PRIORITY Criminal Justice NEEDS INITIATIVE

A project of the RAND Corporation, the Police Executive Research Forum, RTI International, and the University of Denver

Community Supervision in a Digital World

Challenges and Opportunities

Joe Russo, Michael J. D. Vermeer, Dulani Woods, and Brian A. Jackson

EXECUTIVE SUMMARY

Delivering effective community supervision services has always been challenging; however, recent societal shifts have raised the stakes. Increased access to technology and corresponding increases in computer-facilitated crime have resulted in a greater number of tech-savvy individuals under supervision. A complete ban on individuals' access to computers and the internet is generally not justifiable (or practical) except in the most extreme circumstances. Therefore, supervision agencies must be able to assess and manage the risks. Managing a supervisee's virtual presence can deter new crimes or help officers detect new crimes and monitor compliance with conditions of supervision, but it also can be used to identify problematic behaviors that should be addressed before a new crime occurs.

Despite the clear need to manage supervisees' digital activity, many agencies struggle to meet these challenges head-on. To examine this issue, the National Institute of Justice (NIJ), supported by the RAND Corporation in partnership with the University of Denver, hosted a virtual workshop in June 2020. The workshop brought together a group of probation and parole administrators, researchers, and other experts to discuss the challenges related to supervising individuals in an increasingly digital world and what needs to occur to overcome these obstacles. The project team used a structured brainstorming approach to develop a set of *needs*, which is a term we use to describe a specific requirement tied to either solving a problem or taking advantage of an opportunity to help better address a challenge. Workshop participants identified and prioritized 23 individual needs. Thirteen needs were ranked as high priority. Among the high-priority needs, several themes emerged.

First, participants noted that a lack of evidence supporting some management strategies is a major impediment to the implementation of effective practices for digital supervision. Research is needed to help determine which individuals require digital management according to the risk posed. Second, research is needed to help determine which management strategies, if any, are most effective in reducing this risk. Leveraging this evidence, stakeholders (e.g., legislators, judges, prosecutors, agencies) need to be

SELECTED PRIORITY NEEDS

RESULTS

Organizational issues

- Case studies should be developed that promote the benefits of partnerships with external resources (e.g., local and state law enforcement officers, Internet Crimes Against Children task forces, Regional Computer Forensics Laboratories). Effective strategies to foster these collaborations also should be developed.

Tools and training

- User-friendly preview or triage tools should be developed. These tools should be designed for nontechnical officers to scan the spectrum of electronic devices (e.g., smartphones, tablets, computers). Tools must be free or low-cost and sustainable (e.g., supported, regularly updated).

Policy and practice

- Best practices, policies, and templates for a digital intake process (and periodic updates) should be developed that include all of the devices to which the supervisee has access.

Legal and privacy issues

- Educational materials should be developed for stakeholders that illustrate the importance of access to technology for prosocial activities (as opposed to outright bans), the tools available to agencies to manage risks, and the need to allow for management according to an assessment of risk.

Research

- Research should be conducted to examine the feasibility of validated assessment tools that are specifically designed to identify the risk of cyber-related criminal activity.

educated about effective and realistic approaches considering that most supervision agencies operate in a resource-constrained environment. Third, community supervision leaders need guidance on how to effectively implement a digital management capability within their agency. This guidance includes basic officer training on risks and management strategies, and access to (and training on) tools, techniques, and best practices. Leaders also need guidance on how to address the need for advanced forensics capabilities, through either internal resources or external partnerships.

This report, which describes these needs and the context from workshop discussions, is part of an ongoing series of reports on similar workshops facilitated by the Priority Criminal Justice Needs Initiative. See the "About This Report" section for a list of related reports.

WHAT WE FOUND

Of the 23 needs identified, 13 were ranked by workshop participants as high priority. The greatest concentration of high-priority needs (six of 13) were related to the *tools and training* required to monitor supervisees' digital activity. The participants reported that line officers need (1) standardized training to establish a basic level of competence with respect to the potential risks posed by supervisees' use of technology and (2) effective strategies to manage those risks. Furthermore, officers need tools (and training) to allow them to search and process electronic devices that are of concern. Preview or triage tools that are specifically designed for nontechnical officers to use to quickly scan a variety of devices (e.g., computers, tablets, smartphones) are needed, as are "cheat sheets" that officers can reference to help guide them through the next steps if they find evidence of a new crime or need to seize the device. Agency leaders and line staff require education on how social networking sites might be leveraged as a supervision tool. Specifically, policy guidance and training are needed to highlight the issues surrounding monitoring individuals' activity on these sites (e.g., what the benefits are, when it is appropriate, what the proper techniques are, what the potential pitfalls are). With respect to advanced digital management strategies (e.g., forensic examinations), agencies need access to specialized training that is designed specifically for the community supervision context. As an alternative, agencies should explore partnerships to access training through state, local, and federal justice entities.

Agencies need access to specialized training that is designed specifically for the community supervision context.

Organizational issues accounted for three high-priority needs. The participants argued that agency leaders need better guidance and information about how to effectively implement a sustainable digital management program, which might include a variety of strategies to assess and respond to supervisee risk. Greater awareness is needed about the benefits of partnerships with local, state, regional, and federal entities. Such partnerships can provide access to forensic services to community supervision agencies at low or no cost. Furthermore, the participants recommended the development of effective strategies to establish these partnerships and maximize the benefits of collaboration. Finally, agencies might wish to develop the internal capacity for forensic examinations. These agencies will need guidance to evaluate the feasibility and the costs and benefits of developing specialized expertise in this area.

The participants identified two high-priority needs related to *research*. Noting the challenges that agencies face in determining how to allocate their limited resources, the participants argued that tools are needed to assess a supervisee's "cyber risk." An objective assessment of the likelihood that technology would be used to facilitate a new crime could help agencies determine whether a digital management strategy is needed and, if so, at what level of intensity. The participants envisioned that these tools would complement existing risk and needs assessment instruments that measure the general risk of reoffending. The second need addressed the lack of evidence about the effectiveness of digital management strategies. Specifically, research is needed to help identify which strategies work best to change behavior among the various supervisee subgroups.

One high-priority need fell under the *policy and practice* theme. Best practices and templates are needed for the collection of key data (e.g., access to electronic devices, software, applications, social media profiles, passwords) from individuals requiring digital management. The participants noted that this information should be collected early in the supervision process and updated periodically.

The final high-priority need fell under the *legal issues and privacy* theme. The participants articulated that stakeholders (e.g., legislators, judges, prosecutors)—whose decisions affect how community supervision agencies apply digital management strategies—require better education. For example, broad-brush bans on accessing technology might be unrealistic and counterproductive to goals for rehabilitation. Tailored restrictions that are based on risk factors and enforced through digital management strategies might be a more appropriate approach.

INTRODUCTION

The complex responsibility of providing community supervision services has become more challenging as advances in technology have rapidly changed both society and the nature of crime. Personal electronic devices (e.g., computers, tablets, smartphones) have become increasingly affordable and are now ubiquitous. Furthermore, more than 97 percent of U.S. adults under the age of 50 use the internet (Pew Research Center, 2019; see Figure 1). The internet has allowed for unprecedented access to information, entertainment, resources, and education. It has forever changed the way people communicate and do business. The internet is so woven into virtually every aspect of society that access is no longer considered a luxury; instead, it is essential (Adams, 2020).

Although these innovations have improved our lives in many respects, there is a serious dark side. For example, computer-facilitated crime is growing rapidly. According to the Federal Bureau of Investigation's (FBI's) Internet Crime Complaint Center, more than 460,000 complaints were received in 2019, an increase of nearly 33 percent from the previous year (FBI, 2020). Notably, the rate of complaints tripled and sometimes quadrupled between February and June 2020 with the onset of the coronavirus disease 2019 (COVID-19) pandemic in the United States, a period in which more people stayed at home and increasingly engaged in online activities (Johnson, 2020). In particular, increasing online child abuse and exploitation is a disturbing trend. For example, technology companies reported nearly 70 million images and videos of child sexual abuse in 2019, an increase of more than 50 percent from the previous year (Dance and Keller, 2020). Reports to the National Center for Missing and Exploited Children's CyberTipline have increased by more than 63 percent between 2019 and 2020 (O'Donnell, 2020). Furthermore, the number of online enticement reports nearly doubled during the same period. That said, computer-facilitated crime is not limited to sex offenders or white-collar frauds; technology is used to orchestrate a variety of traditional crimes as well. For example, drug trafficking, weapons sales, stalking, harassment, and murder-for-hire schemes are increasingly occurring online (Kopsie, 2019).

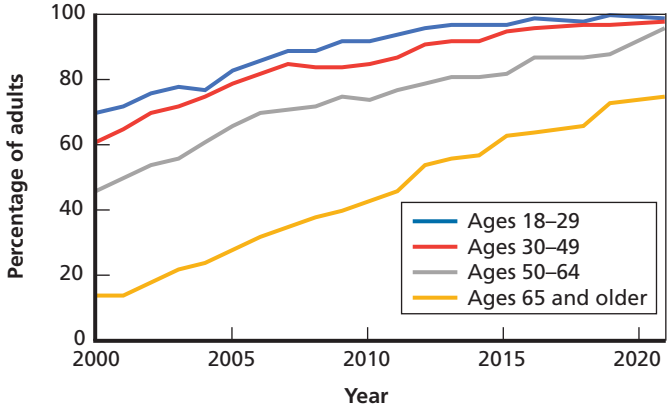
The changing nature of crime, along with the increase in digital literacy among the general population, has resulted in a greater number of tech-savvy individuals under community supervision. This presents unique challenges to the agencies that are responsible for the nearly 4.4 million adults under probation or parole supervision in the United States (Kaeble and Alper, 2020). These agencies have traditionally focused on managing supervisee behavior in the tangible world, but now, they also must be concerned with behavior in the virtual realm. This can seem daunting, given that most agencies are underfunded and overworked. Indeed, only a fraction of all corrections spending is directed to probation and parole operations (Council of State Governments Justice Center, 2018).

For many supervision agencies, managing an individual's digital activity is a relatively new concept, and responses can vary greatly. For example, some jurisdictions (through statute, court, or parole authority order) seek to mitigate risk by strictly prohibiting certain groups of individuals—typically sex offenders—from owning a computer or accessing the internet. Courts across the country, however, are increasingly ruling against blanket bans (Bowker, 2012; Kopsie, 2019). These decisions typically are based on the finding that bans are overly

ABBREVIATIONS

COVID-19	coronavirus disease 2019
FBI	Federal Bureau of Investigation
GPS	Global Positioning System
ICAC	Internet Crimes Against Children
LEO	law enforcement officer
NIJ	National Institute of Justice
PCJNI	Priority Criminal Justice Needs Initiative
RCFL	Regional Computer Forensic Laboratory
SNS	social networking sites

Figure 1. Percentage of U.S. Adults Who Use the Internet, by Age



SOURCE: Adapted from Pew Research Center, 2019.
NOTE: These surveys were conducted from 2000 to 2019.

Given that outright bans are increasingly difficult to justify, except in the most extreme cases, it is imperative that agencies be able to assess and manage the risks posed by supervisee access to technology.

broad and excessive, given the importance of technology to functioning in modern society.

Given that outright bans are increasingly difficult to justify, except in the most extreme cases, it is imperative that agencies be able to assess and manage the risks posed by supervisee access to technology. To do so, restrictions might be required. For example, special conditions of supervision might be imposed that dictate that the individual must

- receive permission from his or her officer to access the internet
- restrict his or her use of technology to specific purposes
- have access restricted to approved devices only
- refrain from accessing pornographic content
- grant officers the authority to conduct warrantless search and seizure of electronic devices.

These special conditions of supervision serve as guidelines that set the stage for specific digital management strategies to help deter or detect criminal activity and/or behaviors that violate the conditions of supervision.[1] Furthermore, these strategies can provide a unique opportunity for proactive engagement and prevention. Research has identified what works in correctional treatment. One of the principal tenets states that identifying and addressing the supervisee's criminogenic needs can reduce the likelihood of recidivism (Bonta and Andrews, 2007). Researchers have identified four major risk factors (i.e., the "big four") that are most associated with recidivism—areas that should be addressed with treatment. These factors are all related: a history of antisocial behavior, antisocial personality pattern, antisocial cognition, and antisocial associates (Duwe, 2017). Jim Tanner, a pioneer in the field of digital management of individuals, has long held that a computer is like a window into the mind of the supervisee and that it is impossible to fully assess these criminogenic factors without considering the digital world (Tanner, 2007). Supervisees, like all people, view material that they like and seek out and consume material that supports their beliefs. Supervisees might be visiting websites or using social networking sites (SNS) to communicate with others with similar antisocial interests (e.g., pedophilia, radicalism, hate groups). Their online associates might be career criminals, and these online interactions might reinforce the supervisees' criminal thinking. These online behaviors might contribute to an increased risk of recidivism, but they often remain invisible to supervision officers. Therefore, managing digital behavior provides the opportunity to identify potential red flags and intervene before a new crime is committed.

Despite the clear and growing need to manage supervisees' virtual presence, many agencies, for a variety of reasons, struggle with how to respond. Bowker, 2017, notes that, in general, agencies tend to gravitate to the extremes; they either cling to the belief that it is easier to totally ban access to computers and the internet or ignore the risks posed by unmanaged access, believing that it is not a problem. Bowker, 2012, further asserts that the perception that supervision officers are somehow unable to manage individuals' computer use is inaccurate. Although there may be exceptions (e.g., supervisees with exceptionally advanced technical skills, supervisees who pose inordinate risk), the majority of supervisees can and should be allowed access to technology without unduly compromising public safety.

Unsurprisingly, there is wide variation in how agencies approach the digital management of supervisees (Kopsie, 2019). Furthermore, there is often inconsistency in application among officers in the same agency. In the following section, we describe the most common digital management strategies currently in use. It is important to note that the approaches are not mutually exclusive, but instead might be used in combination based on the needs of the case, the conditions of supervision, agency policy, and the resources available.

Manual Scans

Digital management does not necessarily require specialized training or tools. For example, an officer might be able to gain

access to a supervisee's cell phone and simply perform a manual scan of the contents. Scrolling through images and videos on the device could reveal important information without disturbing or altering any evidence. Similarly, an officer could scan an individual's internet-enabled television to review the types of movies that he or she has recently streamed.

Preview or Triage Tools

Some agencies use preview or triage tools to conduct an automated scan of an individual's computer or storage media. These tools, which are typically operated by removable media, such as a USB or CD, are relatively user-friendly and require minimal training, making them accessible to nontechnical officers (Bowker, 2012). Scans may be done in the field (i.e., during a home visit) or during an office visit. Common features of these tools include the ability to preview images and videos, view browser history, search files by keyword, identify the most-recent activity, and create and download a report of findings. These tools are not designed to capture every piece of evidence. They are meant to quickly gather information on individual compliance with supervision conditions and, if necessary, document instances of violations or problematic behaviors. In cases in which a scan reveals a suspected new crime, common guidance is to immediately seize and secure the device so that a qualified entity can perform a forensic examination (Tanner, 2015). Using this triage model allows the officer to both obtain timely information that they need to support the supervision process and identify the relatively few cases that need a forensic examination, which require considerable resources.

Forensic Examinations

As discussed in the previous section, officers might have reason to seize a device so that a forensic examination can be conducted. For example, a preview tool might have revealed images of suspected child pornography or there might be reasonable suspicion that the supervisee is engaging in other online criminal behavior. Forensic examinations typically are performed by certified experts who have advanced training on and access to sophisticated tools that allow them to process evidence in a legally defensible manner (e.g., in a way that does not alter or destroy the original data). These investigations are highly technical and, because of the voluminous data-storage capacity of today's devices, can be very time-consuming. Some community supervision agencies have this capability internally. For example, in 2017, the Administrative Office of the United States Courts launched a national laboratory that serves federal probation and pretrial offices across the country. This centralized approach allows individual offices that lack the requisite resources to process digital evidence more expeditiously than if the office had to rely on law enforcement partners (U.S. Courts, 2018). At the state and local levels, very few agencies have this capability.[2] This model is the outlier in large part because building and maintaining this capacity is highly resource-intensive. There are costs associated with obtaining or creating physical space, purchasing hardware and software tools, and dedicating staff to this endeavor. Furthermore, providing for training to maintain certifications is a major recurring expense. Although most agencies would not necessarily have the volume of cases to warrant an internal laboratory, even large organizations might struggle to afford these investments. For example, budget cuts forced the Multnomah County Department of Community Justice (in Oregon) to shutter its successful lab, which officials acknowledged helped keep "victims safe in the community" (Budnick, 2019).

Partnerships

Because most community supervision agencies lack the internal capacity to conduct forensic examinations, they may establish partnerships for support as needed. Typically, they will work with local law enforcement agencies. However, they also might establish partnerships with federal, state, and regional organizations. For example, some agencies dedicate officers to serve on Internet Crimes Against Children (ICAC) task forces.[3] These entities primarily investigate cases involving child abuse and exploitation on the internet. Another example is the Regional Computer Forensic Laboratory (RCFL) program.[4] The 17 RCFLs across the United States provide consultation, forensic services, and a training center for agencies within their geographic boundaries. These relationships can be mutually beneficial (e.g., agencies and RCFLs can share intelligence) and can expand the capacity of resource-constrained community supervision agencies. This approach is not flawless, however, because most entities tend to have significant backlogs, and probation and parole cases might receive less priority (Tanner, 2007).

Remote Computer Monitoring

In contrast to conducting a point-in-time scan or forensic examination, authorities might order the installation of remote-monitoring software on a supervisee's device to continuously detect and deter problematic behaviors (LaMagna and Berejka, 2009). Although these systems vary in specific functional-

ity, they generally capture the online activity (e.g., keystrokes, websites visited, emails sent and received, instant messaging and chat logs, file-sharing activity) of the device and will report any violations or keyword "hits" to authorities. These systems are capable of blocking unauthorized sites and detecting attempts to tamper with or delete the monitoring software. Patterns of activity may be developed by capturing such metrics as the amount of time spent online, the amount of time spent on specific sites or applications, and the time of day the activity is occurring. This information can support the treatment and supervision process. Remote computer monitoring does not require specialized skills on the part of the officer. However, it is important that the officer be able to dedicate time to put the information gleaned into context based on his or her unique knowledge of the individual and the drivers of his or her behavior (Bowker, 2012; Murphy, 2019).

Social Networking Site Investigations

The growing prevalence of SNS in contemporary society means that community supervision agencies must be aware of and manage supervisee activity in these forums. Supervisees may use SNS to engage in criminality (e.g., facilitate human trafficking, coordinate gang activities, groom new victims, share child pornography) and/or to engage with antisocial individuals who reinforce criminal thinking. They also might share information about their whereabouts (which is important if the supervisee absconds or leaves the jurisdiction without approval) or post images of themselves with weapons and/or drugs (Bowker, 2012). Monitoring SNS can help identify problematic behaviors that otherwise might go undetected. The monitoring approaches vary significantly, which introduces complexities. The Global Justice Information Sharing Initiative Advisory Committee notes three distinct methods for conducting SNS investigations: apparent or overt use, discrete use, and covert use (Global Justice Information Sharing Initiative, 2013). Each approach has a different level of intrusiveness. Apparent or overt use may be described as accessing any information that the supervisee makes public. Discrete use typically employs techniques to conceal an officer's identity so that the officer can access public areas of a site without disclosing who they are or sharing their true Internet Protocol (IP) address, which can link back to the agency. As with the apparent or overt use method, no direct contact is made with the individual. Covert use is the most intrusive method and may involve creating a fictitious identity or profile and directly engaging with the supervisee to obtain evidence of a violation or a new crime. This type of investigation requires special skills, training, equipment, and authorization. Officers also may review activity with the supervisee's cooperation (e.g., in the presence of the supervisee). Monitoring an individual's SNS activity can be time-consuming because of the number of sites used and the volume of information shared. Automated tools are available that monitor the internet for references to specific terms, such as the individual's name and profile or screen name (Bowker, 2012).

> Technology will continue to play an important role in society, and computer-facilitated crime will only increase.

Supporting Practices

A variety of other practices can be used to manage a supervisee's digital risk (Bowker, 2012). For example, unannounced home visits and searches can be used to determine whether the supervisee is in possession of unauthorized devices (e.g., computers, gaming systems). Officers may look for such red flags as a large number of high-capacity media storage devices or use tools to interrogate the router to identify all of the devices that are connected in the home. Polygraph examinations are mainly used with sex offenders to help determine whether the supervisee has been deceptive in his or her claims of compliance with restrictions (e.g., access to the internet, viewing inappropriate content). Although they generally are not admissible in court proceedings, polygraph results can help guide the supervision and treatment process (LaMagna and Berejka, 2009). For a supervisee whose location is being monitored (i.e., through Global Positioning System [GPS] tracking), data points can provide clues as to whether he or she might have been accessing the internet without authorization (Bowker, 2012). For example, periods of time spent at public libraries, hotel business centers, or internet cafés might be indicative of circumvention efforts and could warrant investigation.

Looking forward, it is reasonable to surmise that technology will continue to play an important role in society and computer-facilitated crime will only increase. Agencies will find it a challenge to keep pace, given limited resources and the speed at which technology evolves. That said, agencies must

become more proficient. In the 21st century, the virtual world is increasingly relevant to public safety risk and, therefore, it simply cannot be ignored; it must be managed.

Although sex offenders and cybercriminals are the groups that are most likely to have computer-related supervision conditions, not every individual in these groups poses the same cyber risk. Furthermore, all supervisees, regardless of their current charges, have the potential to do harm with technology. Therefore, determining which individuals require digital management, identifying the appropriate intensity of supervision, and implementing effective strategies are all key to successfully minimizing risk.

The Expert Panel

To explore the challenges and opportunities associated with managing supervisees in an increasingly digital world, project staff assembled a panel of probation and parole professionals, researchers, and other experts.

A pool of candidate participants was identified in consultation with the National Institute of Justice (NIJ). Ultimately, a group of 14 experts was convened. The participants and their affiliations are shown in the "Participants" box.

Prior to the workshop, participants were provided with the following read-ahead materials to orient them to the workshop context: "Managing the Risks Posed by Offender Computer Use" (Bowker, 2011), *The Use of Social Media as a Supervision Tool* (American Probation and Parole Association, 2019), and *Digital Forensics and Community Supervision: Improving Technological Supervision of the Twenty-First Century Offender* (Kopsie, 2019).

Because of the social-distancing requirements associated with the COVID-19 pandemic, the workshop was held virtually in two stages in June 2020. During the initial stage, project staff conducted individual interviews with each participant via a web-conferencing application. The length of the interviews ranged from 45 to 90 minutes. The purpose of the interviews was to gather participant insights about the challenges and opportunities associated with managing supervisee use of technology.

To organize discussions, project staff identified five general categories. Participants were also encouraged to speak about the issues that were germane to them, regardless of topic or order:

- **Organizational issues:** What are the high-level challenges agencies face with respect to managing supervisee use of technology (e.g., cultural or leadership issues, lack of awareness of the problem, lack of focus, lack of resources, lack of judicial support)?
- **Policy and practice:** What are the challenges related to operational practice (e.g., implementing a digital management program or focus, developing policy, determining which supervisees to focus on, determining how digital management works with traditional supervision methods and evidence-based practices, pursuing partnerships with law enforcement officers [LEOs])?

PARTICIPANTS

Art Bowker
U.S. Courts, Probation and Pretrial Services, retired

Steven Duke
Brazoria County Adult Probation (Texas)

William Dunham
Michigan Department of Corrections

Kim Flores
California Department of Correction and Rehabilitation

Tawnie Gray
Multnomah County Department of Community Justice (Oregon)

Marcus Hodges
Court Services and Offender Supervision Agency (Washington, D.C.)

Natasha Kopsie
U.S. Probation, District of Arizona

Stephen Larsen
Suffolk County Probation (New York)

Erik McCauley
EJM Digital (Utah)

Dave Murray
Ramsey County Probation (Minnesota)

Rick Parsons
Carbon County Adult Probation (Pennsylvania)

April Pattavina
University of Massachusetts Lowell

Susan Savoy
Maricopa County Adult Probation Department (Arizona)

Joe Winkler
Florida Department of Corrections

- **Tools and training:** What are the challenges and needs related to tools and training (e.g., officer awareness of risks, officer knowledge of technology, search and seizure techniques, monitoring techniques, general versus specific supervisee population issues, improvement of existing tools, comparative evaluations of existing tools, the need for new tools, development of internal capacity for examinations)?
- **Legal and privacy issues:** What are the challenges related to the balance between good supervision and potential overreach (e.g., considering Fourth Amendment issues, special conditions; keeping up with court decisions; monitoring devices that are accessible to, but not owned by, the individual; ensuring the privacy of third parties; managing SNS rules against fictitious identities)?
- **Research:** What evidence is needed to inform the field regarding best practices (e.g., what management approaches, tools, or techniques are most effective or appropriate for staff use; what are the impacts of management approaches on compliance or public safety; does management change supervisee behavior; do we have or need assessment tools specifically for cyber risk)?
- **Other:** What are some of the important issues or pain points that are not sufficiently covered in the other areas?

Project staff captured the input of participants and synthesized it into an initial list of 25 *needs*, which is a term we use to describe a specific requirement tied to either solving a problem or taking advantage of an opportunity to help better address a challenge. The list of needs was provided to the group to review in preparation for the second stage of the workshop. In this second stage, project staff convened all of the participants in three two-hour web meetings held over the course of two days. The purposes of these sessions were to introduce the participants to each other, identify any needs that had not already been raised, consolidate needs that were closely related, fine-tune the wording of the needs statements, and then prioritize the needs. During workshop discussions, participants recommended that two of the needs be consolidated with others; therefore, the final total number of needs was 23. We provide more details about the technical methods used to structure the workshop and and identify and prioritize needs in the technical appendix. In the following section, we describe the results of the prioritization exercise.

> The field of community supervision lacks adequate guidance on how to go about establishing the capacity of digital management such that it becomes a core competency.

RESULTS

Workshop participants identified a total of 23 needs related to providing community supervision services in an increasingly digital world. Thirteen of these needs were categorized as high priority by the participants. These needs were organized into the five major themes that emerged: organizational issues, policy and practice, tools and training, legal and privacy issues, and research. See Figure 2 for the distribution of the needs across the five themes. The full list of needs can be found in the technical appendix.

Overall, more than one-third of all of the needs identified were related to the tools and training required to effectively manage supervisee use of technology, which indicates perceived deficiencies or opportunities in that area. The prioritization exercise (which we describe in greater detail in the technical appendix) elicited rankings of the importance and probability of success of the identified needs from the participants. These rankings were used to sort needs into three tiers (i.e., top, middle, and bottom). Ultimately, 13 of the needs fell into the top tier and are categorized as high-priority needs. These are shown in Table 1. See Figure 3 for a breakdown of the high-priority needs by theme. Nearly half of the top-tier needs (six of 13) fell into the tools and training theme. We discuss the high-priority needs in greater detail in the next section.

DISCUSSION

Organizational Issues

Three high-priority needs fell into the organizational issues theme. According to the participants, most community supervision agencies conceptually understand the importance of incorporating a digital management component as part of supervision. However, there are major obstacles to effective implementation. Primarily, the field of community supervision lacks adequate guidance on how to go about establishing the capacity of digital management such that it becomes a core competency with sustained focus. Implementation guidebooks are needed that highlight best practices and effective strategies. The participants noted that these guidebooks should address such issues as

- the key objectives of digital management
- a description of the variety of available strategies and tools
- model policies and procedures
- legal issues
- infrastructure requirements
- ongoing staffing and training needs.

Furthermore, guidance should be tailored for the various types of agencies (e.g., pretrial, probation, parole), the size of agencies, and resources available.

Participants emphasized that agencies need guidance to better incorporate the information gleaned from these efforts into the supervisee's case management plan. In other words, digital management should be used to continuously inform the supervision process as opposed to operating as an isolated function. To reinforce this approach, the participants recommended that officer expectations be measurable (e.g., the frequency of monitoring individuals' SNS activity) and incorporated into the performance evaluation process, which is not common practice. Finally, agencies should consider the secondary or vicarious trauma impacts on staff who are exposed to disturbing images and videos and provide mental health support to those affected.

Two high-priority needs were related to the resources required to perform advanced digital management techniques (e.g., forensic examinations, cloud investigations). Many agencies lack the internal capacity (e.g., trained staff, tools, infrastructure) to perform these functions, and they might not be aware of—or might not be effectively leveraging—partnerships to help overcome these deficiencies. The participants recommended the development of case studies that illustrate how

Figure 2. Total Number of Needs, by Theme

Figure 3. Breakdown of the 13 Top-Tier Needs, by Theme

partnerships with state and local law enforcement agencies and regional entities (e.g., ICAC task forces, RCFLs) can be mutually beneficial. Best practices are needed to help agencies build these relationships. These partners often can provide community supervision agencies with access to tools and training they would not otherwise be aware of or be able to afford. They also might be able to perform forensic examinations of electronic devices as needed.

Partnerships with external resources can help all agencies, but some may wish to develop the internal capacity for advanced digital management strategies. According to the participants, this would require developing select staff as "cyber specialists." The participants recommended an evaluation of the feasibility, costs, and benefits associated with a specialized-staff approach. To be most effective, specialized staff would need to

Table 1. The 13 High-Priority Needs, by Category

Problem or Opportunity	Need
Organizational issues	
Some agencies might not understand how to establish an effective digital management capacity.	• Develop implementation guidebooks and best practices for establishing a sustainable digital management program as a core competency (and that is tailored for policy and practice and agency size). These guidebooks should include such elements as key objectives; range of management, monitoring, and supervision options; model policies and procedures; legal issues; required tools and infrastructure; and staffing and training needs.
Many agencies lack the resources, expertise, or infrastructure to conduct advanced investigations or forensic exams.	• Develop case studies to promote the benefits (e.g., cost-sharing, information-sharing, access to forensic experts) of partnerships with external resources (e.g., local or state LEOs, ICAC task forces, RCFLs) and effective strategies to foster these collaborations.
The average officer lacks the skills and training to execute advanced digital management approaches and testify in court with confidence.	• Evaluate the costs and benefits of a specialized-staff approach for advanced digital management, to include the identification of specific competencies and certifications for a forensic examiner in the community supervision context. Specialists would train and provide resources to other officers.
Tools and training	
To effectively supervise individuals in a digital world, line officers require a minimum level of competence that is not currently established or maintained.	• Develop a standard, national training curriculum specifically for community supervision officers about the risks and how they can be managed (e.g., what to look for while conducting home visits, different types of storage media, indicators of multiple devices). Training should include approved methods of previewing devices in the field (e.g., manual scans, triage tools) and when and how to seize evidence. This training must be offered and updated regularly. • Develop cheat sheets or briefs for reference when encountering electronic devices in the field (e.g., what to do if evidence of a crime is found, how to properly handle and secure a device, what local resources are available for forensic examination).
Officers need tools to preview and triage electronic devices and storage media.	• Develop user-friendly preview or triage tools that are designed for nontechnical officers to scan the spectrum of electronic devices (e.g., smartphones, tablets, computers). Tools must be free or low-cost and sustainable (e.g., supported and regularly updated).
Monitoring supervisee SNS activity can yield important information, but agencies lack the guidance to take advantage of that information.	• Develop educational materials that highlight the benefits of proactive management of SNS and that are targeted to agency leaders, officers, and external stakeholders. Develop best practices, model policies, and training on how to monitor SNS in a responsible manner (e.g., while protecting the supervisee's legal and privacy rights, third-party rights, and the officer's safety and privacy) while achieving objectives.
Advanced training is needed for more-sophisticated digital management approaches and for officers to testify in court with confidence.	• Develop low-cost, advanced training that is tailored specifically to community supervision specialists. Foster a train-the-trainer approach. • Explore partnerships that allow supervision agencies access to advanced training through local LEOs and/or state and regional groups, such as RCFLs or ICAC task forces.

Table 1—Continued

Problem or Opportunity	Need
Policy and practice	
Establishing a baseline for cyber risk early in supervision can support effective digital management.	• Develop best practices, policies, and templates for a digital intake process (and periodic updates) that includes all of the devices to which the supervisee has access, email addresses, profiles, apps used, SNS used, etc.
Legal and privacy issues	
There is often a disconnect between computer use bans and actual risk, rehabilitative goals, and the ability to enforce the order.	• Develop educational materials for stakeholders that illustrate the importance of managed access to technology for prosocial activities (as opposed to outright bans), the tools available to agencies to manage risks, and the need to allow management according to an assessment of risk. This assessment should acknowledge that the risk is fluid and not just dependent on the nature of the conviction.
Research	
It can be challenging to determine the appropriate level of digital management that is required for supervisees.	• Conduct research to examine the feasibility of validated assessment tools that are specifically designed to identify the risk of cyber-related criminal activity.
There is a dearth of evidence around the effectiveness of digital management strategies.	• Conduct research to determine the effectiveness of digital management strategies (in terms of, e.g., increased compliance or reduced recidivism). Research should examine outcomes against such variables as supervisee type, digital management strategy employed, intensity of the strategy, and the supervising officer's technical capacity (e.g., training and tools) to monitor individuals. Other needs include exploring the value of digital management to reinforce prosocial online behavior and examining the correlation between online and hands-on behaviors.

be dedicated to digital management activities. They would not carry a caseload but instead would be available to assist fellow officers. Furthermore, the evaluation should consider the feasibility of a career path for specialists so that these individuals would have incentives to remain with their agencies and not leave for higher pay in the private sector. Finally, there is a need to establish specific criteria or core competencies that would qualify an officer to be a community supervision cyber specialist. These criteria might include existing professional certifications or new ones that are developed specifically for the unique context of community supervision. The participants acknowledged that the cyber specialist model might not be realistic for smaller agencies or those with significant resource constraints. They cited pressure to reduce average caseload size as a major barrier. Designating an officer as a specialist and relieving them of a caseload increases the load for other officers. The participants also noted that specialized positions typically are more vulnerable to budget cuts and therefore might not be sustainable in the long term without agency commitment.

Policy and Practice

One high-priority need was related to policy and practice. Participants recommended the development of best practices, policies, and templates for a digital intake process to help establish a supervisee's individual baseline for cyber risk. This baseline could be informed by relevant information, such as an inventory of electronic devices an individual owns or to which they have access; software or applications to which they have access; email accounts or passwords; social media profiles, screen names, and passwords; internet service providers used; and removable media (e.g., external hard drives, USB flash drives, optical discs, memory cards) that they own.[5] Other practices might be useful as well. For example, one participant reported that he asks the supervisee to rate his or her technical abilities as part of the digital intake process. Although supervisees might not be entirely forthcoming, the participant noted that this self-assessment is often valuable in helping to determine risk and in guiding the digital management strategies employed. The participants recommended that a digital intake process occur early in the supervision process and be updated periodically over the course of supervision.

> Every community supervision officer should have at least a rudimentary level of knowledge and skills related to supervisee digital management.

Tools and Training

Six high-priority needs were related to the tools and training required to support supervisee digital management.

Given the role that technology plays in contemporary society and its expected trajectory, it is necessary, according to the participants, for every community supervision officer to have at least a rudimentary level of knowledge and skills related to supervisee digital management. A national training curriculum, designed *specifically* for probation and parole officers (as opposed to law enforcement operations or investigations), is required. This was a point of emphasis; as one participant put it, "the big gap is the lack of training geared to our routine daily work activities." The participants recommended that the training should include the general risks related to individual use of technology, specific risks associated with different supervisee groups (e.g., sex offenders, gangs, financial criminals), strategies to manage these risks, indicators to be aware of while conducting home visits (e.g., different types of storage media, unauthorized devices), how to use agency-approved preview and triage tools, and when and how to seize devices in a way that maintains the chain of custody and secures potential evidence. Ideally, this training should be free of charge or low-cost and should be updated frequently to account for changes in the technology landscape.

Community supervision officers are increasingly encountering electronic devices and/or storage media, regardless of whether they are in the field or meeting with individuals in the office. The participants articulated the need for user-friendly preview and triage tools to scan the spectrum of devices (e.g., smartphones, tablets, computers). These tools should be designed specifically for community supervision purposes and should allow a nonexpert officer to quickly scan a device and create a report of key findings. Furthermore, these tools must be free or low-cost and be sustainable (e.g., supported and regularly updated) to account for changes in technology over time. The participants noted that existing free preview tools that are designed to operate on computers (e.g., Field Search) are beneficial but have become obsolete over time. This is in large part due to a lack of ongoing support but also can be attributed to the increased prevalence of other devices, such as smartphones and tablets. One participant noted that "computers were involved in less than 10 percent of all searches in the previous year." Therefore, new tools are needed.

The participants also called for the development and dissemination of model cheat sheets or information briefs that officers could refer to while in the field. These resources would provide guidance to address common scenarios, such as what actions to take if evidence of a crime is detected on an electronic device, how to properly handle and secure a device so as not to compromise the evidence, and what local resources are available to assist with forensic exams. The participants recognized that the briefs would have to be updated regularly and customized to account for agency policy and specific partnerships established or resources available in a particular jurisdiction or area.

According to the participants, monitoring supervisee activity on SNS (e.g., Facebook, YouTube, Instagram) can yield important intelligence, but this approach is underutilized. Furthermore, among agencies that use this technique, there is great variation in how it is used. For example, some agencies might allow officers to view only content that is publicly accessible, while other agencies might allow for more-intensive techniques, such as establishing fictitious identities or profiles to engage with supervisees. Some allow this approach only for certain activities, such as fugitive-apprehension efforts. One participant described the current state of digital management as "the Wild West," with each agency—and each officer within each agency—"doing their own thing." The absence of guidance might lead some agencies to avoid SNS monitoring altogether, and, therefore, they likely would miss out on relevant information that could support the supervision process. To address these issues, the participants articulated that stakeholders (e.g., courts, agency leadership, officers) need education, best practices, and model policies on how SNS monitoring may be best leveraged to support supervision objectives in a manner that avoids infringing upon the individual's right to privacy, protects

the rights of third parties (e.g., friends of friends), and protects the officer's identity. According to the participants, specific guidance is needed regarding how information found online may be used in court proceedings (e.g., authentication); they noted that some judges do not see this type of evidence as real. It should be noted, however, that, as with all supervisees' digital activity, the value of information gleaned is not limited to use in court proceedings. Posts on SNS could provide important data points, which, by themselves or combined with other data, could help the supervision officer determine whether intervention is necessary before a negative outcome occurs. Finally, best practices should address practical considerations. For example, agencies seeking to incorporate an SNS monitoring capability might need to modify their information technology protocols because many jurisdictions use firewalls or filters that prevent staff access to SNS. In these cases, isolated computers (i.e., those that are not connected to the agency's main network) may be designated for SNS monitoring purposes.

Finally, to support agencies that wish to develop the capacity to perform forensic examinations and investigations internally, advanced training that is free or low-cost is required. The participants argued for the importance of a national curriculum that is tailored specifically for community supervision to include a train-the-trainer component.

Legal and Privacy Issues

Discussions with the participants revealed significant variation in how community supervision agencies approach the digital management of individuals. In some jurisdictions, statutes and court or paroling authority orders might prohibit supervisees from accessing computers and the internet. The participants argued that these practices should be examined for several reasons. For example, several courts have ruled against total bans. Furthermore, many argue that access to the internet is essential to functioning in modern society (e.g., searching and applying for a job, looking for community resources); therefore, bans run counter to rehabilitative goals. Furthermore, the ubiquity of the internet makes these bans virtually impossible to consistently enforce. For example, it can be difficult to find a cellular phone that is not internet-enabled. Other everyday items are increasingly internet-enabled (e.g., gaming systems, smart appliances, vehicles), and the internet may be accessed at any number of public sites, including libraries, schools, and business centers. As one participant noted, "conditions banning the use of the internet are largely window dressing because they are so difficult to enforce." Finally, the participants noted that the majority of individuals will not remain under supervision forever; therefore, they will need to learn how to use technology responsibly so that they can function well in society.

The participants argued that stakeholders (e.g., legislators, judges, prosecutors, supervision agencies) need education highlighting the importance of managed access to technology for prosocial activities, as opposed to outright bans. Stakeholders should be clear about the capabilities and limitations of community supervision agencies to manage an individual's virtual presence and should consider individual supervisee risk rather than painting categories of supervisees with a broad brush when determining restrictions (e.g., banning all sex offenders from SNS). The participants noted that every supervisee—not just certain groups of supervisees—has the potential to use technology to do harm. Furthermore, supervisee groups are not homogeneous in terms of cyber risk, and no two supervisees pose the same risk. Finally, risk is not constant. Flexibility is needed to enhance or relax restrictions and digital management strategies based on compliance and progress while under supervision.

Research

Reflecting the increasing emphasis on evidence-based practices in the field of corrections, the participants acknowledged current gaps in the knowledge base with respect to managing supervisee use of technology. Bridging these gaps not only would help agencies provide more-effective supervision but also would help justify investments in digital management strategies. Two high-priority needs emerged within the research theme.

One basic element of evidence-based practice stresses that agencies should focus their resources on those individuals at the greatest risk of reoffending (Bonta and Andrews, 2007). Although many agencies employ risk and needs assessment (RNA) instruments to determine risk and to assign supervision

> The ubiquity of the internet makes total bans on internet use virtually impossible to consistently enforce.

levels, the participants noted that these instruments do not specifically address the issue of cyber risk (i.e., the potential impact of unmonitored access to technology as an aggravating factor). The participants identified some tools and guides (e.g., Brake and Tanner, undated; Parsons et al., 2014), but these tools focus on sex offenders and have not been independently validated. The participants called for the development of validated assessment tools that gauge cyber risk across supervisee groups. Ideally, these tools would augment existing RNA instruments and help agencies identify those individuals who warrant digital management and, if so, the level of supervision required.

Although digital management tools and techniques have been deployed for more than two decades, the participants noted that there remains a dearth of research on effectiveness. Research is needed to determine which specific digital management strategies are most effective in general and which are most effective with various supervisee groups (e.g., sex offenders, gang members, violent offenders, financial criminals).

The participants recognized that identifying the most-appropriate measures of effectiveness will be challenging. In general, the more intensive the management approach is, the more likely it is that violations and crimes will be discovered. Therefore, simple reductions in recidivism might not necessarily be the ideal measure. Also, it is known that some crimes, such as sex offenses, are vastly underreported, which makes recidivism a problematic measure. While recidivism is an important factor, the participants recommended research to assess the impacts of digital management on underlying behaviors. For example, do certain digital management strategies (e.g., SNS monitoring, remote computer or phone monitoring, random previews, forensic examinations) produce greater compliance with supervision conditions? Does the strategy employed produce different results for various supervisee groups? With respect to sex offenders, is the intensity of the digital management strategy and/or the technical capacity (e.g., tools and training) of supervising officers correlated in any way to compliance and reoffending? Or, put another way, is the recidivism rate actually higher than previously thought because officers are not focusing on supervisees' digital activity to the extent that they could or should be?

Other lines of inquiry noted by the participants include the role of adult pornography in sex offender management. Specifically, can mainstream pornography use (however it is defined) be considered a healthy outlet for certain supervisees, or is it a concern? What are the opportunities to identify and reinforce prosocial behaviors (e.g., time spent with positive associates) online? Finally, more research is needed to determine the correlation between hands-off behaviors (e.g., possession, receipt, or distribution of child pornography via the internet) and hands-on sexual offenses.

Effective digital management strategies that are based on risk can deter and detect criminal behaviors, prevent future victimization, and identify antisocial (or prosocial) attitudes, beliefs, and associates.

CONCLUSION

To explore the challenges to providing community supervision services in an increasingly digital world, project staff assembled a group of probation and parole professionals, researchers, and other experts. Project staff conducted individual interviews with each participant and virtual conferencing sessions with the entire group to identify key challenges and the needs that, if addressed, would significantly help community supervision agencies meet these challenges. The list of needs was prioritized by the participants.

There was a consensus among the participants that, although most agencies are already underfunded and overworked with their current approaches to their caseloads, it is no longer possible to provide effective community supervision without accounting for how individuals interface with the digital world. Effective digital management strategies that are based on risk can deter and detect criminal behaviors, prevent future victimization, and identify antisocial (or prosocial) attitudes, beliefs, and associates (which is an important component of the behavioral change process). Digital management needs to be

recognized as a core component of community supervision and, therefore, warrants sustained focus.

To accomplish this objective, the participants identified 13 high-priority needs, which we summarize here. The participants stressed that evidence should guide policy; therefore, more research is needed to determine which supervisees (or supervisee groups) pose the most cyber risk to public safety and which strategies are most effective in reducing this risk. Leveraging this evidence, stakeholders (e.g., legislators, judges, prosecutors) need to be educated on effective and realistic approaches. In general, broad-brush mandates (e.g., a complete ban on internet use) can be impractical and counterproductive. Furthermore, external stakeholders need to understand the capacity of supervision agencies to monitor individuals' use of technology and calibrate their expectations accordingly or provide the resources needed to address the challenges.

Community supervision leaders need guidance on how to best implement a digital management capability within their agencies. At a minimum, every officer should have a basic understanding of both the risks posed by supervisee access to technology and management strategies, to include access to preview tools to scan electronic devices, guidance on appropriate methods of monitoring social networking activity, cheat sheets to guide responses in situations in which evidence of a new crime is found, and best practices for gathering relevant cyber-related data from supervisees during initial intake. Finally, leaders need guidance to determine the need for and feasibility of establishing a cyber specialist role within their organizations and the implications (e.g., ongoing advanced training, certifications, hardware, software, increased caseload for other officers) of doing so. Regardless of whether this model is appropriate for a particular agency, leaders need to build effective partnerships with local, state, and federal agencies to expand their digital forensics capabilities, given resource constraints.

The challenges identified by the panel are daunting; however, the appropriate use of digital management strategies, based on risk, can contribute to improved public safety in a variety of ways. The high-priority needs identified by the expert panel provide a road map of what must be accomplished to move toward that goal.

TECHNICAL APPENDIX

In this appendix, we present additional details about the workshop agenda and the process for identifying and prioritizing technology and other needs related to community supervision in a digital world. Through this process, we developed the research agenda that structured the topics presented in the main report. The descriptions in this appendix are drawn and adapted from those in previous publications of the Priority Criminal Justice Needs Initiative (PCJNI) and reflect the adjustments to the needs identification and prioritization process implemented at this workshop.

Pre-Workshop Activities

We recruited participants by first identifying knowledgeable individuals through existing professional networks and professional social networks (e.g., LinkedIn) and by reviewing literature published on digital management and community supervision. We then extended an invitation to those individuals and provided a brief description of the workshop's focus areas. We extended invitations to 16 individuals. Some individuals referred us to other, more-suitable people in their organizations, and, ultimately, 14 accepted and attended the workshop.

Prior to the COVID-19 pandemic, PCJNI workshops were conducted in person in a group setting. However, under the restrictions and risk mitigations implemented in response to the pandemic, our participants and staff were unable to travel. Our typical format involved a two-day, 14-hour in-person meeting (eight hours the first day, six hours the second day). However, after consultation with experts, we determined that it was not advisable to try to directly replicate this meeting format using virtual conferencing tools. Instead, we individually interviewed each participant for approximately an hour.

During these interviews, we asked the participants to discuss the challenges that they or the practitioners they work with have experienced. We also asked them to identify areas in which additional research and development investment could help alleviate the challenges. During these discussions, participants suggested additional areas that were potentially worthy of research or investment. We consolidated and integrated the problems from the interviews into a single list. We performed this consolidation by separately reviewing the findings of the interviews and then creating a list of the problems, opportunities, and potential solutions described by interviewees. We reviewed these lists to consolidate similar items into single entries and create an initial list of needs for the workshop.

In advance of the first meeting of the virtual workshop, participants were provided with the summarized list of issues and needs.

Identification and Prioritization of Needs

The process of expert elicitation was designed to gather unbiased, representative results from experts and practitioners in the field. However, several limitations could affect the findings. The process typically elicits opinions from a relatively small group of experts. As a result, we strive to make the group as representative as possible of different disciplines, perspectives, and geographic regions. However, the final output of the workshop likely will be significantly influenced by the specific group of experts invited to participate. It is possible that the findings from the workshop would vary were a different group of experts selected. Moreover, although the discussion moderators made every effort to act as neutral parties when eliciting opinions from the collected experts, the background and experience of the moderators had the potential to influence which questions they posed to the group and how they phrased those questions. This also could introduce bias that could influence the findings.

To develop and prioritize a list of technology and policy issues that are likely to benefit from research and investment, we followed a process similar to one that we used in previous PCJNI workshops (see, for example, Jackson et al., 2015; Jackson et al., 2016; and references therein). The needs were prioritized using a variation of the Delphi Method, a technique developed at RAND to elicit expert opinion about well-defined questions in a systematic and structured way (RAND Corporation, undated).

Participants discussed and refined problems related to each category and identified potential solutions (or *needs*) that could address each problem. In addition, needs could be framed in response to opportunities to improve performance by adopting or adapting a new approach or practice (e.g., applying a new technology or tool in the sector that had not been used before).

Virtual Meetings

Once each participant had been interviewed and the needs had been consolidated, we held three two-hour virtual meetings using Zoom, a virtual meeting platform. These meetings were configured such that the participants could see each other's video feeds and collaborate to refine and edit the consolidated needs.

Participants were shown the needs in each category and invited to discuss them. At the end of the discussion of each group of needs, participants were given an opportunity to review and revise the list of problems and opportunities that they had identified. Participants were invited to edit the wording of the needs and were given the opportunity to describe any additional needs that might have been left out after the initial consolidation from the interviews. The participants' combined lists for each topic were displayed one by one on the screen-sharing portion of Zoom using Microsoft PowerPoint slides that were edited in real time to incorporate participants' revisions and comments.

Once the participants agreed on the wording of each slide, we asked them to anonymously vote using a web interface (specifically, the PollAnywhere functionality from Turning Technologies). We asked each participant to score each need and associated strategies to address those needs using a 1–9 scale for two dimensions: importance and probability of success.

For the *importance* dimension, participants were instructed that 1 was a low score and 9 was a high score. Participants were told to score a need's importance with a 1 if it would have little or no impact on the problem and with a 9 if it would reduce the impact of the problem by 20 percent or more. Anchoring the scale with percentage improvements in the need's performance is intended to help make rating values more comparable from participant to participant.

For the *probability of success* dimension, participants were instructed to treat the 1–9 scale as a percentage chance that the need could be met and broadly implemented successfully. That is, they could assign the need's chance of success between 10 percent (i.e., a rating of 1) and 90 percent (i.e., a rating of 9). This dimension was intended to include not only technical concerns (i.e., whether the need would be hard to meet) but also the effect of factors that might cause practitioners to not adopt the new technology, policy, or practice even if it were developed. Such factors could include, for example, cost, effect on practitioner workloads, other staffing concerns, and societal concerns.

After the participants rated the needs displayed on a particular slide (i.e., for either importance or probability of success), the polling software displayed a histogram-style summary of responses. If there was a significant disagreement among the participants (the degree of disagreement was determined by a visual inspection of the histogram), they were asked to discuss or explain their votes at one end of the spectrum or the other. If a second round of discussion occurred, participants were given an opportunity to adjust their ratings on the same question. This second-round rating was optional, and any rating submitted by a participant would replace his or her first-round rating. This process was repeated for each question and dimension at the end of each topic area. Figure A.1 shows an example of a slide that was displayed to the participants via the screen-shar-

ing system. Figure A.2 shows an example of the web interface that participants interacted with to rate each need, and Figure A.3 shows an example of what the web interface displayed to them after they rated each need.

Once the participants completed this rating process for all topic areas, we put the needs into a single prioritized list. We ordered the list by calculating an expected value using the method outlined in Jackson et al., 2016. For each need, we multiplied the final (second-round) ratings for importance and probability of success to produce an expected value. We then calculated the median of that product across all of the respondents and used that as the group's collective expected value score for the need.

We clustered the resulting expected value scores into three tiers using a hierarchical clustering algorithm. The algorithm we used was the "ward.D" spherical algorithm from the "stats" library in the R statistical package, version 3.5. We chose this algorithm to minimize within-cluster variance when determining the breaks between tiers. The choice of three tiers is arbitrary but was done in part to remain consistent across the set of technology workshops we have conducted for NIJ. Also, the choice of three tiers represents a manageable system for policymakers. Specifically, the top-tier needs are the priorities that should be the primary policymaking focus, the middle-tier needs should be examined closely, and the bottom-tier needs are probably not worth much attention in the short term (unless, for example, they can be addressed with existing technology or approaches that can be readily and cheaply adapted to the identified need).

Because the participants initially rated the needs by one topic area at a time, we gave them an opportunity at the end of the workshop to review and weigh in on the tiered list of all identified needs. The intention of this step was to let the participants see the needs in the context of the other tiered needs and allow them to consider whether there were some that appeared too high or low relative to the others. To collect these assessments, we emailed the entire tiered list in a Microsoft Word form to the participants. This step allowed the participants to see all of the ranked needs, providing a top-level view that was complementary to the rankings provided session by session. Participants were then asked to examine where each of the needs landed on the overall tiered list and whether this ordering was appropriate or needed fine-tuning. Participants had the option to indicate whether each problem and need pairing should be voted up or down on the list. An example of this form is provided in Table A.1.

Figure A.1. Example Slide That Participants Saw via Screen-Sharing

Need #21 – Tools & Training 12/12

Problem	Associated Need
To execute more sophisticated management approaches and testify in court with confidence, agencies need access to personnel with a specific skill set (e.g., computer/phone forensics) that the average officer does not possess.	Explore partnerships which allow agencies access to advanced training/tools in collaboration with local LEOs and/or state/regional groups such as RCFLs or ICACS; or arrangements which allow access to the services provided by these entities.

Figure A.2. Example Interface for Participant Feedback

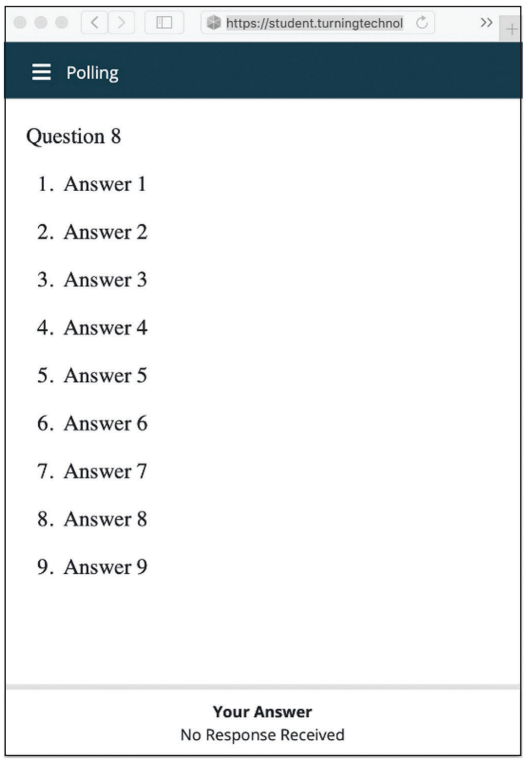
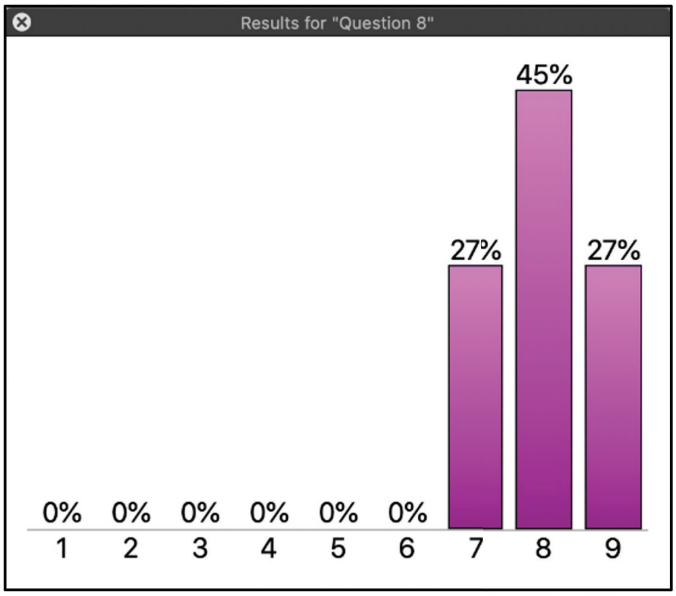


Figure A.3. Example Histogram That Was Displayed to Participants After Voting



We then tallied the participants' third-round responses and applied those votes to produce a final list of prioritized and tiered needs. To adjust the expected values using the up and down votes from the third round of prioritization, we implemented a method equivalent to the one we used in previous work (Hollywood et al., 2016). Specifically, if every participant voted "up" for a need that was at the bottom of the list, then the collective effect of those votes should be to move the need to the top. (The opposite would happen if every participant voted "down" for a need that was at the top of the list.) To determine the point value of a single vote, we divided the full range of expected values by the number of participants voting.

To prevent the (somewhat rare) situation in which small numbers of votes have an unintended outsized impact—for example, when some or all of the needs in one tier have the same or very similar expected values—we also set a threshold that at least 25 percent of the workshop participants must have voted on that need (and then rounded to the nearest full participant). For this workshop, there were 14 participants, so for any votes to have an effect, at least four participants would have had to have voted to move the need up or down.

After applying the up and down vote points to the second-round expected values, we compared the modified scores with the boundary values for the tiers to see whether the change was enough to move any needs up or down in the prioritization. (Note that there were gaps between these boundaries, so some of the modified expected values could fall in between tiers. See Figure A.4.) As with prior work, we set a higher bar for a need to move up or down two tiers (from Tier 1 to Tier 3, or vice versa) than for a need to move to the tier immediately above or below. Specifically, a need could *increase by one tier* if its modified expected value was higher than the highest expected value score in its initial tier. And a need could *decrease by one tier* if its modified expected value was lower than the lowest expected value in its initial tier. However, *to increase or decrease by two tiers* (which was possible only for needs that started in Tier 1 or Tier 3), the score had to increase or decrease by an amount that fully placed the need into the range two tiers away. For example, for a Tier 3 need to jump to Tier 1, its expected value score had to fall within the boundaries of Tier 1, not just within the gap between Tier 1 and Tier 2. See Figure A.4, which illustrates the greater score change required for a need to move two tiers (one need on the far right of the figure) compared with one tier (all other examples shown).

Applying these decision rules to integrate the participants' third-round inputs into the final tiering of needs resulted in numerical separations between tiers that were less clear than the separations that resulted when we used the clustering algorithm in the initial tiering. This can occur because, for example, when the final expected value score for a need that was originally in Tier 3 falls just below the boundary value for Tier 1, that need's final score could be higher than that of some other needs in the item's new tier (Tier 2). See Figure A.5, which shows the distribution of the needs by expected value score after the second-round rating process and then after the third-round voting process.

As a result of the third round of voting, none of the third-round votes were sufficient for any of the needs to change their position within the second-round tiers. The output from this process became the final ranking of the panel's prioritized results.

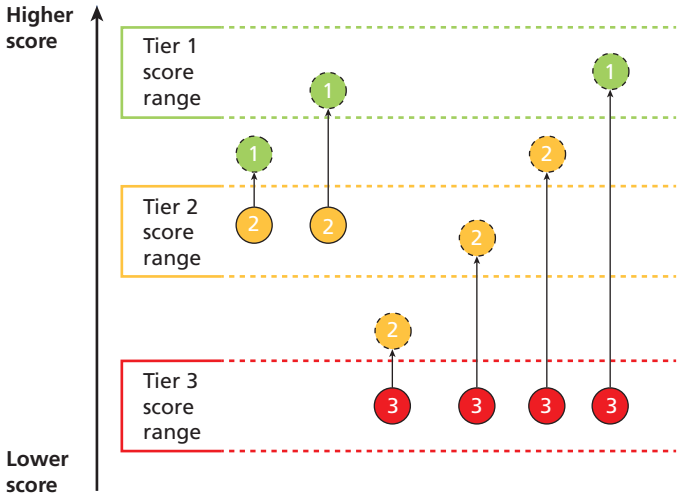
The complete list of identified needs is shown in Table A.2, and the needs are sorted by tier and theme.

Table A.1. Example of the Delphi Round 3 Voting Form

Question	Tier	Vote Up	Vote Down
Tier 1			
Issue: Advanced training is needed for more-sophisticated digital management approaches and for officers to testify in court with confidence. **Need:** Develop low-cost, advanced training that is tailored specifically for community supervision specialists. Foster a train-the-trainer approach.	1		
Issue: There is often a disconnect between computer use bans and actual risk, rehabilitative goals, and the ability to enforce the order. **Need:** Develop educational materials for stakeholders that illustrate the importance of managed supervisee access to technology for prosocial activities (as opposed to outright bans), the tools available to agencies to manage risks, and the need to allow management according to an assessment of risk. This assessment should acknowledge that the risk is fluid and not just dependent on the nature of the conviction.	1		
Tier 2			
Issue: Digital management generates information that is shared with treatment providers. However, important information that is disclosed during treatment is not always shared with agencies. **Need:** Develop best practices for effective collaboration between agencies and therapists, polygraphers, and other related assessors so that privacy regulations may be adhered to without compromising public safety.	2		
Issue: It is challenging to keep up with the unique or emerging ways in which supervisees can circumvent digital management. **Need:** Conduct research on circumvention techniques and the utility of counterforensics measures (e.g., tools to interrogate Wi-Fi or routers to determine what devices have been linked to it).	2		
Tier 3			
Issue: Officers often do not have the capacity to actively monitor the supervisee's social media activity. **Need:** Explore the utility of automated tools, or develop new tools, to efficiently scour SNS for supervisee activity based on the supervisee's profiles.	3		
Issue: Agencies have incorporated digital management into comprehensive supervision approaches for some supervisees (e.g., sex offenders), but similar principles have not been adopted for other high-risk groups. **Need:** Develop best practices and effective strategies for integrating digital management as a component of overall case management for other high-risk groups (e.g., cyber-related criminals, violent criminals, gangs, hackers, financial criminals). Guidance should consider officer workload capacity and supervisee privacy versus public safety needs.	3		

NOTE: Shaded cells indicate that up or down votes were not possible (e.g., Tier 1 is the top tier, so it was impossible to upvote items in that tier).

Figure A.4. How a Need's Increase in Expected Value Might Result in Its Movement Across Tier Boundaries



NOTE: Each example need's original tier is shown by a circle with a solid border (the two needs starting in Tier 2 and the four needs starting in Tier 3). Each need's new tier after the third-round score adjustment is shown by the connected circle with a dotted border.

Figure A.5. Distribution of the Tiered Needs Following Rounds 2 and 3

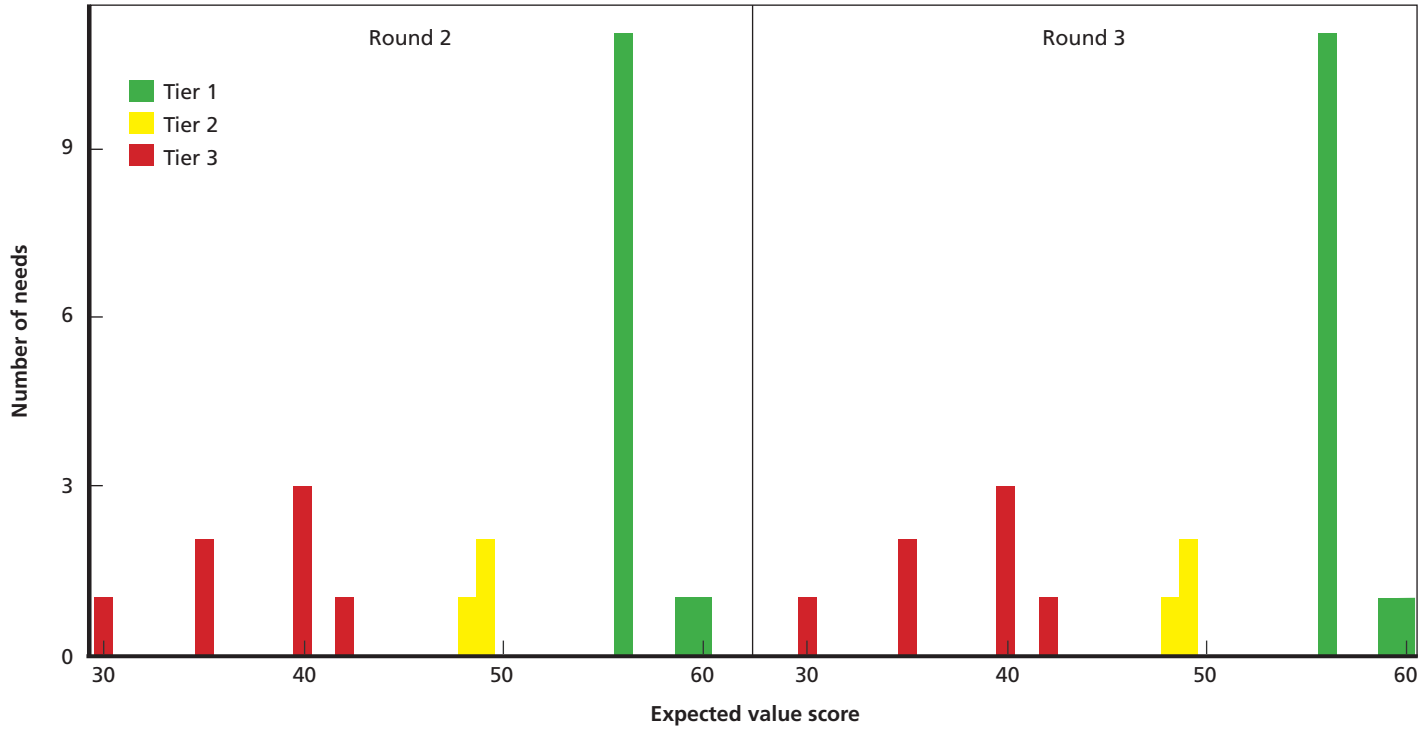


Table A.2. Complete List of Needs, by Tier

Problem or Opportunity	Need	Tier
Organizational issues		
Some agencies might not understand how to establish an effective digital management capacity.	• Develop implementation guidebooks and best practices for establishing a sustainable digital management program as a core competency (and that is tailored for policy and practice and agency size). These guidebooks should include such elements as key objectives; range of management, monitoring, and supervision options; model policies and procedures; legal issues; required tools and infrastructure; and staffing and training needs.	1
Many agencies lack the resources, expertise, or infrastructure to conduct advanced investigations or forensic exams.	• Develop case studies to promote the benefits (e.g., cost-sharing, information-sharing, access to forensic experts) of partnerships with external resources (e.g., local or state LEOs, ICAC task forces, RCFLs) and effective strategies to foster these collaborations.	
The average officer lacks the skills and training to execute advanced digital management approaches and testify in court with confidence.	• Evaluate the costs and benefits of a specialized-staff approach for advanced digital management, to include the identification of specific competencies and certifications for a forensic examiner in the community supervision context. Specialists would train and provide resources to other officers.	
Tools and training		
To effectively supervise individuals in a digital world, line officers require a minimum level of competence that is not currently established or maintained.	• Develop a standard, national training curriculum specifically for community supervision officers about the risks and how they can be managed (e.g., what to look for while conducting home visits, different types of storage media, indicators of multiple devices). Training should include approved methods of previewing devices in the field (e.g., manual scans, triage tools) and when and how to seize evidence. This training must be offered and updated regularly. • Develop cheat sheets or briefs for reference when encountering electronic devices in the field (e.g., what to do if evidence of a crime is found, how to properly handle and secure a device, what local resources are available for forensic examination).	1
Officers need tools to preview and triage electronic devices and storage media.	• Develop user-friendly preview or triage tools that are designed for nontechnical officers to scan the spectrum of electronic devices (e.g., smartphones, tablets, computers). Tools must be free or low-cost and sustainable (e.g., supported and regularly updated).	
Monitoring supervisee SNS activity can yield important information, but agencies lack the guidance to take advantage of that information.	• Develop educational materials that highlight the benefits of proactive management of SNS and that are targeted to agency leaders, officers, and external stakeholders. Develop best practices, model policies, and training on how to monitor SNS in a responsible manner (e.g., while protecting the supervisee's legal and privacy rights, third-party rights, and the officer's safety and privacy) while achieving objectives.	
Advanced training is needed for more-sophisticated digital management approaches and for officers to testify in court with confidence.	• Develop low-cost, advanced training that is tailored specifically for community supervision specialists. Foster a train-the-trainer approach. • Explore partnerships that allow supervision agencies access to advanced training through local LEOs and/or state and regional groups, such as RCFLs or ICAC task forces.	
Policy and practice		
Establishing a baseline for cyber risk early in supervision can support effective digital management.	• Develop best practices, policies, and templates for a digital intake process (and periodic updates) that includes all of the devices to which the supervisee has access, email addresses, profiles, apps used, SNS used, etc.	1

Table A.2—Continued

Problem or Opportunity	Need	Tier
Legal and privacy issues		
There is often a disconnect between computer use bans and actual risk, rehabilitative goals, and the ability to enforce the order.	• Develop educational materials for stakeholders that illustrate the importance of managed individual access to technology for prosocial activities (as opposed to outright bans), the tools available to agencies to manage risks, and the need to allow management according to an assessment of risk. This assessment should acknowledge that the risk is fluid and not just dependent on the nature of the conviction.	1
Research		
It can be challenging to determine the appropriate level of digital management that is required for supervisees.	• Conduct research to examine the feasibility of validated assessment tools that are specifically designed to identify the risk of cyber-related criminal activity.	1
There is a dearth of evidence around the effectiveness of digital management strategies.	• Conduct research to determine the effectiveness of digital management strategies (in terms of, e.g., increased compliance or reduced recidivism). Research should examine outcomes against such variables as supervisee type, digital management strategy employed, intensity of the strategy, and the supervising officer's technical capacity (e.g., training and tools) to monitor individuals. Other needs include exploring the value of digital management to reinforce prosocial online behavior and examining the correlation between online and hands-on behaviors.	
Organizational issues		
Forensic tools can be expensive, and it can be challenging for agencies to select the appropriate tools for their needs.	• Explore the benefits of a centralized procurement system (e.g., a master contract) and an evaluation mechanism to allow agencies access to products and services at prenegotiated rates. The system should be supported by independent evaluations and buyer's guides for tools and services, comparison charts of capabilities versus costs, and records of ongoing costs (e.g., hardware, software updates, training, and staff time).	2
Policy and practice		
Digital management generates information that is shared with treatment providers. However, important information that is disclosed during treatment is not always shared with agencies.	• Develop best practices for effective collaboration between agencies and therapists, polygraphers, and other related assessors so that privacy regulations may be adhered to without compromising public safety.	2
Research		
It is challenging to keep up with the unique or emerging ways in which supervisees can circumvent digital management.	• Conduct research on circumvention techniques and the utility of counter-forensics measures (e.g., tools to interrogate Wi-Fi or routers to determine what devices have been linked to it).	2
Organizational issues		
Some stakeholders (e.g., legislators, agency executives, judges) lack an understanding of the importance of digital management to the supervision process, the skills and resources, and the ongoing training required. Some try to avoid risks by denying supervisees access to digital devices.	• Develop a national training program or educational materials demonstrating the necessity of managing (rather than banning) supervisee use of technology, the challenges agencies face, and the value of effective monitoring (e.g., the prevention of crime and new victims, the detection of new crimes or violations, intelligence to support the treatment and rehabilitation process).	3

Table A.2—Continued

Problem or Opportunity	Need	Tier
Tools and training		
Officers often do not have the capacity to actively monitor the supervisee's social media activity.	• Explore the utility of automated tools, or develop new tools, to efficiently scour SNS for supervisee activity based on the supervisee's profiles.	3
Unique internet-enabled devices (e.g., gaming systems, smart TVs) present unique challenges (e.g., specialized skills and tools are needed, scanning them is very time-consuming).	• Develop tools, best practices, and guides to help agencies better manage these devices (e.g., methods to manually scan the devices, guidance on the advantages and disadvantages of banning use for certain supervisees or groups because of forensic limitations).	
Policy and practice		
Agencies are missing opportunities to fully leverage the spectrum of supervisee digital information.	• Explore the costs, benefits, and utility of analyzing integrated data streams (e.g., computer use, SNS activity, GPS location, ShotSpotter location) and applying these data internally for supervision purposes and for information-sharing across jurisdictions. Demonstrate the impact on public safety.	3
Agencies have incorporated digital management into comprehensive supervision approaches for some individuals (e.g., sex offenders), but similar principles have not been adopted for other high-risk supervisee groups.	• Develop best practices and effective strategies for integrating digital management as a component of overall case management for other high-risk groups (e.g., cyber-related criminals, violent criminals, gangs, hackers, financial criminals). Guidance should consider officer workload capacity and supervisee privacy versus public safety needs.	
The digital management landscape changes rapidly, and agencies and officers struggle to keep abreast of the latest information.	• Develop, market, and foster online forums or communities of learning for community supervision staff to engage in ongoing networking, information-sharing, and collaboration on best practices, resources, new tools, training opportunities, supervisee countermeasures, etc. Forums should be administered by a national entity (e.g., the National Institute of Corrections) and be accessible to staff of all skill levels.	
Legal and privacy issues		
Some digital management approaches are not employed by agencies specifically because leaders have concerns about officers' ability to credibly testify in court about how the tool was used.	• Develop education and training materials for agency leaders, judges, prosecutors, and defense attorneys on the capabilities and limitations of digital management approaches (e.g., some preview or triage tools used on a live device can leave a digital footprint but cannot insert or create substantive evidence).	3

Notes

[1] For the purposes of discussion and this report, *digital management* refers to the strategies used to monitor supervisee use of technology. These strategies might include such processes as gathering information about an individual's online presence; searching an individual's home for electronic devices or storage media; visually scanning an individual's device or social networking site posts; conducting social networking investigations; or using tools to conduct point-in-time scans of devices, full forensic examinations, and the continuous remote monitoring of devices.

[2] For example, the Nevada Department of Public Safety–Probation and Parole Division and the Suffolk County Probation Department in New York have the capability to conduct forensic examinations internally, but few other agencies do.

[3] This program, which is funded by the U.S. Department of Justice, is a national network of 61 coordinated task forces representing more than 4,500 federal, state, and local law enforcement and prosecutorial agencies (Office of Juvenile Justice and Delinquency Prevention, undated).

[4] RCFL programs are partnerships between the FBI and other federal, state, and local law enforcement agencies. Together, these organizations operate a regional digital forensics task force.

[5] See Bowker, 2012, for an example of a computer usage questionnaire, which could provide this information for officers.

References

Adams, Stan, "In the Middle of COVID-19: Can We All Agree Now That Internet Access Is a Necessity?" Center for Democracy & Technology, April 2, 2020. As of November 8, 2020: https://cdt.org/insights/in-the-middle-of-covid-19-can-we-all-agree-now-that-internet-access-is-a-necessity/

American Probation and Parole Association, *The Use of Social Media as a Supervision Tool: Issue Paper*, Lexington, Ky., April 24, 2019. As of November 22, 2020: https://www.appa-net.org/eweb/docs/APPA/stances/ip-USMST.pdf

Bonta, James, and D. A. Andrews, *Risk-Need-Responsivity Model for Offender Assessment and Rehabilitation*, Ottawa, ON: Public Safety Canada, 2007. As of November 2, 2020: https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/rsk-nd-rspnsvty/rsk-nd-rspnsvty-eng.pdf

Bowker, Art, "Managing the Risks Posed by Offender Computer Use: An APPA Technology Committee Issue Paper," *American Probation and Parole Association News*, Fall 2011, pp. 40–49. As of November 22, 2020: https://www.appa-net.org/eweb/docs/APPA/stances/ip_MRPOCU.pdf

Bowker, Art, *The Cybercrime Handbook for Community Corrections: Managing Offender Risk in the 21st Century*, Springfield, Ill.: Charles C. Thomas Publishing, 2012.

Bowker, Art, "Cyber-Risk: Can Corrections Get It Right?" blog post, Corrections.com, May 9, 2017. As of November 18, 2020: http://www.corrections.com/cybercrime/

Brake, Stephen, and Jim Tanner, "Determining the Need for Internet Monitoring of Contact Sex Offenders," undated. As of November 23, 2020: http://www.stephenbrakeassociates.com/Internet%20Monitoring%2008.pdf

Budnick, Nick, "Multnomah County to Cut Its Crime-Fighting Computer Lab," *Portland Tribune*, May 21, 2019. As of November 19, 2020: https://pamplinmedia.com/pt/9-news/428909-334305-multnomah-county-to-cut-its-crime-fighting-computer-lab

Council of State Governments Justice Center, *50-State Report on Public Safety: Tools and Strategies to Help States Reduce Crime, Recidivism, and Costs*, New York, July 31, 2018.

Dance, Gabriel J. X., and Michael H. Keller, "Tech Companies Detect a Surge in Online Videos of Child Sexual Abuse," *New York Times*, February 20, 2020.

Duwe, Grant, *The Use and Impact of Correctional Programming for Inmates on Pre- and Post-Release Outcomes*, Washington, D.C.: National Institute of Justice, NCJ 250476, June 2017. As of November 2, 2020: https://www.ncjrs.gov/pdffiles1/nij/250476.pdf

FBI—*See* Federal Bureau of Investigation.

Federal Bureau of Investigation, *2019 Internet Crime Report*, Washington, D.C., 2020.

Global Justice Information Sharing Initiative, *Developing a Policy on the Use of Social Media in Intelligence and Investigative Activities: Guidance and Recommendations*, Washington, D.C.: Bureau of Justice Assistance, February 2013.

Hollywood, John S., Dulani Woods, Andrew Lauland, Sean E. Goodison, Thomas J. Wilson, and Brian A. Jackson, *Using Future Broadband Communications Technologies to Strengthen Law Enforcement*, Santa Monica, Calif.: RAND Corporation, RR-1462-NIJ, 2016. As of June 10, 2021: https://www.rand.org/pubs/research_reports/RR1462.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 June 10, 2021: https://www.rand.org/pubs/research_reports/RR1255.html

Jackson, Brian A., Joe Russo, John S. Hollywood, Dulani Woods, Richard Silberglitt, George B. Drake, John S. Shaffer, Mikhail Zaydman, and Brian G. Chow, *Fostering Innovation in Community and Institutional Corrections: Identifying High-Priority Technology and Other Needs for the U.S. Corrections Sector*, Santa Monica, Calif.: RAND Corporation, RR-820-NIJ, 2015. As of June 10, 2021: https://www.rand.org/pubs/research_reports/RR820.html

Jackson, Brian A., Michael J. D. Vermeer, Kristin J. Leuschner, Dulani Woods, John S. Hollywood, Duren Banks, Sean E. Goodison, Joe Russo, and Shoshana R. Shelton, *Fostering Innovation Across the U.S. Criminal Justice System: Identifying Opportunities to Improve Effectiveness, Efficiency, and Fairness*, Santa Monica, Calif.: RAND Corporation, RR-4242-NIJ, 2020. As of June 10, 2021: https://www.rand.org/pubs/research_reports/RR4242.html

Jackson, Brian A., Michael J. D. Vermeer, Dulani Woods, Duren Banks, Sean E. Goodison, Joe Russo, Jeremy D. Barnum, Camille Gourdet, Lynn Langton, Michael G. Planty, Shoshana R. Shelton, Siara I. Sitar, and Amanda R. Witwer, *The U.S. Criminal Justice System in the Pandemic Era and Beyond: Taking Stock of Efforts to Maintain Safety and Justice Through the COVID-19 Pandemic and Prepare for Future Challenges*, Santa Monica, Calif.: RAND Corporation, RR-A108-8, 2021. As of June 10, 2021: https://www.rand.org/pubs/research_reports/RRA108-8.html

Johnson, Derek B., "Congress Targets COVID Cyber Fraud," *Federal Computer Week*, June 17, 2020. As of November 6, 2020: https://fcw.com/articles/2020/06/17/johnson-congress-covid-cyber.aspx

Kaeble, Danielle, and Mariel Alper, *Probation and Parole in the United States, 2017–2018*, Washington, D.C.: Bureau of Justice Statistics, No. NCJ 252072, August 2020. As of October 29, 2020: https://www.bjs.gov/index.cfm?ty=pbdetail&iid=6986

Kopsie, Natasha, *Digital Forensics and Community Supervision: Improving Technological Supervision of the Twenty-First Century Offender*, master's thesis, Utica, N.Y.: Utica College, May 2019.

LaMagna, Richard C., and Marc Berejka, "Remote Computer Monitoring: Managing Sex Offenders' Access to the Internet," *Journal of Offender Monitoring*, Vol. 21, No. 1, Spring/Summer 2009, pp. 11–24.

Murphy, Heather, "How Convicts Ordered to Stay Offline Try to Slip Their Digital Leashes," *New York Times*, May 26, 2019.

O'Donnell, Brenna, "COVID-19 and Missing & Exploited Children," National Center for Missing and Exploited Children, October 20, 2020. As of November 2, 2020: https://www.missingkids.org/blog/2020/covid-19-and-missing-and-exploited-children

Office of Juvenile Justice and Delinquency Prevention, "Internet Crimes Against Children Task Force Program," webpage, undated. As of June 14, 2021: https://ojjdp.ojp.gov/programs/internet-crimes-against-children-task-force-program

Parsons, Richmond, Nicholas Honyara, David L. Delmonico, and Elizabeth J. Griffin, "The Child Abuse Material Instrument (CAMI): Collecting and Utilizing Forensic Data in Child Pornography Cases," *Perspectives: Journal of the American Probation and Parole Association*, Vol. 38, No. 1, 2014.

Pew Research Center, "Internet/Broadband Fact Sheet," June 12, 2019. As of November 6, 2020: https://www.pewresearch.org/internet/fact-sheet/internet-broadband/

RAND Corporation, "Delphi Method," webpage, undated. As of June 10, 2021: https://www.rand.org/topics/delphi-method.html

Russo, Joe, Michael J. D. Vermeer, Dulani Woods, and Brian A. Jackson, *Risk and Needs Assessments in Prisons: Identifying High-Priority Needs for Using Evidence-Based Practices*, Santa Monica, Calif: RAND Corporation, RR-A108-5, 2020. As of June 10, 2021: https://www.rand.org/pubs/research_reports/RRA108-5.html

Russo, Joe, Dulani Woods, George B. Drake, and Brian A. Jackson, *Leveraging Technology to Enhance Community Supervision: Identifying Needs to Address Current and Emerging Concerns*, Santa Monica, Calif.: RAND Corporation, RR-3213-NIJ, 2019. As of June 10, 2021: https://www.rand.org/pubs/research_reports/RR3213.html

Russo, Joe, Dulani Woods, John S. Shaffer, and Brian A. Jackson, *Countering Threats to Correctional Institution Security: Identifying Innovation Needs to Address Current and Emerging Concerns*, Santa Monica, Calif.: RAND Corporation, RR-2933-NIJ, 2019. As of June 10, 2021: https://www.rand.org/pubs/research_reports/RR2933.html

Tanner, Jim, "Beyond Prosecution: Improving Computer Management of Convicted Sex Offenders," Boulder, Colo.: Knowledge-Based Solutions, 2007. As of November 2, 2020: http://www.kbsolutions.com/beyond.pdf

Tanner, Jim, "Field Search Manual," Windows version 5.2 (FSWin.exe), December 2015.

U.S. Courts, "National Lab Keeps Officers One Digital Step Ahead," Judiciary News, June 27, 2018. As of November 19, 2020: https://www.uscourts.gov/news/2018/06/27/national-lab-keeps-officers-one-digital-step-ahead

Acknowledgments

The authors would like to acknowledge the participation and assistance of the members of the Community Supervision in a Digital World: Challenges and Opportunities expert workshop. This effort would not have been possible without their willingness to participate. The authors also would like to acknowledge the contributions of Steve Schuetz of the National Institute of Justice. The authors also acknowledge the valuable contributions of the peer reviewers of the report, Greg Brown of the University of Colorado Denver, Lois Davis of the RAND Corporation, and the anonymous reviewers from the U.S. Department of Justice.

The RAND Justice Policy Program

RAND Social and Economic Well-Being is a division of the RAND Corporation that seeks to actively improve the health and social and economic well-being of populations and communities throughout the world. This research was conducted in the Justice Policy Program within RAND Social and Economic Well-Being. The program focuses on such topics as access to justice, policing, corrections, drug policy, and court system reform, as well as other policy concerns pertaining to public safety and criminal and civil justice. For more information, email justicepolicy@rand.org.

About the Authors

Joe Russo is a researcher with the University of Denver, where he has supported a variety of programs funded by NIJ. His research focuses on institutional and community corrections technologies and on identifying the high-priority technology needs of agencies across the country. He has served in the New York City Department of Correction and the New York City Department of Probation. He has an M.S. in criminal justice.

Michael J. D. Vermeer is a physical scientist at the RAND Corporation. His interests and expertise cover topics related to science and technology policy, criminal justice, national security, cybersecurity and privacy, and emerging technologies. He co-leads the Priority Criminal Justice Needs Initiative. His other work is related to development planning, program evaluation, and other analyses to guide strategic decisionmaking in the armed services and government agencies. He holds a Ph.D. in inorganic chemistry.

Dulani Woods is a quantitative analyst adept at data acquisition, transformation, visualization, and analysis. His research typically focuses on justice and homeland security policy. He began his career as a Coast Guard officer on afloat and ashore assignments in Miami, Florida; New London, Connecticut; and Baltimore, Maryland. He holds an M.S. in agricultural economics (applied economics).

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. He has a Ph.D. in bioinorganic chemistry.

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, 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 research effort, called the Priority Criminal Justice Needs Initiative, is a component of the Criminal Justice Requirements & Resources Consortium (RRC) and is intended to support innovation within the criminal justice enterprise. For more information about the RRC and the Priority Criminal Justice Needs Initiative, please see www.rand.org/well-being/justice-policy/projects/priority-criminal-justice-needs.

This report is one product of that effort. In June 2020, RAND and University of Denver staff conducted an expert workshop on community supervision in a digital world. The workshop was convened to identify high-priority technology and policy needs related to supervising individuals in an increasingly digital world. This report presents the proceedings of that workshop, topics considered, needs that panel participants developed, and overarching themes that emerged from the panel discussion. This report and the results it presents should be of interest to community corrections agency administrators, community corrections officers, correctional assessment and treatment staff, risk-needs assessment technology providers, digital supervision technology providers, and the research community. Other RAND research reports from the Priority Criminal Justice Needs Initiative that might be of interest are

- Joe Russo, Dulani Woods, George B. Drake, and Brian A. Jackson, *Leveraging Technology to Enhance Community Supervision: Identifying Needs to Address Current and Emerging Concerns*, Santa Monica, Calif.: RAND Corporation, RR-3213-NIJ, 2019
- Joe Russo, Michael J. D. Vermeer, Dulani Woods, and Brian A. Jackson, *Risk and Needs Assessments in Prisons: Identifying High-Priority Needs for Using Evidence-Based Practices*, Santa Monica, Calif: RAND Corporation, RR-A108-5, 2020
- Brian A. Jackson, Michael J. D. Vermeer, Kristin J. Leuschner, Dulani Woods, John S. Hollywood, Duren Banks, Sean E. Goodison, Joe Russo, and Shoshana R. Shelton, *Fostering Innovation Across the U.S. Criminal Justice System: Identifying Opportunities to Improve Effectiveness, Efficiency, and Fairness*, Santa Monica, Calif.: RAND Corporation, RR-4242-NIJ, 2020
- Brian A. Jackson, Michael J. D. Vermeer, Dulani Woods, Duren Banks, Sean E. Goodison, Joe Russo, Jeremy D. Barnum, Camille Gourdet, Lynn Langton, Michael G. Planty, Shoshana R. Shelton, Siara I. Sitar, and Amanda R. Witwer, *The U.S. Criminal Justice System in the Pandemic Era and Beyond: Taking Stock of Efforts to Maintain Safety and Justice Through the COVID-19 Pandemic and Prepare for Future Challenges*, Santa Monica, Calif.: RAND Corporation, RR-A108-8, 2021
- Joe Russo, Dulani Woods, John S. Shaffer, and Brian A. Jackson, *Countering Threats to Correctional Institution Security: Identifying Innovation Needs to Address Current and Emerging Concerns*, Santa Monica, Calif.: RAND Corporation, RR-2933-NIJ, 2019.

Mentions of products or companies do not represent endorsement by NIJ, the University of Denver, or the RAND Corporation.

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

This publication was made possible by Award Number 2018-75-CX-K006, awarded by the National Institute of Justice, Office of Justice Programs, U.S. Department of Justice. The opinions, findings, conclusions, and recommendations expressed in this publication are those of the author(s) and do not necessarily reflect those of the Department of Justice, the RAND Corporation, or the organizations represented by any of the workshop participants.

Research Integrity

Our mission to help improve policy and decisionmaking through research and analysis is enabled through our core values of quality and objectivity and our unwavering commitment to the highest level of integrity and ethical behavior. To help ensure our research and analysis are rigorous, objective, and nonpartisan, we subject our research publications to a robust and exacting quality-assurance process; avoid both the appearance and reality of financial and other conflicts of interest through staff training, project screening, and a policy of mandatory disclosure; and pursue transparency in our research engagements through our commitment to the open publication of our research findings and recommendations, disclosure of the source of funding of published research, and policies to ensure intellectual independence. For more information, visit www.rand.org/about/principles.

Limited Print and Electronic Distribution Rights

www.rand.org

RAND CORPORATION

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

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