smart devices, have made some citizens increasingly inseparable from the devices they use. As part of its periodic surveys, Cisco Systems asks professionals about their device usage and feelings, and respondents have reported strong attachments to the devices. In the 2012 survey focusing on members of Generation Y, 42 percent of respondents indicated that they "'would feel anxious, like part of them was missing' if they couldn't check their smartphones constantly" (Cisco, 2012, p. 9). Furthermore, when confronted with the (admittedly artificial) choice between having Internet access or keeping a sense of smell, more than four in ten picked the Internet.[8] Devices and the "virtual selves" that reside in them are becoming part of how people see themselves; for example, people spend money on virtual goods that exist only in online systems and see such goods as part of their effort to define their own identities (see, for example, Koles and Nagy, 2012; Nagy and Koles, 2014). Moreover, individuals' profiles and information posted on social media are becoming central to self-definition and interaction in highly connected peer groups.[9] In a Pew survey, 85 percent of the interviewees said they believed that "people get to show different sides of themselves on social media that they cannot show offline" (Lenhart

et al., 2015, p. 58), although they also indicated that what is shared on social media is "less authentic" and that some feel pressure to shape what they share so that it (and, by extension, they) will be viewed positively by their peers.

For some users, it is about not just *connecting* but *recording*. To illustrate with an extreme example, in the 2000s, a community of individuals began "lifelogging"—that is, extensively recording everything they did, where they went, their communications, their biometric measurements, and so on—supported by dedicated technologies, such as clip-on cameras that take pictures periodically. In recent years, that community has reportedly waned, although a resurgence might be enabled by improvements in data storage and tools to make sense of the data. Demonstrating how technologies blur into one another, one suggested reason for the decline in lifelogging is that the scope of data captured in social media profiles provides some of the same things sought by more-extensive recording (Elgan, 2016).

Further blurring boundaries, extensive recording data from smart devices and other platforms have become common elements for *providers* of technologies rather than their users. As a result, it is now commercial firms that have become the lifeloggers that want to use Internet browsing, communications, location data, contacts, and other streams of information for marketing and advertising purposes. It has been broadly documented that mobile applications frequently collect (and transmit) data about users (Privacy Rights Clearinghouse, 2016), in some cases for the sole purpose of assembling data that can be sold to advertisers (e.g., when applications whose functions do not require a smartphone's microphone or camera request access to those features). As a result, users may be casting a much more detailed "data shadow" of their thoughts and actions onto their devices than they know, complicating analogies between such a device and a physical diary (where an individual makes a conscious decision what to record and not record, presumably aware of the potential for those papers to be examined in the course of a duly authorized law enforcement search). Although the Supreme Court's *Riley v California* opinion did not turn on the fact that data in a cell phone may be recorded without the user's knowledge, the scope of the data in such devices and their difference from simpler paper documents (like a diary or journal) was central in the decision to deny warrantless searches of cell phone data incident to arrest (*Riley v California*, 2014).

Beyond just making it *possible* to record things—whether in a basic way via snapping photos on a mobile phone or exhaustively in the context of lifelogging—research has suggested that using these technologies has had an effect on how their users think, what information they remember, and *where* they remember it. Studies have suggested that given connectivity to extensive resources, such as the Internet, individuals become "better at recalling where to retrieve information rather than the information itself" (Loh and Kanai, 2015, p. 3). The use of devices can shape what information is retained in memory initially. Other research found that the act of externally recording events in a smart device affects how well those events are internally recorded and maintained in the memory of the person recording them (Henkel, 2014). According to one study, when participants knew that they had snapped a picture, they "put less effort into processing and remembering" what they had photographed (Loh and Kanai, 2015, p. 3). In other experiments, similar effects were shown with text data. Researchers gave participants a set of words in a computer file and asked only some in the experiment to save the file before studying a new word list. Those that saved performed *worse* at recalling words from the saved file but *better* at recalling the second word list. This suggests that the participants who performed the keystrokes to save the file had essentially delegated the task of remembering the words to the computer, freeing up their brains for the second list (Storm and Stone, 2015). This unconscious "outsourcing of memory" to technology could be viewed both as evidence for the blurring boundary between a person and a device and as support for the argument that analogies to physical objects (like diaries) may not be sufficient.

Seeking to gain a window into users' minds, other research has used the data captured from sensors and in user interactions

> "The ability to encrypt data has and will continue to provide protections against self-incrimination. We are already at a point where several programs are unbreakable."
>
> – Panel Member

> "What happens when this technology becomes so pervasive that it is on the judge, the witnesses, the jury, and the lawyers? . . . What if I can tell from a [fitness tracker] that the defense team is anxious at a key point in the trial? . . . It will be big."
>
> – Panel Member

with their smartphones to draw conclusions about internal characteristics, including a user's emotional state. Saeb and colleagues (2015) used location data and phone usage to predict whether a person suffered from depression. Muaremi, Arnrich, and Tröster (2013) used smartphone data (both with and without additional sensors) to try to measure stress in a worker population. Sensors in wearables (e.g., heart rate monitors in smart watches) could enable more-detailed inferences about such states. Other technologies being added to these platforms (e.g., sentiment analysis of text entered) are directly designed to detect a user's emotional state to shape user experiences. For example, Carter (2015) suggested using webcam data to gauge the emotional response of viewers who see Internet advertisements to help shape sales messages. Biometric data from personal fitness devices can also be analyzed to make inferences about individuals' emotions or activities. Data collected from a personal fitness tracker has already been used in court to disprove a woman's allegation that she had been sexually assaulted in her home—because her fitness tracker showed that she "had been awake and walking around the entire night, not sleeping as she had claimed" (Chauriye, 2016). Analysis of data streams related to the emotional state of an individual at the time of an alleged crime or victimization could be used in similar ways. It has even been proposed to link data recording and emotion assessment, triggering recording when physiological indicators suggest excitement or fear (Niforatos et al., 2015).

In the future, the location of such data and capability may move from devices and technologies that people carry (smartphones) or wear (fitness trackers, smart clothing) onto or even *under* their skin, with the technology becoming part of the body in a physical sense. Already, some devices implanted for medical reasons (e.g., pacemakers, cochlear implants) have varying levels of onboard data collection and processing and allow data to be accessed from outside the body.[10] Even now, some early adopters have implanted less-mainstream technologies into their bodies for a variety of purposes, including a colorblind artist who has implants that allow him to "hear color" (Vincent, 2014) and others who have implanted magnets into their fingers to allow them to interact with metal objects and sense electromagnetic fields in the environment (Popper, 2012). A variety of more-mainstream efforts to develop technologies that connect directly to the brain include tools under development at the Defense Advanced Research Projects Agency to serve as "memory prosthetics" for soldiers who have suffered traumatic brain injury (Strickland, 2014), as well as technologies intended to augment human capabilities by shaping brain function or providing capability or storage augmentation (Jacobsen, 2015; Marcus and Koch, 2014). For a human augmented with additional storage technologies inside his or her brain, the line between the technology and the person seemingly vanishes.

Constitutional rights define a clear difference between (1) information people carry in their heads, where they have a right to remain silent and cannot be compelled to bear witness against themselves, and (2) information available in their "papers and effects," which can be their thoughts, captured outside themselves, and which can be searched or seized with an appropriate warrant and probable cause. But as technologies get closer and closer to a person, and more and more deeply integrated into human experience, when do they appropriately become viewed as part of the person and no longer part of their "papers and effects?" The case of a technology that is implanted within a person would seem to cross that line and be more appropriately viewed as part of the person rather than something they own or possess. But how far beyond the skin should the line be drawn? If use of smart devices leads to changes in the way people think and causes people to store information on those devices rather than in their own brains,

does encryption of those devices take on some of the characteristics of invoking a right to remain silent and to not reveal information not just from the defendant's biological or internal brain but from the "external memory prosthetic" that he can also coincidentally use to read the news on the Internet and make phone calls? Such an analogy is imperfect, but so too is the analogy of a smartphone to a diary or day planner (which is something that is clearly open for investigatory access with probable cause) because it would have to be a magical diary that records as much data as a computer, potentially without the owner's knowledge or consent.

In our panel's discussion, five needs were identified that fell under this theme (see Box 2), including one need that was ranked top priority. As would be expected for such an emerging technology area, all of the needs focused on building a better understanding of the technologies and issues to better educate the legal system in taking on these challenging concerns.

3. Data, Data Everywhere: Mobile Access to Information, Modern Data (Over) Sharing, and the Third-Party Doctrine

Mr. Flanagan has been charged with a crime, and evidence against him includes data from the company that manages fare collection for the local bus system; prosecutors used the data to track his movements. The prosecution and defense attorneys argue to the judge whether such evidence should be admitted.

Prosecutor: *Of course the investigators didn't need a warrant to obtain Mr. Flanagan's movement history. That data came from the company that manages the Transit Online app; he provided that data to them voluntarily and so it only required a business record request to them.*

Defense attorney: *But my client couldn't use the bus system without installing that app to pay his fares, and the only way he can get to his medical appointments and the grocery store is to use the bus. He can't afford to own his own vehicle, so implying that is as voluntary as the data the phone company records so they can bill him is ridiculous.*

Prosecutor: *That doesn't change the fact that he installed the application and agreed to the data that was shared. It is still Transit Online's business record. He could have made another choice regarding how to get where he needed to go.*

Defense attorney: *He lives 5 miles from his nearest neighbor and he's been disabled since he got out of the Marine Corps. Are you suggesting he should have walked the 15 miles to the grocery store? In practical terms, his other choice was basically not to eat or go to the doctor.*

In the criminal justice system, the *third-party doctrine* governs government access to data that individuals have chosen to share with others, or as put by the Supreme Court in *Smith v Maryland*, "this court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties" (*Smith v Maryland*, 1979, p. 744). Because the court found that there is no legitimate expectation of privacy in such information, the government does not need a warrant to obtain it. As a result, for many years, warrants have not been required to access a variety of records, such as telephone billing records that show who an individual calls and the length of those calls.

But the digital age—particularly the rise of mobile computing—has led to questions about whether the third-party doctrine is still appropriate (see, for example, Villasenor, 2013).

Box 2. Needs Identified, Theme 2

Tier 1	• To aid legal consideration, build a taxonomy of new and emerging technologies and the different categories of rights they may affect.
Tier 2	• Examine the Fourth Amendment issues posed by contemporary technologies and surveillance in more depth to inform judicial decisionmaking.
Tier 3	• Conduct ethnography research on how people interact with their digital devices, the types of data that are collected, and how that interaction changes people's view of the boundary between their technologies and their selves. • Conduct research on comparisons of historical technologies and modern digital technologies. This might include a taxonomic mapping of attributes to enable easy comparison. • Research potential issues, legal restrictions, and implications of collecting personal biometric information. For example, real-time emotion or physiological data from fitness devices could provide new opportunities for attorneys to monitor juror responses to testimonies.

Digital technologies have greatly expanded the instances in which data are collected by third parties on individuals (or, in the language of the third-party doctrine, instances in which individuals share data about themselves with others) in the course of the services provided (see, for example, Solove, 2004). And while telephone billing records might reveal important and sometimes intimate details about an individual, the service records produced by today's mobile information ecosystem has the potential to be even more revealing—for example, location data that track an individual's movements to work, school, social gatherings, political activities, medical appointments, and so on; website browsing data that provide a window into what an individual is thinking about at the time; and posts to social media sites that, at least for some people, may take the place of person-to-person phone calls, capturing communication in written form that might have once been conveyed verbally in a way that was not routinely stored.[11] The revealing nature of these streams of content and metadata is the foundation of the online advertising industry, where the goal is to fuse this information in an effort to know exactly when (and, considering mobile devices, where) to deliver an advertisement to someone for a pharmaceutical, a medical provider, or any number of other products or services so that the he or she will be primed to pay attention and be influenced by the message that is delivered.

The sharing of much of these data with third parties—for example, the social media companies and Internet service providers that carry it—is certainly voluntary. A person posting something on Facebook the website certainly understands that Facebook the company will have access to what is posted. However, an individual's decision to participate in such networks and share data on them may be shaped by a variety of influences. For example, when social networks are central in interpersonal interactions, there is significant social pressure to participate and costs to choosing to opt out.[12] But there are also well-documented cases of applications available on smartphones and other devices in which the data shared with the firms involved—driven by their desire to amass data on users to sell to advertisers—calls into question what voluntary sharing truly means. Such cases have included applications that access users' location data, personal contacts, calendar, and the device microphone or camera when those features are unrelated to the task the application was performing—and although users have the option to deny such access, not all users may be aware of the collection or how to stop it.[13]

As the economy and technology continue to evolve, it is also an open question whether certain types of information collection and data-sharing will become more and more necessary and therefore more difficult for citizens to opt out of. As suggested in the vignette at the beginning of this section, ride-sharing or other transportation systems may routinely record a person's movements when providing services and appropriately billing individuals for their use. While akin to phone billing records in many respects, records that capture everywhere a person goes could reveal even more-intimate details than her communication history. To the extent that such systems become the primary transportation mode in a particular area or for a specific population (e.g., individuals who cannot afford their own vehicles), whether such information should be considered "voluntarily turned over to third parties"—and therefore meriting no privacy protection—is a legitimate question. And if such information collection and use become ubiquitous in products—for example, all automobiles are equipped with black boxes that record driving behavior and performance, or future intelligent transportation systems capture such data themselves (see Douma, Garry, and Simon, 2012)—the ability of even individuals with resources to readily opt out of data collection and sharing could disappear.[14] Other examples of products related to personal medical care raise analogous concerns. For example, an asthma inhaler has been developed that—in concert with a smartphone application—can capture location data when patients use the device. Such data would contribute to better understandings of environmental factors that trigger asthma attacks, but if such sharing is not straightforward to opt out of, it would raise similar issues about voluntary sharing for patients, given the circumstances in which they must use the device (Su et al., 2016). Questions have also been raised about the use of data if employees are forced (or even strongly encouraged) to use wearable devices in the course of their employment (Haggin, 2016).

Although not explicitly regarding the third-party doctrine, workshop discussion explored a current example that raises analogous questions of voluntary sharing and how the intersection of technology and wealth might produce differential protection of individuals' rights: In many jail or prison settings, all telephone calls through the institutional phone system are routinely recorded for security purposes (see, for example, Alameda County District Attorney's Office, 2005). While privileged attorney-client calls can be excluded from recording, data released from a large commercial provider of recording services showed that is not always implemented (Williams, 2015). An individual who is represented by a public defender may have no other option but to communicate through that

system, while a wealthier defendant may be represented by a private attorney who comes to meet in person at the facility or may be able to post bail and then freely meet with his attorney outside a custodial environment. Therefore, it is an open question whether a prisoner's acceptance of the recording should be considered wholly voluntary,[15] because the other choice would be to forgo communication with counsel, undermining the right to effective representation.

In considering both the capabilities of current mobile devices and the evolution of the full range of technologies considered in the workshop, analysis of the "digital exhaust" or virtual footprints left by individuals has the potential to provide capabilities to criminal justice agencies that before involved actions that were much more clearly invasive—and generally required warrants. For instance, access to smartphone location logs provides data similar to physical surveillance of a person or installation of a tracking device on the person's vehicle. Integrating facial recognition technology with public video sensors could similarly provide movement data that do not depend on whether someone is carrying a device. Smart appliances, such as voice-activated televisions, that have microphones that are always on and listening for commands could provide data similar to a planted listening device in the same location, and they would require only virtual access to the device through the network rather than physical access to the location. Fitness trackers or medical devices providing detailed physiological data could monitor information similar to the sensors that are part of a polygraph—but without physically connecting sensors to the person. The promise of such technologies for criminal justice is that they can enable investigations that are more effective and efficient. However, the technologies simultaneously create tension regarding how easier, and often virtual rather than physical, access to individuals, their belongings, and their homes could impinge on constitutionally protected rights. Such data might also help individuals defend themselves—using smartphone data to establish and support an alibi, for example—but doing so will depend on companies being as forthcoming to requests for data from a citizen's defense team or public defender as they are when those requests come from police or other governmental investigators.

In a world in which (over)sharing of data with third parties is becoming almost necessary to navigate commerce, employment, and social interactions, is the third-party doctrine still fair, and does it appropriately reflect society's assessment of rights in data?[16] We have focused on the potential use of such data by criminal justice agencies, but other participants in the criminal justice system could potentially use the data in ways that stress the justice process as well. In our workshop, panelists raised questions about the following:

> "Historical cell phone analysis is the DNA of the 21st century. If this evidence is available early in a case, it will lead to early plea resolution of cases. This has certainly been true with DNA and other forensic evidence."
> – Panel Member

- the use of social media information and other digital exhaust in screening jurors
- the problem of jurors using their mobile devices to do their own research during legal proceedings and, therefore, bring information into the courtroom beyond the evidence presented
- the use of social media and the ability to find and connect with people to intimidate witnesses
- the ways that even searching for individuals online might jeopardize the integrity of the legal process (for example, when a juror looks at counsel's professional social media profile, and the website automatically notifies the lawyer of the contact).

In the panel discussion, two needs within this theme rose to the top tier—fundamentally examining how the validity of the third-party doctrine may shift given the increasing requirement for disclosure of data to third parties and addressing the pressures that social media use by varied criminal justice participants can put on the process (see Box 3). Several needs fell into the second tier, largely focused on jurors' social media behavior and on mobile devices during proceedings.

Box 3. Needs Identified, Theme 3

Tier 1	• Develop model laws, courtroom policies, education, and ethical guidelines to govern appropriate social media activities. In particular, define the rules for attorneys, judges, jurors, defendants, witnesses, and others regarding connecting with each other. • Examine how the validity of the third-party doctrine may shift when societal systems are difficult to navigate without massive disclosure of data to third parties. This is especially important given that modern life necessitates individuals turning over large amounts of data about themselves to others.
Tier 2	• Create improved mechanisms (e.g., educational videos, motivational stories, signed pledges, priming tools) to inform and remind juries that the process is designed to ensure a fair trial and that outside research is a detriment to achieving that end. • Assess the costs and benefits of making government records easily available online. Online records can create adverse outcomes for some. • Assess the effectiveness of juror communication strategies to make sure jurors are informed. Jurors often do not understand the rationale for why they cannot do outside research, so they could benefit from further communications. • Develop methods for assessing or measuring the ability to potentially limit inappropriate extrajudicial research. Current approaches are of unknown effectiveness. • Measure the impact of jurors' extrajudicial research on case outcomes. The effects of such outside research during trials are currently unknown.
Tier 3	• Build tools to facilitate monitoring juror and defendant activity on social media platforms. • Conduct research and education on appropriate legal comparisons or analogies between historical or physical technologies and modern digital technologies. This might include a taxonomic mapping of the attributes of services, technologies, and technology types. This is especially important because in corrections facilities—such as jails, which are primarily populated by the poor who cannot afford bail—individuals may have no choice but to communicate via technologies that are monitored and recorded, potentially further incriminating themselves by giving new information to the government.

4. Smart (Enough) Justice: Building Justice System Expertise for Complex Technical Concerns

Mr. Jones is on trial for murdering Mrs. Davis, and evidence against him includes data from the fitness tracker that he wears as required by his health insurer. During trial, the prosecutor presents this evidence to the jury.

Prosecutor: *Based on the log data from his fitness device, we know that Mr. Jones was present at the location and was physically agitated at the time of the crime. It isn't clear what more there is to say. He was there. He was angry. And the body of Mrs. Davis was found there soon after.*

Mr. Jones's defense lawyer sits quietly, not disputing the argument.

However, the judge has recently read about errors in the locations calculated by these devices. Furthermore, she wears one too and knows from personal experience that her tracker's data on her emotional state are wrong at least one-third of the time.

Judge, to defense counsel: *Do you have any response or objection, Counselor?*

Defense attorney: *No, Your Honor. No objections.*

For the judge to act further would be outside the bounds of her role in the case, so she nods to the prosecutor to continue, and the conclusions based on the fitness tracker are not challenged.

Existing processes in the legal and court systems are designed to recognize and address the fact that ever-evolving technology changes may create tensions surrounding the protection of individuals' rights. Police collection of the extensive data available in mobile devices and the intrusion that such collection represents can be overseen by the judiciary through search warrants; a recent Supreme Court decision (*Riley v California*, 2014) established that a warrant is indeed required for such a search. At the prosecution stage, discretion in the decision to charge, indict, or seek resolution through plea bargaining provides a separate step for assessing the appropriateness of evidence and the processes through which it was collected (American Bar Association, undated). Furthermore,

the adversarial justice process and arguments made by defense counsel—whether in court or in plea bargaining—are intended to provide a mechanism to challenge evidence, its collection, and its use and to preserve defendants' rights though the process. But as the vignette opening this section suggests, the effectiveness of each of these steps—judicial control exerted in the warrant process, prosecutorial decisionmaking, and defense—depends on the knowledge of the participants that challenges should be raised at all and how to do so. And the rapid evolution of technology for collecting data and for processing it into evidence supporting court arguments challenges the ability of court participants to build and maintain the knowledge and technical expertise needed to play those roles effectively.

In today's technology environment, in which electronic data can range from relatively simple digital evidence pulled from a smartphone's browser history to an analysis of abstract measurements extracted from a fitness tracker and used to argue about a defendant's emotional state during an alleged crime, what do judges, prosecutors, and defense counsel need to know to sufficiently understand how electronic devices compile, store, and process data? When varied types of data are brought into plea negotiation or court proceedings, what documentation is required to support the admissibility of electronic evidence or to mount successful challenges to its relevance to a case? If the nation relies on the adversarial process between prosecution and defense to both advance justice and protect individuals' rights, what is the obligation to ensure that defense counsel—particularly when that counsel is an underresourced public defender representing someone without the financial means to access more knowledge or technical expertise—is not so technologically "outgunned" that the process cannot function in the way that it was designed? Given that the amount of data needed to establish the validity and reliability of measurements made by some types of technology (e.g., the accuracy of a location tracking system) can go well beyond the types of data routinely applied in criminal cases (e.g., not just data extracted from one device but also quality control and validation data from the entire system of which the device is a part), is it even reasonable to assume that these issues can be adjudicated appropriately as part of that process? The answers to these questions may have serious implications for the due process protections of individuals if electronic evidence is not appropriately developed and challenged by counsel and ruled on by an informed judiciary.

Whether the existing rules of evidence have sufficient requirements to address the sheer volume, extensive variation, and complexity associated with the many types of electronically stored information (ESI) produced by modern technological systems has been a matter of some debate. For example, Kerr (2005) argued that existing legal rules that cover the search warrant process are insufficient to effectively handle the unique aspects of ESI, stating that such applications have "caused a great deal of doctrinal confusion" (p. 85). However, there appears to be consensus among other scholars that the existing Federal Rules of Evidence are sufficient to establish legal foundations for discovery, motions, presentation, and cross-examination of ESI, if appropriately applied (see Frieden and Murray, 2011, and references therein). These principles include requirements for judiciary control over evidence collection (e.g., executing search warrants), review at the prosecution stage to determine whether the information contained in the ESI is sufficient to move the case forward, and the discovery and subsequent motions and challenges process between the prosecution and the defense.

As a result, much of the literature on due process protections related to ESI has focused on how to effectively apply the existing rules of evidence. Frieden and Murray (2011) argue that counsel should draw analogies between the source of ESI and the most similar, non-ESI or traditional source of evidence. ESI sources are more likely to involve issues of accuracy, authenticity, and therefore admissibility, but the inputs, processing, and storage of ESI are still maintained by people and must be questioned in the same way that any witness would be (Eissenstat, 2008). ESI must be authenticated just like any other evidence to determine whether it is indeed what it purports to be. If authenticity cannot be established, the evidence is irrelevant and inadmissible. Authentication includes establishing the chain of custody, corroboration, and integrity of the system used to maintain the evidence based on ESI. Pretrial preparation, particularly ESI documentation, is essential to defend any challenges to the authenticity of evidence based on such data.[17]

In federal court and in states that have adopted it, the *Daubert* standard (*Daubert v Merrell Dow Pharm*, 1993) guides the admissibility of expert testimony and has been applied to the evidence derived from ESI. Other legal scholars (see, for example, Imwinkelried, 2005) have taken requirements set forth in the *Daubert* standard and the related *Frye* test—which bases the admissibility of an expert's testimony about scientific tests or results on whether the technique used to produce the results is viewed as generally acceptable by the scientific community (arising from *Frye v United States*, 1923)—to develop a multistep

> "As technology continues to advance, this problem will keep coming up. We've seen with Stingrays that when lawyers and judges know what to look for, they can properly address the legality of the warrant or court order."[18]
>
> – Panel Member

process that can be used to support electronic evidence authentication. Depending on the type of electronic information offered into evidence, part of this process is likely to include understanding the metadata associated with the electronic evidence, and that metadata can be used to support claims of authentication, counter hearsay arguments, document the chain of custody, and otherwise support or refute the admissibility of the evidence. Electronic evidence may also require a stronger standard of admissibility when it is used to provide evidence of a claim, as opposed to illustrating a claim made through witness testimony or other offered evidence. The "best evidence" rule, which generally prioritizes original documentation over summary or conclusionary evidence, may also be applied to question whether evidence based on ESI should be admitted. However, given the massive amounts of data sometimes available for legal cases, as well as the requirement to analyze or process such evidence to make it meaningful for a case,[19] it may be impractical or impossible to present the original ESI.

The body of literature on electronic evidence means that there is guidance available to participants in the legal process regarding such data—but whether constitutional rights are being protected hinges on whether judges and counsel are sufficiently informed about ESI to appropriately and effectively apply that guidance. Such knowledge is critical to challenge the admissibility of electronic evidence resulting from poor chain of custody documentation; evidence of data tampering or hacking; overlooked data (including metadata); and poor data inputs, analytic processes, or systems (Shirk, 2007). In addition to the questions raised by the workshop panel, available literature suggests that knowledge is far from universal throughout the legal system: A study of judicial perceptions of knowledge about electronic evidence found that judges expected counsel to be the experts and to raise whatever objections are needed when litigating the admissibility of ESI (Kessler, 2010). Furthermore, the judges noted that they were largely inclined to admit electronic evidence offered by the prosecution absent any objections by the defense (Kessler, 2010), further underscoring the need for the defense bar to be educated in ESI (National Association of Criminal Defense Lawyers, 2010). Because judges need to navigate difficult legal and technological questions regarding even current technologies, this implicit expectation that counsel will educate the bench is problematic, particularly in the wake of concerns raised about forensic science more generally, the science behind currently accepted technical evidence, and the organizational systems charged with producing and safeguarding the validity of that evidence.[20]

The need for stronger knowledge in the legal system regarding such digital evidence is known, and there is no shortage of courses and opportunities for continuing legal education on such topics. For example, the National District Attorneys Association offers web-based training to apply the Fourth Amendment to electronic evidence; sample topics include how a digital device stores information, how to secure evidence housed in the cloud, use of Internet Protocol addresses in the investigative process, drafting search warrants to obtain electronic evidence, and understanding the wide range of digital devices that maintain potential evidence. Similarly, the American Bar Association offers training on understanding the legal liability associated with smart devices, the Internet of Things, government surveillance efforts, and privacy and social media. Although such training sources are available, there is scant information on how many attorneys and judges participate in these trainings, what type of cases trainees litigate or oversee, or whether the information contained in the trainings or education is applied where appropriate. Given heterogeneity across court systems, it is likely that levels of expertise vary considerably among judges, attorneys, and other judicial actors, as well as from case to case. Challenges to the admissibility of electronic evidence may be common under certain circumstances and rare under others, which can raise due process concerns. Furthermore, such challenges may more often be related to procedure as opposed to the authenticity of the evidence.[21]

Given the complexities of ESI from existing devices, the level of expertise in the legal system to address *emerging* ESI concerns is also an important unknown. Significant concern has been raised about how uncertainty in conclusions and potential biases are presented (or not presented) when traditional forensic science evidence is used in court, limiting the ability for the legal process to fully consider its quality and objectivity (National Research Council, 2009, pp. 184–186). For emerging technologies that produce data streams that may involve different types of processing and interpretation before use in court (e.g., physiological measurements from a personal medical device and sensor measurements from a network-connected home appliance), the presentation of the data for judicial review and court argument will be similarly critical, and the expertise needed to evaluate it may differ significantly from that required for current forensic science techniques.

The variability in knowledge about electronic evidence among judges and prosecution and defense counsel points to many of the needs identified by the panel. There is a need for knowledge about not only how various devices capture, maintain, and process ESI but also how existing rules of evidence and procedure can be effectively applied to protect the due process rights of defendants when ESI is considered as evidence during case preparation and litigation. The panel identified ten needs that fell within this theme, ranging from fundamental requirements for knowledge to prepare the justice system for emerging technologies to very specific training resources and educational requirements to lay the groundwork for transferring that information to current and future justice system actors (see Box 4).

Box 4. Needs Identified, Theme 4

Tier 1	• To aid legal consideration, build a taxonomy of new and emerging technologies and the different categories of rights they may affect. • Develop model laws, courtroom policies, education, and ethical guidelines to govern appropriate social media activities. In particular, define the rules for attorneys, judges, jurors, defendants, witnesses, and others regarding connecting with each other. • Develop training resources for justice system participants at all levels to question and assess the scope and nature of warrants at all parts of the process. This is especially important given the role of prosecutors and judges in issuing warrants and of defense attorneys in challenging search and seizure of new technological data. • Develop best practices and qualifications for initial and continuing education requirements to raise the level of knowledge for all justice system participants of modern electronic technologies and scientific evidence. • Examine how different jurisdictions are handling testimony and confrontation regarding different types of data and technology and the data streams they produce to move toward more-uniform treatment from court to court. Because it is not yet settled what confrontation means for data extracted from digital devices, research in this area can help clarify the issue.
Tier 2	• Develop an algorithm or checklist for steps to follow when dealing with information technology as evidence (e.g., preservation of potential evidence). Limits in knowledge among court practitioners mean that electronic evidence is not always used appropriately. • Examine the Fourth Amendment issues posed by contemporary technologies and surveillance in more depth to inform judicial decisionmaking.
Tier 3	• Develop a consensus regarding what confrontation means in different levels of virtualization—for example, immersive photographic presentations, physics-based models, and full reconstruction of events in virtual environments based on testimony rather than data. This will grow in relevance as virtual reality and simulations become more prevalent. • Create standards to quickly and transparently assess the authenticity of converted and admitted video evidence. Many processes for dealing with video data, such as rendering it for display, can change the data in subtle ways. • Research potential issues, legal restrictions, and implications of collecting personal biometric information. For example, real-time emotion or physiological data from fitness devices could provide new opportunities for attorneys to monitor juror responses to testimonies. • Build tools that better enable narrow examinations (e.g., sets of hashed file collections segregated by investigation types). This could help examiners in the criminal justice system handle the growing volume of data available from personal devices.

5. Virtual Reality, Only Virtually Just? Understanding Whether Virtual Presence, Simulation, and Immersive Presentation Advance or Hinder Justice

Mr. Williams is on trial for attacking and murdering Mrs. Rivera in an alley. Based on evidence presented during trial, the prosecution has reconstructed the crime in a virtual environment.

Prosecutor: *Ladies and Gentlemen of the jury, during this case, you have heard the evidence presented and have listened to my colleague from the public defender's office argue his theory of what happened in the alley that night. We would like to bring all of this together for you. Please put on the headsets next to each of your seats.*

The jurors put on the virtual reality headsets, which cover their eyes and ears. The reenactment begins.

Prosecutor: *What you are seeing is based on the reams of technical data the forensic lab presented. We have the victim . . .*

Mrs. Rivera appears in the simulation, walking across the street with a fearful expression on her face.

Prosecutor: *. . . and we have the defendant.*

Mr. Williams appears behind her, walking quickly.

Prosecutor: *We know from reconstruction of the camera evidence that he followed her for a block before she disappeared into the side alley where the crime was committed, never to walk out again.*

In the simulation, Mr. Williams pushes Mrs. Rivera into the alley. Some of the jurors appear tense.

Prosecutor: *We have heard the defense argue that Mr. Williams had nothing to do with pushing her into the alley. The defense claims that Mr. Williams saw and heard nothing as Mrs. Rivera was brutally attacked because he was in a hurry and listening to music on his way home. Is that credible to you? Standing where you are, hearing what you are hearing?*

The simulation takes the jurors in front of the entryway to the darkened alley, and ominous music plays in their ears. A woman screams, and the simulation goes dark. The jurors remove their headsets.

Prosecutor: *The prosecution rests.*

Some of the jurors appear visibly unnerved by what they just experienced. The public defender then picks up a legal pad to begin his more traditional oral summation for the case.

Whether it is appropriate to use technology to present information in court proceedings has been an enduring question as available technologies and tools have continued to evolve over time. Over the decades, the questions have focused on the use of video and other photographic technologies in court (Williams et al., 1975), videoconferencing for appearance of detained defendants or remote witness testimony (also know as video presence or virtual presence) (Johnson and Wiggins, 2006), and simulations of crimes or crime scenes (Dunn, Salovey, and Feigenson, 2006). New visual technology has the potential to both enhance and impede protection of a defendant's due process rights; therefore, judges and attorneys must consider and balance those implications with the emerging expectations of the public for technology to facilitate efficient case processing and the presentation of complete and compelling information at trial.

As introduced in the beginning of this report, remote appearances and videoconferencing are being adopted in court systems—even while questions remain about their effects. We saw these differences of view among our panel members, as illustrated in two panelists' comments on the next page. Video appearances are used in courtrooms throughout the country for hearings that are presumed to not affect the outcome of a case, such as hearings to determine bail, waive right to a jury trial, receive a jury verdict, enter a plea, sentence a defendant, and conduct post-conviction and parole reviews (Babcock and Johansen, 2011). For these types of hearings, remote appearances may protect the rights of the defendants by affording swifter access to justice than would be possible if the hearing were conducted in person. However, questions remain about whether appearances and testimony through videoconferencing systems impede or support a defendant's rights to confront witnesses, to effective assistance of counsel, and to an unbiased and fair tribunal, and whether such appearances have the same effects as in-person appearances (see, for example, Johnson and Wiggins, 2006).

Review of the use of videoconferencing technology in court cases has resulted in mixed results. *Wilkins v Wilkinsin* (2002) held that remote appearances in parole revocation hearings violate a defendant's right to be present at all matters during the adjudication of his case. State courts have held that other types of hearings, such as those to determine bail or to

enter a plea, can be conducted with the defendant appearing via videoconference (Babcock and Johansen, 2011). However, questions remain about whether defendants take the proceedings as seriously as they might if they were actually in court; whether judges and attorneys present in the courtroom treat the defendant the same as they would if he were physically present; and whether the defendant has sufficient access to counsel prior to, during, and following remote appearances (Terry, Johnson, and Thompson, 2010). As a result, many caution against any use of remote appearances for detained inmates beyond hearings that might otherwise be delayed if an in-person appearance were required. But what that standard means in practice could shift over time if underinvestment in the court system means that the availability of physical facilities for proceedings and hearings does not keep up with increases in demand.[22] The American Bar Association standards identify a preference for in-person court appearances whenever possible.

Research on the impact of appearing via videoconference on the outcomes of bail hearings has also produced varied results. Videoconferencing was identified as a successful method for conducting interviews and bail hearings in Canada with incarcerated individuals based on the finding that bail outcomes were not different for defendants appearing remotely compared with those who appeared in person (R.A. Malatest and Associates Ltd., 2010). However, another study conducted in Cook County, Illinois, found that felony defendants appearing via videoconference experienced a 51-percent increase in the average bond amount set at the bail hearing during the study period, which was significantly greater than the 13-percent increase in bond amount experienced by the control group of felony defendants who appeared in person for bail hearings (Diamond et al., 2010). Research on the use of remote video appearances for immigration hearings found that individuals appearing remotely were more likely to be deported but no less likely to have their claims denied by a judge (Eagly, 2015). This finding was explained by evidence showing that detainees appearing remotely were less likely to retain counsel, apply to remain lawfully in the United States, or seek an immigration benefit known as voluntary departure. Other studies have found that it is harder for the defense and other court advocates to communicate before and during hearings when the defendant appears via videoconference and that the rate of defense representation was lower in virtual courts where defendants appear remotely (Terry, Johnson, and Thompson, 2010). These processes led to differential outcomes in the rate of guilty pleas and custodial sentences for remote appearances compared with traditional, in-person appearances.

For cases that proceed to trial, concerns have been raised about defendants' constitutional right to confront witnesses who offer testimony via videoconference. The U.S. Supreme

"Increased use of telepresence deprives a defendant of the right of confrontation and can dilute the effectiveness of direct examination, cross-examination, and other courtroom processes." – Panel Member

"In an era of digital communication and instant access, remote technology can find a place in the courtroom setting. Routine status dates are great examples. Hearings and trials will depend on the nature of the evidence." – Panel Member

Court has weighed in on this issue, although justices disagreed about the appropriateness of the practice. (Justice Antonin Scalia memorably wrote, "Virtual confrontation might be sufficient to protect virtual constitutional rights; I doubt whether it is sufficient to protect real ones" [Scalia, 2002].) Despite some findings that remote testimony of character witnesses in criminal cases did not affect case outcomes (Lederer, 2009), other studies suggest that it may be difficult for a judge or jury to determine a witness's demeanor when testimony is provided through videoconference (Babcock and Johansen, 2011; Bailenson et al., 2011), which can be exacerbated by technical issues, such as an audio delay (Abraham et al., 2008). Other remote testimony simulations have demonstrated that in-person testimony was rated as more believable and honest by mock jurors (Johnson and Wiggins, 2006) and that emotion level was more difficult to gauge for witnesses appearing via remote videoconference (Havener, 2014).

While videoconferencing for defendant appearances and witness testimony is already happening in courtrooms throughout the country, innovators are developing technologies that push further into virtual space, and these might be used in courtrooms in the future. For instance, advances in technology are under way to support more-realistic virtual representations of individuals not in the courtroom, to illustrate testimony, and to provide evidence. Such advances could help address some concerns regarding current telepresence technologies by increasingly making virtual and in-person meetings indistinguishable from each other (Edwards, 2011). Virtual reality or more-immersive technologies could create the illusion that an individual is present when she is not. Such technology includes robot avatars and three-dimensional representations. The ability of such technology to make remote locations and individuals feel truly present is currently limited by cost, existing Internet connection speeds, and display resolution limits (Bailenson et al., 2006; Edwards, 2011). But if developers can access rapid enough data transmission that eliminates lag that can make interactions seem unrealistic, such technologies could address due process concerns in this area. However, doing so could raise new concerns about whether someone could interfere with the data streams to produce simple ends (e.g., disrupt a trial) or even attempt more-subtle manipulation of proceedings (e.g., add subtle distortions to the video stream to make a witness appear less truthful).

> "These new technologies are [computer graphics] on steroids. The more real and personal interpretations of evidence and testimony [are made] through these presentations, the less the ability of jurors to fairly evaluate the actual evidence."
>
> — Panel Member

A great deal of focus has been given to video presence and confrontation, but concerns also exist for the use of other virtualization in court proceedings—such as simulations that render otherwise abstract data or complex bodies of facts into consumable, even immersive, visual presentations. Studies have shown a preference for visual presentation of evidence wherever possible (Heintz, 2002), under the premise that jurors and judges retain significantly more information when they both see and hear evidence as opposed to hearing it alone (see, for example, Lederer, 1997). Studies have explored many influences on jurors that shape verdicts in cases, including attorney behavior. To the extent that use of technology shapes the jury's view of attorney competence or the strength of evidence in a case, it will shape verdicts (Wood et al., 2011). If the presentation simply reinforces the weight of already strong evidence, such effects might be a beneficial outcome; however, the concern is that some virtual representations could be so realistic that they are given greater weight by jurors than testimony that is presented only via an inherently nonvisual witness statement (Leonetti and Bailenson, 2010; Feigenson, 2006).

This concern has manifested for many years over the use of computer animations in court cases. Studies using even relatively simple animations have shown mixed effects on verdicts (Dunn, Salovey and Feigenson, 2006, and references therein; Nemeth, 2011, and references therein). With advances in video game technologies, simulation capability

has increased markedly in recent years, greatly expanding the types of animations that are possible. Presentations of forensic evidence have taken advantage of real-time video game engines to render the evidence in simulated, near-three-dimensional form, allowing types of presentation different from what is possible with photographs and other "flat" exhibits (Schofield, 2011). Experiments have also shown that the persuasiveness of visual evidence can be sufficient to induce false recall of events, emphasizing the authentication requirements for such exhibits (Wade, Green, and Nash, 2010). Current focus on development of immersive virtual reality tools for gaming will expand this capability further, meaning the technology showcased in the vignette at the opening of this section may become readily available. Tools are also in development to more readily capture data for such representations of crime scenes ("Juries 'Could Enter Virtual Crime Scenes' Following Research," 2016; Bliss, 2015). Developments in such industries are expected to reduce the costs of these types of technologies, further lowering a barrier for their use in trial contexts.

Given the persuasiveness of such immersive tools, examinations of their use have drawn distinctions between virtual presentations that use data from witness statements and those that use data from physical measurements of the scene and forensic analysis, as well as presentations used to prove a point (e.g., digital photographs, which can be enhanced or sections highlighted) and those used to illustrate testimony or other evidence already entered into the record (Eissenstat, 2008). Use of such technologies is not yet common in the criminal justice system. As it is introduced, questions of fairness and bias must be addressed if the costs or other barriers prevent some parties from using virtual representations, and therefore lacking the same visual and technologically compelling manner to present their cases.

Within this theme, the panel identified four needs that focused predominantly on telepresence—the virtual technology of today—and on how courts would need to consider more-complex virtual presentations in the future (see Box 5).

SETTING THE RESEARCH AGENDA

Given the sometimes very rapid advance of technology, the criminal justice system and its stakeholders must prepare for technology's potential to shape criminal justice functions in the future. The goal of this study was to contribute to the effort to do so by identifying research needs to understand and mitigate potentially negative effects of technology on the protection of individuals' rights and by identifying and exploring how new technologies could aid in protecting those rights. During the workshop, discussion explored technologies that already exist (for example, telepresence) and some that could be developed well into the future (e.g., human-augmenting technologies).

Looking across the top-tier needs that fell into each of the five themes, we can divide the research agenda defined by the panel's top priorities into three main groups: *best practice and training development*, *evaluation*, and broader *fundamental research* on key technology and related issues.

Best Practice and Training Development

Because key actors in the justice system—including law enforcement officers and investigators, prosecutors, defense counsel, and the judges overseeing the entire process—must understand the implications of new technol-

Box 5. Needs Identified, Theme 5

Tier 1	• Develop best practices for using telepresence (e.g., monitor size, positioning, and access to physical evidence for distant participants) in court proceedings. Society is becoming more comfortable with telepresence in situations in which traditional face-to-face discussions are typically conducted, so the public may come not only to accept but to expect telepresence capabilities. • Assess or extend existing research and best practices on appropriate use of telepresence given potential effects on the effectiveness of counsel. Defendants have a right to effective representation, and there are ongoing questions on the effect of telepresence on interactions between counsel and other court participants. • Perform robust multidisciplinary assessments to evaluate what is gained and lost when using telepresence.
Tier 3	• Develop a consensus regarding what confrontation means for different levels of virtualization—for example, immersive photographic presentations, physics-based models, and full reconstruction of events in virtual environments based on testimony rather than data. This will grow in relevance as virtual reality and simulations become more prevalent.

ogy, a significant portion of the top-tier needs addressed the development of training and best practices. Most of these needs—not unexpectedly—focused on technologies and issues that the justice system is encountering today, including best practices for

- assessments of criminal justice data quality
- data retention
- disclosure of collected data
- public examination and correction of criminal justice data
- use of telepresence
- model laws and policies for addressing social media use by criminal justice participants.

Because developing and disseminating best practices have been components of criminal justice innovation efforts for many years, a variety of such resources are available. As a result, some of the best practices identified in the workshop's research agenda are likely already available, while others still need to be developed. For example, because telepresence and video-conferencing have been used for some time already, efforts to identify best practices for that use are under way and resources have been published already (Center for Legal and Court Technology, 2014; NCSC, undated-c). The challenge that social media poses to some steps of the criminal justice system has also been recognized for some time (see, for example, Dysart and Kimbrough, 2013), and significant work has been devoted to the issue by a variety of entities. For example, survey data collection has assessed how significant a problem juror social media use is and how judges have responded (Dunn, 2011), as well as what jurors say about their use of social media during trials (St. Eve and Zuckerman, 2012; St. Eve, Burns, and Zuckerman, 2014). Substantial efforts have also been devoted to this issue by NCSC, which provides both information on social media issues writ large and a compilation of existing policies and guidelines (NCSC, undated-a). Other professional organizations (American Bar Association, 2013) and groups (Committee on Codes of Conduct, 2010) have also weighed in on the issue. The fact that these issues were raised—and rose to high priority—suggests either a need for broader adoption of existing best practices or supplementing the resources that are available.

Although best practices exist for many of the issues discussed during our workshop (e.g., criminal justice data retention and disclosure), panelists also raised concerns that do not appear to have been systematically considered to date. Central among these concerns was data quality, which the panel related to how long data should be stored (data retention), how the public should be informed about how data of different types and quality are being used, and individuals' ability to review and correct data about them in criminal justice data systems. For example, policies focused on sharing criminal justice information have considered reliability of types of data, raised the question of whether citizens should have a right to review information about them, and explored whether information quality should be tied to whether data are shared beyond the originating agency (Illinois Integrated Justice Information System, 2006).[23] Issues of data reliability and quality have also been raised for specific types of data collected by the justice system, such as social media data (see Global Justice Information Sharing Initiative, 2013), and in the context of criminal justice intelligence-sharing.[24] However, the authors are not aware of existing efforts to develop best practices or guidelines that fully capture the linkage of data quality and reliability with retention and use as articulated by the panel.

Beyond best practices, the panelists also identified needs related to educating various actors in the criminal justice system to better take on the complexities of new technologies. For example, panelists emphasized that judges need to be technologically savvy to effectively review and issue warrants, and so do defense attorneys to effectively challenge evidence in the adversarial court process. Needs identified in this area focused on better defining initial training requirements and—for practitioners in mid-career—continuing education requirements and accompanying training resources to better inform the entire justice system about technology concerns. Furthermore, resources—such as conferences, professional organizations, and outside training programs—are already available in this area, which suggests that the need is for implementation and adoption, and as a result, changes in continuing education requirements in particular could drive improvements.

Evaluation

A much smaller portion of the top-priority needs identified by the panel can be grouped together as evaluation research. One need focused on risk assessment tools, which have been a focus of significant attention in recent years because of a desire to reduce incarceration rates, especially to avoid imprisoning individuals who are likely to have a low recidivism risk. However, the assessment tools have raised concerns that they produce unfair outcomes at the individual level, particularly for members of minority groups. Evaluating such tools is challenging because they are applied in justice decisions to supplement

rather than replace human judgment, and they therefore might produce different effects as a result of the data they use, biases in the decisionmakers involved, or both.[25] Although the development of such tools has been the focus of research in criminology and related fields for many years, evaluation work to better tease out their effects is needed to ensure broader confidence in their outcomes. Both the questions raised by the panel and the recent debate about the fairness of these tools indicated a need for further work on applying them appropriately and assessing how they alter outcomes for members of different demographic, economic, and other groups.[26]

The second need that focused on evaluation was related to the use of telepresence (beyond the specific technology and other best practices that the panel indicated should be developed, already discussed earlier). The need highlighted here was to assess current best practices (and evaluate how they could be expanded appropriately) while addressing the concern that using telepresence rather than in-person meetings could reduce the effectiveness of counsel for defendants (particularly individuals defended by time-limited public defenders).

Fundamental Research

Because many of the issues discussed during the panel covered technologies that are still developing, related shortfalls in knowledge on several issues will require fundamental research to inform future decisions. The top-priority needs that fell into this category were as follows:

- To aid in legal consideration, build a taxonomy of new and emerging technologies and the different categories of rights they might affect.
- Examine how different jurisdictions are handling testimony and confrontation regarding different types of technology and the data streams they produce to move toward more-uniform treatment from court to court.
- Examine how the validity of the third-party doctrine may shift when societal systems are difficult to navigate without massive disclosure of data to third parties.
- Research the implications of data volume on the ability (related to both time and resources) of the defense and prosecution to analyze and understand it so that rights are not affected simply by the scale of data produced in a case.

By exploring key emerging ideas and challenges where there is significant uncertainty, research that is focused on these topics would also make it possible to learn from the potentially diverse ways that individual jurisdictions are wrestling with them. Such research would build on existing efforts to explore in this area (such as our workshop), ongoing legal scholarship and consideration of these issues in courts at different levels (e.g., third-party doctrine concerns), and the experience in specific events or cases. For example, there is already substantial research on issues of confrontation and video presence (see, for example, Aguiñaga, 2014; Tokson, 2007; Lederer, 2009; Weber, 2014) and how video presence may affect outcomes (Eagly, 2015), which can provide a foundation for considering confrontation in the broader scope of emerging technologies considered here.

Other needs that fall into this broader fundamental research category include work on two specific technologies. The first is telepresence, different facets of which have appeared in all three of the categories of this research agenda. While the panelists had concerns about what might be lost by using telepresence rather than in-person meetings (reflected in the needs discussed earlier), there was also a belief that we do not fully understand what the consequences of telepresence are and how they might vary in different counsel-client interactions or for different types of proceedings. The second need related to tools to provide automated assistance for analyzing large data sets; such tools could help minimize the potential for large amounts of data about a case to slow the justice process or hurt the effectiveness of client representation. This problem has been recognized for many years in civil litigation, where data volume has been a core issue in considering e-discovery in commercial and other types of cases (Pace and Zakaras, 2012). Just as a large volume of information can complicate the investigation and prosecution of a case (see, for example, Resnick, 2013), it can also create challenges for the defense (Broderick et al., 2015), increasing the workload and time required for case preparation and potentially increasing the chance that important data will be missed. Automated tools to assist with large volumes of data have been developed and evaluated for civil litigation (Grossman and Cormack, 2011; Markoff, 2011; Baron, 2011; and Byram, 2012). A variety of tools have similarly been developed for forensics and investigative applications, although fewer tools appear to be broadly available in the criminal defense context. There are commercial products that focus on data management and trial presentation assistance (as well as the software to aid in e-discovery cited previously), but few appeared to go as far as the automated analytic assistance suggested in the panel discussion.

A Closer Look at the Identified Needs—and Why Research Should Not Be Limited to the Top Tier

The prioritization process used in the workshop is designed to identify research and other needs that rise to the top of the agenda based on their perceived value and the likelihood of success. The rationale behind that filtering is to try to get the greatest benefit from research and development, focusing on important problems that will pay off if investments are made to address them. However, looking beyond the panel's top priorities, the ratings that were assigned to issues that fell below the top tier showed that—in most cases—needs fell out of the top tier not because the panel thought they were not important but because of concerns about how difficult it would be to meet the need.

Looking at the median measures of importance assigned to each of the needs that fell in Tiers 2 and 3, *none* received a median rating of less than 6 out of 9, and 13 of 21 (more than 60 percent) received a median rating of 8 or higher.[27] The majority of the non-top-tier needs that received a median rating of 8 or above made up the entirety of Tier 2—where the differentiator between Tiers 1 and 2 was the estimates of probability of success. For the Tier 2 needs, the median estimates for probability of success ranged between 5 and 6. This high ranking of importance across the full set of needs identified by the panel was very unusual compared with earlier efforts in this larger project (see, for example, Jackson et al., 2016, and references therein), suggesting that there is potentially less value in focusing just on the highest-ranked research needs in this area. As a result, the second tier can be viewed as a group of needs that the panel rated as essentially as important as the top-tier needs, but panel members felt that these issues were somewhat more difficult to solve or that the solutions were more difficult to implement.

Within that second tier, needs fell into each of the three research agenda categories, including additional needs for best practice development (relating to the use of automated algorithms, data availability for proceedings, and disclosure regarding analytics use), evaluation (of juror communication strategies), and fundamental research (assessing the costs and benefits of making court records easily available electronically, continuing to assess the Fourth Amendment issues surrounding new technologies, and measuring the effects of juror misbehavior). Needs also focused on training development, both for the public (focused on ensuring that jurors understand their responsibilities and acceptable behavior as a member of a jury) and for practitioners (with respect to digital evidence). These needs—many of which touch on extremely forward-looking technology concerns—were perceived as being very risky, but that might be a rationale to pursue research on these issues rather than a justification to shy away from doing so. Beyond simply answering the specific issues raised in each need individually, such research could contribute to the judicial system making better decisions regarding these technologies and their use. Navigating such issues as the accuracy of data from location-monitoring technologies, the meaning of biometric data from wearable or implantable devices for court cases, and appropriate analysis and application of long histories of digital footprints about individuals (stored on systems with varying degrees of security and assurance) require that judges and other court participants have the knowledge and information needed to apply the technologies in ways that appropriately preserve justice and fairness.

The second tier also included one of the two needs that fell outside the five themes described earlier. That need was to build tools and techniques to improve response rates to juror summons (which was rated 8 of 9 for importance). As was the case for other needs within the research agenda, juror nonresponse has been a concern for some time and the focus of efforts to improve communication and shape compliance through enforcement and other strategies (see, for example, NCSC, 2009a, 2009b). The fact that the central distinction between the first and second tiers of priorities was a difference in perceived likelihood of success, rather than judgments about importance, would argue for a broader research agenda in this area than focusing only on the top priorities would produce.

CONCLUSIONS

As society changes, the criminal justice system must adapt to ensure that its activities and processes are sufficient to meet the goals society depends on it to achieve. One central element of that adaptation is ensuring that justice processes protect the rights of individuals guaranteed in the Constitution. While not the only vector of change in society, technology can be a powerful force, with the potential to transform what is possible for citizens and criminal justice organizations alike.

In considering how the criminal justice system protects individuals' rights, concern often focuses on how technological change can increase the power of government compared to individual citizens. The information available on mobile

devices means that actions that law enforcement has had to take physically—such as tracking an individual's movements as part of an investigation—can potentially now be done virtually. Capabilities that are built into devices linked to the Internet of Things can—if used in particular ways—practically become wide-area sensors that would have been too costly (and likely far too controversial) for criminal justice agencies to deploy for their own purposes. Sensors that citizens choose to wear for their own reasons—such as fitness trackers and medical devices—may provide windows (if imperfect ones) into the wearer's mental or emotional state.

However, technological change has also shaped criminality, creating new challenges for justice agencies to navigate while still safeguarding individuals' rights. Just as technological change has made it possible for law enforcement to act virtually in some cases, it has also virtualized old crimes and created new electronic variations of criminal behavior. Such crime creates new requirements on the criminal justice system to build and maintain the capabilities and knowledge to address them. But it also creates new tensions, such as the recent debate about strong encryption, which can both help individuals to protect themselves (reducing such crime) and make it more difficult for law enforcement to investigate savvy criminals. The increased visibility of these technologies into individuals' lives and law enforcement's desire to access such data to solve crimes highlight the effect that citizen trust of law enforcement has in this area. The greater that trust is and the greater the use of similar technologies for maintaining public confidence in criminal justice agencies' behavior, the more access to these sorts of data citizens are likely to accept—increasing the potential for these technologies to contribute to crime prevention and response.

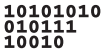
But from an individual's perspective, some of these technological shifts might create opportunities to safeguard rather than threaten the protection of individuals' constitutional rights. Mobile technologies that make individual behavior more transparent can also make the actions of individual members of government agencies more transparent, and analytics designed to mine databases looking for individual criminality might also be turned on data sets of organizational behavior to find evidence of misbehavior that would otherwise be hidden. But maintaining balance in the effects of technology on individuals' rights and protection of due process within the justice system is challenged by resource concerns. The ability of a criminal defendant to deploy big data in his own defense will balance government's ability to leverage such information in prosecution only if he has the tools available to do so.

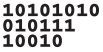
These tensions and trade-offs—some of which already exist from technologies that are available and being deployed now, and some of which may arise in the future—require the criminal justice system and its stakeholders to think ahead and prepare.

These tensions and trade-offs—some of which already exist from technologies that are available and being deployed now, and some of which may arise in the future—require the criminal justice system and its stakeholders to think ahead and prepare. Although making analogies to past technologies can be useful for thinking through future ones, doing so is unlikely to provide all the insight needed. A smartphone might look a lot like a diary, until the capabilities of the technology shift just enough that it no longer looks like one at all. This effort sought to contribute to that process of thinking ahead, laying out not just near-term needs for addressing technologies available today but also longer-term, more-fundamental research topics to provide the justice system better ways to address the challenges posed by the likely rapid shifts in information, sensing, and other technologies that will continue to occur in the future.

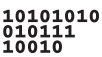
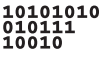
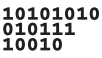
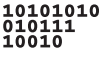
APPENDIX. COMPREHENSIVE LIST OF IDENTIFIED NEEDS

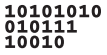
This appendix presents all of the needs identified by the panel, sorted by tier, and their associated theme(s).

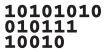
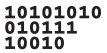
Legend	
	Are You *Really* Sure? Issues of Data and Analytic Quality for Just Decisions
	My Technology, Myself: A Blurring Line Between Technology and the Person?
	Data, Data Everywhere: Mobile Access to Information, Modern Data (Over) Sharing, and the Third-Party Doctrine
	Smart (Enough) Justice: Building Justice System Expertise for Complex Technical Concerns
	Virtual Reality, Only Virtually Just? Understanding Whether Virtual Presence, Simulation, and Immersive Presentation Advance or Hinder Justice

Problem or Opportunity	Associated Need	Tier	Related Theme(s)
Society is becoming more comfortable with telepresence in situations in which traditional face-to-face meetings are typically conducted.	Develop best practices for using telepresence (e.g., monitor size, positioning, and access to physical evidence for distant participants) in court proceedings.	1	
Digital and other new technologies blur the boundaries between traditional categories of rights (e.g., Fifth Amendment versus search and seizure concerns) that complicate assessment.	To aid legal consideration, build a taxonomy of new and emerging technologies and the different categories of rights they may affect.	1	 
Social media platforms have created opportunities for inappropriate activities, such as attorneys, judges, and jurors "friending" each other. Some media platforms (e.g., LinkedIn, Twitter) report to the user when other users follow or view their page, which is a form of monitoring and can be perceived as intimidating. Also, social media now provide outside entities with new opportunities to intimidate witnesses and jurors.	Develop model laws, courtroom policies, education, and ethical guidelines to govern appropriate social media activities.	1	 
The complexity and lack of understanding of modern technologies make it difficult for practitioners (law enforcement, prosecutors, defenders, and judges) to effectively prepare, understand, and evaluate the accuracy and appropriateness of documents that are being prepared and approved (e.g., affidavits, warrants).	Develop training resources for justice system participants at all levels to question and assess the scope and nature of warrants at all parts of the process.	1	

Problem or Opportunity	Associated Need	Tier	Related Theme(s)
Using and relying so heavily on modern technologies requires turning over significant amounts of information to third parties.	Examine how the validity of the third-party doctrine may shift when societal systems are difficult to navigate without massive disclosure of data to third parties.	1	10101010 010111 10010
The scope of relevant data in some cases, coupled with the limited resources available to the defense and prosecution, can effectively deny the ability to fully challenge the data in court proceedings. Data types in this category include but are not limited to video, audio, computer, and forensic scientific data.	Research the implications of data volume on the ability (related to both time and resources) of the defense and prosecution to analyze and understand it so that rights are not affected simply by the scale of data produced in a case.	1	
There are institutional and generational drivers toward using telepresence to augment or replace traditional in-person interactions and court proceedings.	Assess or extend existing research and best practices on the appropriate use of telepresence given potential effects on the effectiveness of counsel.	1	
The utility of risk assessments is unknown (e.g., in making bail and sentencing decisions). Specifically, such assessments may overemphasize reliance on criminal histories and negatively reinforce outcomes.	Assess the evidence and accuracy of risk assessment tools.	1	
There is insufficient breadth of knowledge in the legal community on the form and function of modern computer-based technologies, such as communication technologies and social media.	Develop best practices and qualifications for initial and continuing education requirements to raise level of knowledge for all justice system participants on modern electronic technologies and scientific evidence.	1	
Criminal justice agencies are creating, collecting, storing, and reusing data that are of questionable quality. Once recorded, such data lose their full context, often go unchallenged, and are treated as facts. In other words, low-quality data are sometimes being used for high-impact decisions.	Develop best practices for assessing the quality and content of existing data sets in criminal justice agencies.	1	
Criminal justice agencies are creating, collecting, storing, and reusing data that are of questionable quality. Once recorded, such data lose their full context, often go unchallenged, and are treated as facts. In other words, low-quality data are sometimes being used for high-impact decisions.	Develop best practices for data-retention policies that correspond to the importance and quality of the data.	1	
Criminal justice agencies are creating, collecting, storing, and reusing data that are of questionable quality. Once recorded, such data lose their full context, often go unchallenged, and are treated as facts. In other words, low-quality data are sometimes being used for high-impact decisions.	Develop best practices for disclosing the types of data collected or used by law enforcement to support investigations and targeting.	1	
The sources of data used in risk assessment tools are not fully transparent, and not all data used may be accurate. As a result, inappropriate or disproportionate governmental responses might result.	Develop best practices for public examination and correction of risk assessment results when they are used in justice decisions and dispute errors in the source data used to perform them.	1	
The scope of relevant data in some cases, coupled with limited resources available to the defense and prosecution, can effectively deny the ability to fully confront the data (in a legal sense).	Develop semi-automated tools to tag, categorize, and analyze large volumes of data to shrink analysis timelines.	1	

Problem or Opportunity	Associated Need	Tier	Related Theme(s)
It is not yet settled what confrontation means for data extracted from digital devices—for example, when location data extracted from a cell phone are the witnesses, who is the accused confronting?—and different states currently have different approaches.	Examine how different jurisdictions are handling testimony and confrontation regarding different types of technology and the data streams they produce to move toward more-uniform treatment from court to court.	1	
Society is becoming more comfortable with telepresence in situations in which traditional face-to-face meetings are typically conducted.	Perform robust multidisciplinary assessments to evaluate what is gained and lost when using telepresence.	1	
Some artificial-intelligence technologies (e.g., machine learning) have internal algorithms that cannot be fully explained by the human analysts who apply them.	Develop best practices related to what level of certainty is necessary from automated algorithms for different justice system applications (e.g., probable cause, evidentiary purposes) and what confrontation means in such circumstances.	2	
Because of the complexity or proprietary nature of the processes to assess or derive evidence through third-party vendors or labs, there is a diminished capacity to assess the authenticity and reliability of evidence.	Develop best practices regarding the availability, accessibility, and timeliness of digital data to be used in proceedings.	2	
Jurors often do not understand the reasons behind restrictions on their performing outside research related to the case they are hearing.	Create improved mechanisms (e.g., educational videos, motivational stories, signed pledges, priming tools) to inform and remind juries that the process is designed to ensure a fair trial and that outside research is a detriment to achieving that end.	2	
Online availability of court records can lead to adverse effects for some populations.	Assess the costs and benefits of making government records easily available online.	2	
Jurors often do not understand the reasons behind restrictions on their performing outside research related to the case they are hearing.	Assess the effectiveness of juror communication strategies to make sure jurors are informed.	2	
There is not a clear shared understanding of the scope of risk assessment tools and where they have been validated for use.	Develop a system for clearly communicating when a risk assessment tool is being used outside the scope of its validated purpose.	2	
There is insufficient breadth of knowledge in the legal community on the form and function of modern computer-based technologies, such as communication technologies and social media.	Develop an algorithm or checklist for steps to follow when dealing with information technology as evidence (e.g., preservation of potential evidence).	2	
The nearly ubiquitous availability of online and social media has dramatically increased the potential for inappropriate extrajudicial research by jurors and other participants in the justice system.	Develop methods for assessing or measuring the ability to potentially limit inappropriate extrajudicial research.	2	
Contemporary technologies and surveillance methods challenge existing Fourth Amendment doctrines.	Examine the Fourth Amendment issues posed by contemporary technologies and surveillance in more depth to inform judicial decisionmaking.	2	 

Problem or Opportunity	Associated Need	Tier	Related Theme(s)
Often, response rates of potential jurors to summons are quite low (less than 50 percent) and do not include a broad selection of citizens.	Highlight existing best practices, tools, and systems that can improve juror response rates and general representativeness (e.g., integrating motor vehicle records, welfare records, and follow-up programs).	2	None
The nearly ubiquitous availability of online and social media has dramatically increased the potential for inappropriate extrajudicial research by jurors and other participants in the justice system.	Measure the impact of jurors' extrajudicial research on case outcomes.	2	
Virtual simulations and event reconstructions are becoming more accessible and therefore more prevalent. When such exhibits are pre-recorded, many production and other choices are made that can significantly shape their content and message. Challenging such evidence by opposing counsel is therefore more complex than for traditional evidentiary exhibits because the effects of choices made during production many not be transparent to participants in court proceedings. These concerns suggest that existing rules of evidence (e.g., Rule 403, which allows exclusion of relevant evidence that is viewed as having too great a potential to mislead the jury or create unfair prejudice) may be insufficient.	Develop a consensus regarding what confrontation means for different levels of virtualization—for example, immersive photographic presentations, physics-based models, and full reconstruction of events in virtual environments based on testimony rather than data.	3	 
The general population is unaware of the types of information that are being recorded involuntarily by their digital devices.	Conduct ethnography research on how people interact with their digital devices, the types of data that are collected, and how that interaction changes people's views of the boundary between their technologies and their selves.	3	
Most pieces of information that are collected by personal technologies (e.g., smartphones, fitness trackers) are not compelled by the government; therefore, many of the constitutional protections against self-incrimination may not apply to data retrieved from such devices.	Conduct research on comparisons of historical technologies and modern digital technologies. This might include a taxonomic mapping of attributes to enable easy comparison.	3	
There is often a mismatch between data-retention policies and statutes of limitation.	Assess the implications of differing retention policies on digital data with respect to the statutes of limitations for different offenses.	3	
Justice processes, including preparation for court proceedings, can take significant amounts of time to bring a case to resolution.	Assess the readiness of online, kiosk, or automated systems (e.g., algorithms) for use in administering justice processes.	3	None
The upload, conversion, and redaction of outside video for use in court systems, including rendering that video to make it compatible with specific storage or display technologies, changes the original video evidence and potentially creates additional authentication burdens for its use in court proceedings.	Create standards to quickly and transparently assess the authenticity of converted and admitted video evidence.	3	

Problem or Opportunity	Associated Need	Tier	Related Theme(s)
Body-worn technologies (e.g., fitness trackers) may broadcast previously inaccessible biometric information, such as heart rate and skin temperature. This provides new opportunities for attorneys to monitor juror responses to testimony, a witness's comfort with being on the stand, and so on.	Research potential issues, legal restrictions, and implications of collecting personal biometric information.	3	
Digital forensic examiners are either unwilling or unable to limit automated examinations to narrow, warrant-defined categories of information.	Build tools that better enable narrow examinations (e.g., sets of hashed file collections segregated by investigation types).	3	
The nearly ubiquitous availability of online and social media has dramatically increased the potential for inappropriate extracurricular research by jurors and other participants in the justice system.	Build tools to facilitate monitoring juror and defendant activity on social media platforms.	3	
In corrections institutions (e.g., jails, which are primarily populated by the poor who cannot afford bail), individuals may have no choice but to communicate via technologies that are monitored and recorded, potentially further incriminating themselves by giving new information to the government.	Conduct research and education on appropriate legal comparisons or analogies between historical or physical technologies and modern digital technologies. This might include a taxonomic mapping of the attributes of services, technologies, and technology types.	3	

Theme icon credits — Getty Images, Digital Vision Vectors: filo, bubaone, Victor; iStock: Kittisak_Taramas

Notes

[1] The use of pretrial risk assessment tools is becoming more common and is replacing more-subjective approaches for making these decisions (see Mamalian, 2011). Researchers have found some evidence that these tools result in a higher rate of release of defendants pretrial (Danner, VanNostrand, and Spruance, 2015).

[2] The five themes do not capture all of the 37 identified needs, nor do all individual needs always fall cleanly into a single theme to the exclusion of the others. However, the themes do capture the essence of the discussion and the majority of the needs. Two needs did not fall into any of the themes, meaning that more than 90 percent of the identified needs could be assigned to one (in 29 cases, 78 percent of the total needs) or two (in six cases, 16 percent of the total needs) of the themes.

[3] This example was raised in the discussion during our workshop.

[4] A workshop participant made an analogy between the data held by credit reporting agencies and that held by criminal justice organizations, both of which are used to inform consequential decisions that affect individuals. In the credit context, however, provisions of the Fair Credit Reporting Act provide consumers access and procedures to dispute contents of their credit file that they believe are inaccurate.

[5] Both analysts (e.g., Verbruggen, 2016; Doleac and Stevenson, 2016) and the company that produces the proprietary risk algorithm called COMPAS (see Dieterich, Mendoza, and Brennan, 2016) have responded to the analysis by Angwin and colleagues (2016), which concluded that the technique produces biased outcomes. The fact that the algorithm at issue is proprietary came up in this discussion, where it was argued that the lack of transparency limited the ability to evaluate how the algorithm calculates its risk scores. In addition, Singh, Grann, and Fazel (2013) have raised the related concern that many risk techniques have been evaluated only by researchers related to the techniques' development, linking conflict of interest concerns to the discussion about the proprietary nature of these techniques.

[6] For example, see illustrative discussion of search methods and concerns in Bernabei and Kabat, 2015.

[7] See, in particular, discussion in Joh, 2016, pp. 28–32.

[8] Fewer were willing to trade their sense of taste to maintain Internet access, however (Cisco, 2014).

[9] In Cisco's survey results, two-thirds of respondents indicated that they spent "equal or more time online with friends than in person" (Cisco, 2012). In more-recent Pew research, text messaging dominated the modes that friends used to connect daily (Lenhart et al., 2015).

[10] Although concerns have been raised that medical devices might be hacked to cause bodily harm, the central issue for our purposes is the data that they could provide if accessed without the individual's knowledge or authorization (see, for example, Storm, 2011).

[11] The level of Fourth Amendment protection for social media content is still not fully resolved. See, for example, Murphy and Fontecilla, 2013.

[12] See, for example, discussion of Facebook in Raynes-Goldie, 2010.

[13] In an analysis done well before the broad spread of mobile smart devices, Sovern (1999) framed this issue in terms of the transaction costs involved with individuals opting out.

[14] This scenario is supported by the use of legal restrictions to prevent individuals from modifying the software even in vehicles that they own. See, for example, discussion in Wiens (2015) of initial efforts by vehicle companies to use the Digital Millennium Copyright Act to make modification of vehicle software illegal. An exemption allowing such activities was issued by the Library of Congress (which manages the exemption process for the Act) in October 2015 (see U.S. Copyright Office, 2015).

[15] The fact that the phone conversation is being recorded is traditionally disclosed in a prominent and obvious way, such as signs posted at the telephone stations.

[16] For discussion of this issue in the legal literature, see, for example, Henderson, 2006–2007; Spencer, 2013; and Kerr, 2009.

[17] Authenticating data must also consider the possibility that evidence on a person's device was not actually placed there by that person (e.g., someone with unauthorized access put it there) or is intentionally incorrect (e.g., someone falsified the digital data to make it appear that he was using a device at a location when he was actually somewhere else). For a discussion of these issues, see De Santis et al., 2011.

[18] Stingrays are surveillance devices that simulate cellular network sites so that phones in an area connect to the Stingray automatically. This allows the Stingray operator to collect identifying information about the phones and other carried devices and capture web connections, phone calls, and text messages as they pass through the simulator to the cellular network.

[19] For example, the defense or prosecution may have to process or render raw sensor data before presenting it.

[20] The National Research Council (2009) found serious shortcomings in the science behind many commonly accepted forensic practices. The report further highlighted the need for effective litigation and knowledge on the part of participants in the criminal justice system to understand and question the science and processes behind evidence based on forensics and ESI.

[21] The limited information that is available suggests that *Daubert* challenges to electronic evidence admission are rare and that knowledge to effectively apply the rules of evidence to ESI is still lacking (see, for example, Grossman, 2006; International Association of the Chiefs of Police, undated). The authentication requirement for electronic evidence in particular is not often challenged and therefore can be overlooked by courts (Grossman, 2006). However, when authentication of electronic evidence *is* raised, it appears to be the

most common source of successful challenges to the admissibility of ESI (Eissenstat, 2008).

[22] Expanding remote appearances beyond these types of hearings has the potential to result in a system that affords a different level of justice for defendants who are detained pretrial and those who have the economic resources to be released on bail or bond (Babcock and Johansen, 2011).

[23] Some of these same concerns have been raised in the context of commercial data-mining of criminal justice records (that is, when the data leave government control) (CriMNet Program Office, 2008).

[24] Per 28 C.F.R. 23, which describes criminal intelligence systems operating policies, "procedures shall provide for the periodic review of information and the destruction of any information which is misleading, obsolete or otherwise unreliable and shall require that any recipient agencies be advised of such changes which involve errors or corrections" (Code of Federal Regulations, 2015).

[25] For a discussion of this issue, see, for example, Bushway and Smith, 2007.

[26] For examples of recent debates about the tools' fairness, see discussion from a variety of perspectives in James, 2015; White House, 2015; Executive Office of the President, 2016; National Legal Aid and Defender Association, 2015; and Electronic Privacy Information Center, undated.

[27] Of the 13, 12 received a median rating of 8 and one of 8.5.

Bibliography

Abraham, H. K., H. A. Albrecht, H. J. Greanias, H. R. Byrne, J. W. Schwartz, J. J. Dolan, and H. T. Sutton, *Annual Report of the Automation and Technology Committee to the Illinois Judicial Conference*, Illinois Supreme Court, 2008.

Aguiñaga, J. Benjamin, "Confronting Confrontation in a FaceTime Generation: A Substantial Public Policy Standard to Determine the Constitutionality of Two-Way Live Video Testimony in Criminal Trials," *Louisiana Law Review*, Vol. 75, No. 1, 2014. As of December 12, 2016: http://digitalcommons.law.lsu.edu/lalrev/vol75/iss1/10

Alameda County District Attorney's Office, "Intercepting Prisoner Communications," *Point of View*, Winter 2005. As of December 12, 2016: http://le.alcoda.org/publications/point_of_view/files/IPC.pdf

American Bar Association, "Criminal Justice Section Standards: Prosecution Function," undated. As of December 12, 2016: http://www.americanbar.org/publications/criminal_justice_section_archive/crimjust_standards_pfunc_blk.html

———, "Formal Opinion 462: Judge's Use of Electronic Social Networking Media," February 21, 2013. As of December 12, 2016: http://www.americanbar.org/content/dam/aba/administrative/professional_responsibility/formal_opinion_462.authcheckdam.pdf

Angwin, Julia, Jeff Larson, Surya Mattu, and Lauren Kirchner, "Machine Bias: There's Software Used Across the Country to Predict Future Criminals. And It's Biased Against Blacks," *ProPublica*, May 23, 2016. As of December 12, 2016: https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing

Ashdown, Gerald G., and Michael A. Menzel, "The Convenience of the Guillotine? Video Proceedings in Federal Prosecutions," *Denver University Law Review*, Vol. 80, 2002–2003.

Babcock, Emily, and Kate Johansen, "Remote Justice? Expanding the Use of Interactive Video Teleconference in Minnesota Criminal Proceedings," *William Mitchell Law Review*, Vol. 37, No. 2, 2011, pp. 653–682.

Bailenson, Jeremy N., Jim Blascovich, Andrew C. Beall, and Beth Noveck, "Courtroom Applications of Virtual Environments, Immersive Virtual Environments, and Collaborative Virtual Environments," *Law and Policy*, Vol. 28, No. 2, 2006, pp. 249–270.

Baron, Jason R., "Law in the Age of Exabytes: Some Further Thoughts on 'Information Inflation' and Current Issues in E-Discovery Search," *Richmond Journal of Law and Technology*, Vol. XVII, No. 3, 2011. As of December 12, 2016: http://jolt.richmond.edu/v17i3/article9.pdf

Barry, Nicholas, "Man Versus Machine Review: The Showdown Between Hordes of Discovery Lawyers and a Computer-Utilizing Predictive-Coding Technology," *Vanderbilt Journal of Entertainment and Technology Law*, Vol. 15, No. 2, 2013, pp. 343–374.

Barry-Jester, Anna Maria, Ben Casselman, and Dana Goldstein, "Should Prison Sentences Be Based on Crimes That Haven't Been Committed Yet?" FiveThirtyEight, August 4, 2015. As of December 12, 2016: http://fivethirtyeight.com/features/prison-reform-risk-assessment/

Bernabei, Lynne, and Alan R. Kabat, "Do We Really Need Experts in This Case and When Should We Hire Them?" paper presented at the Ninth Annual Labor and Employment Law Conference, Philadelphia, Pa., November 2015. As of December 12, 2016: http://www.americanbar.org/content/dam/aba/events/labor_law/2015/november/annual/papers/99.authcheckdam.pdf

Beskind, Mark A., "Data Accuracy in Criminal Justice Information Systems: The Need for Legislation to Minimize Constitutional Harm," *Journal of Information Technology and Privacy Law*, Vol. 6, No. 4, 1985, pp. 677–723.

Bliss, Laura, "The 'Oculus Rift' and the Courtroom," *The Atlantic: Citylab*, March 17, 2015. As of December 12, 2016: http://www.citylab.com/crime/2015/03/the-oculus-rift-and-the-courtroom/385351/

Brayer, Patrick C., "The Disconnected Juror: Smart Devices and Juries and Juries in the Digital Age of Litigation," *Notre Dame Journal of Law, Ethics & Public Policy Online*, 2016. As of December 12, 2016:
http://scholarship.law.nd.edu/ndjlepp_online/5

Broderick, Sean, Donna Lee Elm, Andrew Goldsmith, John Haried, and Kiran Raj, *Criminal E-Discovery: A Pocket Guide for Judges*, Federal Judicial Center, 2015. As of December 12, 2016:
http://www.fjc.gov/public/pdf.nsf/lookup/Criminal-e-Discovery.pdf/$file/Criminal-e-Discovery.pdf

Bushway, Shawn, and Jeffery Smith, "Sentencing Using Statistical Treatment Rules: What We Don't Know Can Hurt Us," *Journal of Quantitative Criminology*, Vol. 23, No. 4, 2007, pp. 377–387.

Byram, Elle, "The Collision of the Courts and Predictive Coding: Defining Best Practices and Guidelines in Predictive Coding for Electronic Discovery," *Santa Clara High Technology Law Journal*, Vol. 29, No. 4, 2012, pp. 675–701. As of December 12, 2016:
http://digitalcommons.law.scu.edu/chtlj/vol29/iss4/4

Carter, Jamie, "How Mining Human Emotions Could Become the Next Big Thing in Tech," TechRadar, April 20, 2015. As of December 12, 2016:
http://www.techradar.com/us/news/world-of-tech/future-tech/emotional-data-from-the-likes-of-the-apple-watch-is-this-the-next-boom--1291151

Center for Legal and Court Technology, *Best Practices for Using Video Teleconferencing for Hearings and Related Proceedings*, draft report, October 8, 2014. As of December 12, 2016:
https://www.acus.gov/sites/default/files/documents/Draft_Best%2520Practices%2520Video%2520Hearings_10-09-14_1.pdf

Chauriye, Nicole, "Wearable Devices as Admissible Evidence: Technology Is Killing Our Opportunity to Lie," *Catholic University Journal of Law and Technology*, Vol. 24, No. 2, 2016, pp. 495–528. As of December 12, 2016:
http://scholarship.law.edu/cgi/viewcontent.cgi?article=1018&context=jlt

Chicago Appleseed Fund for Justice and Chicago Council of Lawyers, "Re: Proposal No. 12-01 (P.R. 0196)—Defendant's Appearance by Videoconference," letter to Supreme Court Rules Committee Secretary, November 26, 2012. As of December 12, 2016:
http://www.chicagoappleseed.org/wp-content/uploads/2012/12/Proposal-no.-12-01-P.R.-0196-Defendants-Appearance-by-Videoconference.pdf

Cisco, "Gen Y: New Dawn, for Work, Play, Identity," *Cisco Connected World Technology Report*, 2012. As of December 12, 2016:
http://www.cisco.com/c/dam/en/us/solutions/enterprise/connected-world-technology-report/2012-CCWTR-Chapter1-Global-Results.pdf

———, *2014 Cisco Connected World Technology Final Report*, 2014. As of December 12, 2016:
http://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/connected-world-technology-report/cisco-2014-connected-world-technology-report.pdf

Code of Federal Regulations, Title 28, Part 23, Criminal Intelligence systems Operating Policies, July 1, 2015.

Committee on Codes of Conduct, *Resource Packet for Developing Guidelines on Use of Social Media by Judicial Employees*, Judicial Conference of the United States, Washington, D.C.: Office of the General Counsel, April 2010. As of December 12, 2016:
http://www.uscourts.gov/file/2909/download?token=zx5S4OOE

CriMNet Program Office, *Commercial Data Mining of Criminal Justice System Records*, Delivery Team Report to the Criminal and Juvenile Justice Information Task Force, St. Paul, Minn., August 2008. As of December 12, 2016:
https://www.leg.state.mn.us/docs/2009/mandated/090200.pdf

Danner, Mona J. E., Marie VanNostrand, and Lisa M. Spruance, *Risk-Based Pretrial Release Recommendation and Supervision Guidelines: Exploring the Effect on Officer Recommendations, Judicial Decision-Making, and Pretrial Outcome*, St. Petersburg, Fla.: Luminosity, Inc., August 2015. As of December 12, 2016:
http://luminosity-solutions.com/site/wp-content/uploads/2014/02/Risk-Based-Pretrial-Guidelines-August-2015.pdf

Data & Civil Rights, "Data & Civil Rights: A New Era of Policing and Justice," web page, 2015. As of December 12, 2016:
http://www.datacivilrights.org/2015/

Daubert v Merrell Dow Pharm, 509 U.S. 579, 1993.

Davis, Kevin, "Witness Harassment Has Gone Digital, and the Justice System Is Playing Catch-Up," *ABA Journal*, 2013. As of December 12, 2016:
http://www.abajournal.com/magazine/article/witness_harassment_has_gone_digital_and_the_justice_system_is_playing_catch

De Santis, Alfredo, Aniello Castiglione, Giuseppe Cattaneo, Giancarlo De Maio, and Mario Ianulardo, "Automated Construction of a False Digital Alibi," in A M. Tjoa, Gerald Quirchmayr, Ilsun You, and Lida Xu, eds., *Availability, Reliability and Security for Business, Enterprise and Health Information Systems*, Berlin: Springer-Verlag, 2011, pp. 359–373.

Diamond, Shari Seidman, Locke E. Bowman, Manyee Wong, and Matthew M. Patton, "Efficiency and Cost: The Impact of Videoconferenced Hearings on Bail Decisions," *The Journal of Criminal Law and Criminology*, Vol. 100, No. 3, Summer 2010, pp. 869–902. As of December 12, 2016:
http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=7365&context=jclc

Dieterich, William, Christina Mendoza, and Tim Brennan, *COMPAS Risk Scales: Demonstrating Accuracy Equity and Predictive Parity: Performance of the COMPAS Risk Scales in Broward County*, Northpointe, Inc., July 8, 2016. As of December 12, 2016: https://www.documentcloud.org/documents/2998391-ProPublica-Commentary-Final-070616.html

Doleac, Jennifer L., and Megan Stevenson, "Are Criminal Risk Assessment Scores Racist?" Brookings, August 22, 2016. As of December 12, 2016: https://www.brookings.edu/blog/up-front/2016/08/22/are-criminal-risk-assessment-scores-racist/

Douma, Frank, Thomas Garry, and Stephen Simon, "ITS Personal Data Needs: How Much Do We Really Need to Know?" Minneapolis, Minn.: Intelligent Transportation Systems Institute, CTS 12-21, July 2012.

Dunn, Meghan, "Jurors' Use of Social Media During Trials and Deliberations: A Report to the Judicial Conference Committee on Court Administration and Case Management," Federal Judicial Center, November 22, 2011.

Dunn, Meghan A., Peter Salovey, and Neal Feigenson, "The Jury Persuaded (and Not): Computer Animation in the Courtroom," *Law and Policy*, Vol. 28, No. 2, 2006, pp. 228–248.

Dysart, Katie L., and Camalla M. Kimbrough, "#Justice? Social Media's Impact on the U.S. Jury System," American Bar Association, Trial Evidence Committee, August 22, 2013. As of December 12, 2016: http://apps.americanbar.org/litigation/committees/trialevidence/articles/summer2013-0813-justice-social-media-impact-us-jury-system.html

Eagly, Ingrid V., "Remote Adjudication in Immigration," *Northwestern University Law Review*, Vol. 109, No. 4, 2015, pp. 933–1020.

Edwards, John, "Telepresence: Virtual Reality in the Real World," *IEEE Signal Processing Magazine*, Vol. 28, No. 6, November 2011, pp. 9–12, 142.

Elgan, Mike, "Lifelogging Is Dead (for Now)," ComputerWorld, April 4, 2016. As of December 12, 2016: http://www.computerworld.com/article/3048497/personal-technology/lifelogging-is-dead-for-now.html

Eissenstat, Eric, "Making Sure You Can Use the ESI You Get: Pretrial Considerations Regarding Authenticity and Foundation of ESI," *Oklahoma Bar Journal*, Vol. 79, No. 7, 2008. As of December 12, 2016: http://www.okbar.org/members/BarJournal/archive2008/Mararchive08/obj797esi.aspx

Electronic Privacy Information Center, "Algorithms in the Criminal Justice System," web page, undated. As of December 12, 2016: https://epic.org/algorithmic-transparency/crim-justice/

Executive Office of the President, *Big Data: A Report on Algorithmic Systems, Opportunity, and Civil Rights*, Washington, D.C., May 2016. As of December 12, 2016: https://www.whitehouse.gov/sites/default/files/microsites/ostp/2016_0504_data_discrimination.pdf

Fass, Tracy L., Kirk Heilbrun, David Dematteo, and Ralph Fretz, "The LSI-R and the COMPAS: Validation Data on Two Risk-Needs Tools," *Criminal Justice and Behavior*, Vol. 35, No. 9, September 2008, pp. 1095–1108.

Fazel, Seena, Jay P. Singh, Hellen Doll, and Martin Grann, "Use of Risk Assessment Instruments to Predict Violence and Antisocial Behaviour in 73 Samples Involving 24,827 People: Systematic Review and Meta-Analysis," *BMJ*, Vol. 345, 2012, p. e4692.

Feigenson, Neal, "Too Real: The Future of Virtual Reality Evidence," *Law and Policy*, Vol. 28, No. 2, May 2006, pp. 271–293.

Frieden, Jonathan D., and Leigh M. Murray, "The Admissibility of Electronic Evidence Under the Federal Rules of Evidence," *Richmond Journal of Law and Technology*, Vol. XVII, No. 2, 2011.

Frye v United States, 293 F. 1013 D.C. Cir., 1923.

Global Justice Information Sharing Initiative, *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations*, February 2013. As of December 12, 2016: http://www.iacpsocialmedia.org/Portals/1/documents/SMInvestigativeGuidance.pdf

Gottfredson, Don M., "Prediction and Classification in Criminal Justice Decision Making," *Crime and Justice*, Vol. 9: *Prediction and Classification: Criminal Justice Decision Making*, 1987, pp. 1–20.

Gottfredson, Stephen D., "An Overview of Selected Methodological Issues," *Crime and Justice*, Vol. 9, *Prediction and Classification: Criminal Justice Decision Making*, 1987, pp. 21–51.

Grossman, Andrew M., "No, Don't IM Me: Instant Messaging, Authentication, and the Best Evidence Rule," *George Mason Law Review*, Vol. 13, 2006, pp. 1309–1339.

Grossman, Maura R., and Gordon V. Cormack, "Technology-Assisted Review in E-Discovery Can Be More Effective and More Efficient Than Exhaustive Manual Review," *Richmond Journal of Law and Technology*, Vol. XVII, No. 3, 2011. As of December 12, 2016: http://jolt.richmond.edu/v17i3/article11.pdf

Haggin, Patience, "How Should Companies Handle Data from Employees' Wearable Devices?" *Wall Street Journal*, May 22, 2016.

Havener, Shannon, *Effects of Videoconferencing on Perception in the Courtroom*, thesis, Tempe, Ariz.: Arizona State University, April 2014. As of August 29, 2016: https://repository.asu.edu/attachments/135164/content/Havener_asu_0010N_13889.pdf

Heintz, Michael E., "The Digital Divide and Courtroom Technology: Can David Keep Up With Goliath?" *Federal Communications Law Journal*, Vol. 54, No. 3, 2002, pp. 567–589.

Henderson, Stephen E., "Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too," *Pepperdine Law Review*, Vol. 34, 2006–2007, pp. 975–1026.

Henkel, Linda A., "Point-and-Shoot Memories: The Influence of Taking Photos on Memory for a Museum Tour," *Psychological Science*, Vol. 25, No. 2, 2014, pp. 396–402. As of December 12, 2016: http://pss.sagepub.com/content/25/2/396.full.pdf+html

Hermann, Jourdin, "The Surveillance State: Do License Plate Readers Impinge upon Americans' Civil Liberties?" *Themis: Research Journal of Justice Studies and Forensic Science*, Vol. 3, 2015. As of December 12, 2016: http://scholarworks.sjsu.edu/themis/vol3/iss1/4

Illinois Integrated Justice Information System, "Privacy Issues Confronting the Sharing of Justice Information in an Integrated Justice Environment," September 2006. As of December 12, 2016: http://www.icjia.state.il.us/iijis/public/pdf/PRV/PRV_commiteeIssues_September2006.pdf

Imwinkelried, Edward J., "Digitized Evidence," *National Law Journal*, March 7, 2005.

International Association of the Chiefs of Police, "Understanding Digital Evidence," Law Enforcement Cyber Center, undated. As of August 27, 2016: http://www.iacpcybercenter.org/investigators/digital-evidence/understanding-digital-evidence/

Jackson, Brian A., *How Do We Know What Information Sharing Is Really Worth? Exploring Methodologies to Measure the Value of Information Sharing and Fusion Efforts*, Santa Monica, Calif.: RAND Corporation, RR-380-OSD, 2014. As of December 12, 2016: http://www.rand.org/pubs/research_reports/RR380.html

Jackson, Brian A., Duren Banks, John S. Hollywood, Dulani Woods, Amanda Royal, Patrick W. Woodson, and Nicole J. Johnson, *Fostering Innovation in the U.S. Court System: Identifying High-Priority Technology and Other Needs for Improving Court Operations and Outcomes*, Santa Monica, Calif.: RAND Corporation, RR-1255-NIJ, 2016. As of December 12, 2016: http://www.rand.org/pubs/research_reports/RR1255.html

Jacobsen, Annie, "Engineering Humans for War," *The Atlantic*, September 23, 2015. As of December 12, 2016: http://www.theatlantic.com/international/archive/2015/09/military-technology-pentagon-robots/406786/

James, Nathan, *Risk and Needs Assessment in the Criminal Justice System*, Washington, D.C.: Congressional Research Service, R44087, October 13, 2015. As of December 12, 2016: https://fas.org/sgp/crs/misc/R44087.pdf

Joh, Elizabeth E., "The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing," *Harvard Law & Policy Review*, Vol. 10, 2016, pp. 15–42.

Johnson, Molly Treadway, and Elizabeth C. Wiggins, "Videoconferencing in Criminal Proceedings: Legal and Empirical Issues and Directions for Research," *Law and Policy*, Vol. 28, No. 2, 2006, pp. 211–227.

"Juries 'Could Enter Virtual Crime Scenes' Following Research," BBC News, May 24, 2016. As of December 12, 2016: http://www.bbc.com/news/uk-england-stoke-staffordshire-36363172

Kadish, Sanford H., "Methodology and Criteria in Due Process Adjudication—A Survey and Criticism," *Yale Law Journal*, Vol. 66, No. 3, 1957, pp. 319–363.

Kaminski, Margot E., and Shane Witnov, "The Conforming Effect: First Amendment Implications of Surveillance, Beyond Chilling Speech," *University of Richmond Law Review*, Vol. 49, No. 2, 2015, pp. 465–518.

Kerr, Orin S., "Search Warrants in the Era of Digital Evidence," *Mississippi Law Journal*, Vol. 75, 2005, pp. 85–145.

———, "The Case for the Third-Party Doctrine," *Michigan Law Review*, Vol. 107, No. 4, 2009, pp. 561–601.

Kessler, Gary Craig, *Judges' Awareness, Understanding, and Application of Digital Evidence*, dissertation, Davie, Fla.: Nova Southeastern University, 2010.

Koles, Bernadett, and Peter Nagy, "Virtual Customers Behind Avatars: The Relationship Between Virtual Identity and Virtual Consumption in Second Life," *Journal of Theoretical and Applied Electronic Commerce Research*, Vol. 7, No. 2, 2012, pp. 87–105.

Laudon, Kenneth C., "Data Quality and Due Process in Large Interorganizational Record Systems," *Communications of the ACM*, Vol. 29, No. 1, January 1986, pp. 4—11.

Lederer, Fredric I., "The Courtroom as a Stop on the Information Superhighway," *Reform,* No. 71, 1997, pp. 4–9. As of December 12, 2016: http://scholarship.law.wm.edu/cgi/viewcontent.cgi?article=1056&context=popular_media

———, "Some Thoughts on the Evidentiary Aspects of Technologically Presented or Produced Evidence," *Southwestern University Law Review*, Vol. 28, No. 2, 1999, pp. 389–404.

———, "Courtroom Technology: For Trial Lawyers the Future Is Now," *Criminal Justice*, Spring 2004a, pp. 14–21.

———, "The Courtroom 21 Project: Creating the Courtroom of the Twenty-First Century," *The Judges Journal*, Winter 2004b, pp. 39-43.

———, "Courtroom Technology: A Status Report," in Kamlesh N. Agarwala and Murli D. Tiwari, eds., *Electronic Judicial Resource Management*, Mumbai: MacMillan, 2005.

———, "The Legality and Practicality of Remote Witness Testimony," *The Practical Litigator*, September 2009, pp. 19–30.

Lenhart, Amanda, Aaron Smith, Monica Anderson, Maeve Duggan, and Andrew Perrin, *Teens, Technology and Friendships*, Pew Research Center, August 6, 2015. As of December 12, 2016: http://www.pewinternet.org/files/2015/08/Teens-and-Friendships-FINAL2.pdf

Leonetti, Carrie, and Jeremy Bailenson, "High-Tech View: The Use of Immersive Virtual Environments in Jury Trials," *Marquette Law Review*, Vol. 93, No. 3, 2010, pp. 1073–1120.

Liebow, David, "DWI Source Code Motions After Underdahl," *Minnesota Journal of Law, Science, and Technology*, Vol. 11, No. 2, 2010, pp. 853–875. As of December 12, 2016: http://scholarship.law.umn.edu/mjlst/vol11/iss2/15

Logan, Wayne A., and Andrew Guthrie Ferguson, "Policing Criminal Justice Data," *Minnesota Law Review*, Vol. 101, April 2016, pp. 541–616.

Loh, Kep Kee, and Ryota Kanai, "How Has the Internet Reshaped Human Cognition?" *The Neuroscientist*, 2015, pp. 1–15.

Mamalian, Cynthia A., *State of the Science of Pretrial Risk Assessment*, Pretrial Justice Institute, March 2011. As of December 12, 2016: https://www.pretrial.org/download/risk-assessment/PJI%20State%20of%20the%20Science%20Pretrial%20Risk%20Assessment%20(2011).pdf

Marcus, Gary, and Christof Koch, "The Future of Brain Implants," *Wall Street Journal*, March 14, 2014. As of December 12, 2016: http://www.wsj.com/articles/SB10001424052702304914904579435592981780528

Markoff, John, "Armies of Expensive Lawyers, Replaced by Cheaper Software," *New York Times*, March 4, 2011.

Muaremi, Amir, Bert Arnrich, and Gerhard Tröster, "Towards Measuring Stress with Smartphones and Wearable Devices During Workday and Sleep," *BioNanoScience*, Vol. 3, No. 2, 2013, pp. 172–183.

Murphy, Erin, "The New Forensics: Criminal Justice, False Certainty, and the Second Generation of Scientific Evidence," *California Law Review*, Vol. 95, No. 3, 2007, pp. 721–797.

Murphy, Justin P., and Adrian Fontecilla, "Social Media Evidence in Government Investigations and Criminal Proceedings: A Frontier of New Legal Issues," *Richmond Journal of Law and Technology*, Vol. XIX, No. 3, 2013. As of December 12, 2016: http://jolt.richmond.edu/v19i3/article11.pdf

Nagy, Peter, and Bernadett Koles, "The Digital Transformation of Human Identity," *Convergence*, Vol. 20, No. 3, 2014, pp. 276–292.

National Association of Criminal Defense Lawyers, *Principles and Recommendations to Strengthen Forensic Evidence and Its Presentation in the Courtroom*, Austin, Tex., February 27, 2010. As of August 30, 2016: https://www.nacdl.org/WorkArea/DownloadAsset.aspx?id=21802&libID=21772

National Center for State Courts, "Managing Social Media," web page, undated-a. As of December 12, 2016: http://www.ncsc.org/Information-and-Resources/Social-Media/Managing-Social-Media.aspx

———, "Privacy/Public Access to Court Records: Resource Guide," web page, undated-b. As of December 12, 2016: http://www.ncsc.org/Topics/Access-and-Fairness/Privacy-Public-Access-to-Court-Records/Resource-Guide.aspx

———, "Video Technologies: Resource Guide," web page, undated-c. As of December 12, 2016: http://www.ncsc.org/Topics/Technology/Video-Technologies/Resource-Guide.aspx

———, "Jury Managers' Toolbox: Best Practices for Jury Summons Enforcement," 2009a. As of December 12, 2016: http://www.ncsc-jurystudies.org/~/media/Microsites/Files/CJS/Toolbox/FTA%20Best%20Practices.ashx

———, "Jury Managers' Toolbox: Best Practices to Decrease Undeliverable Rates," 2009b. As of December 12, 2016: http://www.ncsc-jurystudies.org/~/media/Microsites/Files/CJS/Toolbox/Undeliverable%20Best%20Practices.ashx

National Legal Aid and Defender Association, *Risk and Needs Assessments: What Defenders and Chief Defenders Need to Know*, July 2015. As of December 12, 2016: http://www.nlada100years.org/sites/default/files/NLADA_Risk_Needs_Assessments.pdf

National Research Council, *Strengthening Forensic Science in the United States: A Path Forward*, Washington, D.C.: National Academies Press, August 2009. As of December 12, 2016: https://www.ncjrs.gov/pdffiles1/nij/grants/228091.pdf

NCSC—*See* National Center for State Courts.

Nemeth, Robert J., "Enhanced Persuasion in the Courtroom: Visually Dynamic Demonstrative Evidence and Juror Decision Making," in Richard L. Wiener and Brian H. Bornstein, eds., *Handbook of Trial Consulting*, New York: Springer, 2011, pp. 203–214

Niforatos, Evangelos, Veranika Lim, Christian Vuerich, Marc Langheinrich, and Agon Bexheti, "PulseCam: Biophysically Driven Life Logging," MobileHCI'15 conference paper, Copenhagen, Denmark, 2015. As of December 12, 2016: https://www.researchgate.net/profile/Evangelos_Niforatos/publication/282357594_PulseCam_Biophysically_Driven_Life_Logging/links/560e47cc08ae967420111e0d.pdf

Pace, Nicolas M., and Laura Zakaras, *Where the Money Goes: Understanding Litigant Expenditures for Producing Electronic Discovery*, Santa Monica, Calif.: RAND Corporation, MG-1208-ICJ, 2012. As of December 12, 2016: http://www.rand.org/pubs/monographs/MG1208.html

Pepper, John, Carol Petrie, and Sean Sullivan, "Measurement Error in Criminal Justice Data," in Alex R. Piquero and David Weisburd, eds., *Handbook of Quantitative Criminology*, New York: Springer, 2010, pp. 353–374.

Perry, Walter L., Brian McInnis, Carter C. Price, Susan Smith, and John S. Hollywood, *Predictive Policing: The Role of Crime Forecasting in Law Enforcement Operations*, Santa Monica, Calif.: RR-233-NIJ, RAND Corporation, 2013. As of December 12, 2016: http://www.rand.org/pubs/research_reports/RR233.html

Police Executive Research Forum, *COMPSTAT: Its Origins, Evolution and Future in Law Enforcement Agencies*, Washington, D.C., 2013. As of December 12, 2016: http://www.policeforum.org/assets/docs/Free_Online_Documents/Compstat/compstat%20-%20its%20origins%20evolution%20and%20future%20in%20law%20enforcement%20agencies%202013.pdf

Popper, Ben, "Cyborg America: Inside the Strange New World of Basement Body Hackers," *The Verge*, August 8, 2012. As of December 12, 2016: http://www.theverge.com/2012/8/8/3177438/cyborg-america-biohackers-grinders-body-hackers

Privacy Rights Clearinghouse, "Privacy in the Age of the Smartphone," June 1, 2016. As of December 12, 2016: https://www.privacyrights.org/content/privacy-age-smartphone

R.A. Malatest and Associates Ltd., *Evaluation of the Bail Reform Pilot Project, Peace Region and Surrey*, March 31, 2010.

Ratcliffe, Jerry H., *Intelligence-Led Policing*, 2nd ed., Abingdon, Oxon, UK: Routledge, 2016.

Raynes-Goldie, Kate, "Aliases, Creeping, and Wall Cleaning: Understanding Privacy in the Age of Facebook," *First Monday*, Vol. 15, No. 1, January 2010.

Resnick, Brian, "Is There Such a Thing as Too Much Evidence? Assembling the Case Against Dzhokhar Tsarnaev Won't Be as Simple as It Appears from the News," *National Journal*, April 24, 2013.

Riley v California, 573 U.S. ___, 2014.

Roth, Michael D., "Laissez-Faire Videoconferencing: Remote Witness Testimony and Adversarial Truth," *UCLA Law Review*, Vol. 48, No. 1, 2000, pp. 185–219.

Saeb, Sohrab, Mi Zhang, Christopher J. Karr, Stephen M. Schueller, Marya E. Corden, Konrad P. Kording, and David C. Mohr, "Mobile Phone Sensor Correlates of Depressive Symptom Severity in Daily-Life Behavior: An Exploratory Study," *Journal of Medical Internet Research*, Vol. 17, No. 7, 2015, p. e175.

Scalia, Antonin, Statement of the Supreme Court of the United States, 207 F.R.D. 89, 94, 2002.

Schofield, Damian, "Playing with Evidence: Using Video Games in the Courtroom," *Entertainment Computing*, Vol. 2, 2011, pp. 47–58.

Shelton, Donald E., Gregg Barak, and Young S. Kim, "Studying Juror Expectations for Scientific Evidence: A New Model for Looking at the CSI Myth," *Court Review*, Vol. 47, 2011, pp. 8–18.

Shirk, Eric, "The Dangers of Do-It-Yourself Computer Forensics," *Law Practice Today*, American Bar Association, Law Practice Management, November 2007.

Simon, Jonathan, "Reversal of Fortune: The Resurgence of Individual Risk Assessment in Criminal Justice," *Annual Review of Law and Social Science*, Vol. 1, 2005, pp. 397–421.

Singh Jay P., Martin Grann, and Seena Fazel, "Authorship Bias in Violence Risk Assessment? A Systematic Review and Meta-Analysis," *PLoS ONE*, Vol. 8, No. 9, 2013, p. e72484.

Smith v Maryland, 442 U.S. 735, 1979.

Smith, Jessica, "Remote Testimony and Related Procedures Impacting a Criminal Defendant's Confrontation Rights," *Administration of Justice Bulletin*, No. 2013/02, Chapel Hill, N.C.: UNC School of Government, February 2013, pp. 1–18. As of December 12, 2016: http://sogpubs.unc.edu/electronicversions/pdfs/aojb1302.pdf

Solove, Daniel J., *The Digital Person: Technology and Privacy in the Information Age*, New York: New York University Press, 2004.

Sovern, Jeff, "Opting In, Opting Out, or No Options at All: The Fight for Control of Personal Information," *Washington Law Review*, Vol. 74, 1999, pp. 1033–1117.

Spencer, Shaun B., "The Surveillance Society and the Third-Party Privacy Problem," *South Carolina Law Review*, Vol. 65, No. 2, 2013, pp. 373–410.

St. Eve, Amy J., Charles P. Burns, and Michael A. Zuckerman, "More from the #Jury Box: The Latest on Juries and Social Media," *Duke Law & Technology Review*, Vol. 12, No. 1, 2014, pp. 64–91.

St. Eve, Amy J., and Michael A. Zuckerman, "Ensuring an Impartial Jury in the Age of Social Media," *Duke Law & Technology Review*, Vol. 11, No. 1, 2012, pp. 1–29.

Statement of the Supreme Court of the United States, Amendments to Rule 26(b) of the Federal Rules of Criminal Procedure, April 29, 2002.

Storm, Benjamin C., and Sean M. Stone, "Saving-Enhanced Memory: The Benefits of Saving on the Learning and Remembering of New Information," *Psychological Science*, Vol. 26, No. 2, 2015, pp. 182–188.

Storm, Darlene, "Black Hat: Lethal Hack and Wireless Attack on Insulin Pumps to Kill People," ComputerWorld, August 4, 2011. As of December 12, 2016: http://www.computerworld.com/article/2470689/healthcare-it/black-hat--lethal-hack-and-wireless-attack-on-insulin-pumps-to-kill-people.html

Strickland, Eliza, "DARPA Project Starts Building Human Memory Prosthetics" *IEEE Spectrum*, August 27, 2014. As of December 12, 2016: http://spectrum.ieee.org/biomedical/bionics/darpa-project-starts-building-human-memory-prosthetics

Su, Jason G., Meredith A. Barrett, Kelly Henderson, Olivier Humblet, Ted Smith, James W. Sublett, LaQuandra Nesbitt, Chris Hogg, David Van Sickle, and James L. Sublett, "Feasibility of Deploying Inhaler Sensors to Identify the Impacts of Environmental Triggers and Built Environment Factors on Asthma Short-Acting Bronchodilator Use," *Environmental Health Perspectives*, June 2016. As of December 12, 2016: http://ehp.niehs.nih.gov/wp-content/uploads/advpub/2016/6/EHP266.acco.pdf

Terry, M., D. S. Johnson, and P. and Thompson, "Virtual Court Pilot Outcome Evaluation," Ministry of Justice Research Series 21/10, London, December 2010.

Tokson, Matthew J., "Virtual Confrontation: Is Videoconference Testimony by an Unavailable Witness Constitutional?" *University of Chicago Law Review*, Vol. 74, No. 4, 2007, pp. 1581–1614. As of December 12, 2016: http://chicagounbound.uchicago.edu/uclrev/vol74/iss4/13

Trottier, Daniel, "Police and User-Led Investigations on Social Media," *Journal of Law, Information and Science*, Vol. 23, No. 1, 2014, pp. 75–96.

Upturn, *Civil Rights, Big Data, and Our Algorithmic Future: A September 2014 Report on Social Justice and Technology*, September 2014. As of December 12, 2016: https://bigdata.fairness.io/

U.S. Copyright Office, *Exemption to Prohibition on Circumvention of Copyright Protection Systems for Access Control Technologies*, Washington, D.C., October 2015. As of December 12, 2016: https://copyright.gov/1201/2015/fedreg-publicinspectionFR.pdf

Verbruggen, Robert, "Does Pre-Crime Have a Race Problem?" *The American Conservative*, August 2, 2016. As of December 12, 2016: http://www.theamericanconservative.com/articles/does-pre-crime-have-a-race-problem/

Villasenor, John, "What You Need to Know About the Third-Party Doctrine," *The Atlantic*, December 30, 2013. As of August 26, 2016: http://www.theatlantic.com/technology/archive/2013/12/what-you-need-to-know-about-the-third-party-doctrine/282721/

Vincent, James, "Colour-Blind Artist Implants 'Eyeborg' Device into His Skull to 'Hear' Colours as Sounds," *The Independent*, March 17, 2014. As of December 12, 2016: http://www.independent.co.uk/life-style/gadgets-and-tech/news/colour-blind-artist-implants-eyeborg-device-into-his-skull-to-hear-colours-as-sounds-9196711.html

Wade, Kimberley A., Sarah L. Green, and Robert A. Nash, "Can Fabricated Evidence Induce False Eyewitness Testimony?" *Applied Cognitive Psychol*ogy, Vol. 24, 2010, pp. 899–908.

Weber, Francis A., "Complying with the Confrontation Clause in the Twenty-First Century: Guidance for Courts and Legislatures Considering Video Conference Testimony Provisions," *Temple Law Review*, Vol. 86, 2014, pp. 149–180.

White House, *Big Data: Seizing Opportunities, Preserving Values*, Interim Progress Report, February 2015. As of December 12, 2016: https://www.whitehouse.gov/sites/default/files/docs/20150204_Big_Data_Seizing_Opportunities_Preserving_Values_Memo.pdf

Wiens, Kyle, "WTF? It Should Not Be Illegal to Hack Your Own Car's Computer," *Wired*, January 23, 2015. As of August 26, 2016: http://www.wired.com/2015/01/let-us-hack-our-cars/

Wilkins v Wilkinsin, 01AP-468, 2002 WL 47051, Ohio Court of Appeals, January 15, 2002.

Williams, Gerald R., Larry C. Farmer, Rex E. Lee, Bert P. Cundick, Robert J. Howell, and C. Keith Rooker, "Juror Perceptions of Trial Testimony as a Function of the Method of Presentation: A Comparison of Live, Color Video, Black-and-White Video, Audio, and Transcript Presentations," *Brigham Young University Law Review*, Vol. 1975, No. 2, 1975, pp. 375–421.

Williams, Katie Bo, "Prison Phone Company Denies It Recorded Private Calls," *The Hill*, November 12, 2015. As of December 12, 2016: http://thehill.com/policy/cybersecurity/259916-prison-phone-company-denies-it-recorded-private-calls

Wood, Steve M., Lorie L. Sicafuse, Monica K. Miller, and Julianna C. Chomos, "The Influence of Jurors' Perceptions of Attorneys and Their Performance on Verdict," *The Jury Expert*, January 2011, pp. 23–41.

Yablon, Charles, and Nick Landsman-Roos, "Predictive Coding: Emerging Questions and Concerns," *South Carolina Law Review*, Vol. 64, No. 3, 2013, pp. 633–680.

Acknowledgments

The authors would like to acknowledge the participants in the advisory panel that served as the basis for this report, and their names and affiliations are listed in the text box on p. 8. It would not have been possible to complete this effort without their willingness to give their time and expertise to explore the issues associated with technology and individuals' rights, in both the court system and criminal justice overall. We would also like to acknowledge the contributions of Martin Novak and Steve Schuetz of the National Institute of Justice. James Anderson of the RAND Corporation provided advice and assistance in legal elements of the document. We would also like to acknowledge our peer reviewers Nick Pace of RAND, Erin Murphy of New York University, and one anonymous reviewer from the National Institute of Justice.

The RAND Justice Policy Program

The research reported here was conducted in the RAND Justice Policy Program, which spans both criminal and civil justice system issues, with such topics as public safety, effective policing, police-community relations, drug policy and enforcement, corrections policy, use of technology in law enforcement, tort reform, catastrophe and mass-injury compensation, court resourcing, and insurance regulation. 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 at Brian_Jackson@rand.org. For more information about the Justice Policy Program, see www.rand.org/jie/justice-policy or contact the director at justice@rand.org.

About the Authors

Brian A. Jackson is a senior physical scientist at the RAND Corporation. 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.

Duren Banks is the director of the Courts and Corrections Program in the Center for Justice, Safety, and Resilience at RTI International. She specializes in research and evaluation related to criminal case processing, information-sharing between criminal justice agencies, indigent defense, and multisystem approaches to reduce risk factors for victimization. She received her bachelor's degree from Wake Forest University and master's and Ph.D. degrees from the University of Maryland at College Park.

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.

Justin C. Dawson is a senior research scientist at RTI International. His research focuses on courts and corrections, criminal justice, and international rule of law projects. He has a law degree from Creighton University. He began his career as a trial attorney before becoming a prosecuting attorney with the State of Nebraska and the U.S. Department of Justice.

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. For more information about the NLECTC Priority Criminal Justice Needs Initiative, see www.rand.org/jie/justice-policy/projects/priority-criminal-justice-needs.

This report is one product of that effort. It presents the results of the Technology and Due Process Workshop, a group convened in May 2016 as part of the NIJ/NLECTC Priority Criminal Justice Needs Initiative to identify and prioritize research and other needs that either address concerns or take advantage of opportunities related to emerging technologies and the protection of individuals' constitutional rights in the criminal justice system. 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.

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-1748-NIJ