LEVERAGING THE POWER OF SMARTPHONE APPLICATIONS TO ENHANCE COMMUNITY SUPERVISION

American Probation and Parole Association

Submitted by the Technology Committee

April 7, 2020

ISSUE PAPER

LEVERAGING THE POWER OF SMARTPHONE APPLICATIONS TO ENHANCE COMMUNITY SUPERVISION

INTRODUCTION

This paper will address the use of smartphone applications installed on a client's[1] personal device, or a device provided to the client, to be used in support of the community supervision process.

Community corrections is responsible for the supervision of the vast majority of individuals under correctional control, yet only a small percent of corrections budgets are allocated to this effort. Indeed while 69 percent of the correctional population is under some sort of community supervision (Kaeble and Cowhig, 2018), only 12 percent of corrections spending is directed to probation and parole operations (Pew Center on the States, 2009). Given that many agencies are stretched to capacity, effective community supervision can only be accomplished if all available resources are fully leveraged. Agencies often look to technology to help them do more with less and many are now exploring smartphone applications as a way of providing cost-effective supervision services to their clients.

Two major factors are driving this trend. The first is technical capability; smartphones are essentially powerful handheld computers that also provide cellular communications. Among other features, smartphones typically integrate a touchscreen interface, Internet access, camera, video recorder, location-based services and an operating system capable of running downloaded applications created to support the community supervision process. Further, peripheral devices, such as remote breathalyzers and other sensors, can be linked with the smartphone to expand supervision capabilities. As this technology continues to advance, agencies can leverage these developments in ways that traditional electronic supervision devices simply can't support.

1 The term client will be used in this paper to refer to adults and juveniles involved with community corrections agencies as pretrial or presentence defendants or persons under probation, parole or other forms of community supervision

The second factor is ubiquity as most people now own and are familiar with smartphones. According to the Pew Research Center, 81 percent of U.S. adults have a smartphone and ownership levels are highest (95%) among those ages 18-29 (Pew, 2019).

This issue paper provides readers with important background information about smartphone applications for community supervision, a discussion of capabilities and limitations, and the issues agencies should explore as they consider these solutions.

What Over the past several years a number of smartphone application products for community supervision have entered the market.2 These applications are essentially case management and monitoring software programs designed to run on a mobile device. Leveraging the power inherent in today's smartphones, these applications offer a highly flexible tool designed to support a wide variety of supervision objectives depending on the needs of the case. For example, accountability objectives can be achieved through features such as location monitoring, remote reporting or check-ins. Behavioral change objectives can be facilitated through instant communications with the officer, providing the client with timely access to resources such as programming, and therapeutic counseling via tele-presence.

> ***Smartphone applications have the potential to support the supervision process, however, in order for these benefits to be fully realized, the client must be in possession of - and be the person actually using - the smartphone.***

DIFFERING APPROACHES

Current smartphone applications for community supervision can be distinguished in two main ways. The first is whether the application is installed on a vendor provided phone, also known as "corporate-owned", or on the client's phone, which may be referred to as "bring your own device" (BYOD). The second distinction is how the information generated or collected by the smartphone or application (location, reported data, etc.) is linked to the individual under supervision. We will examine these key differences one at a time.

The Smartphone

The application may be installed on the client's BYOD or integrated into a locked-down, customized smartphone which is available for purchase or lease from the vendor. As with any technology, there are advantages and disadvantages to each approach. The BYOD approach is generally less expensive; however, there may be security concerns as smartphones built for the general consumer market were not designed to be a secure criminal justice monitoring tool. For example, commercial smartphones have an accessible power button as well as compartments

2 The description of smartphone applications for community corrections in this paper draws heavily from Russo and Drake, 2017.

that contain SIM cards and batteries that can be removed. Clients also have access to other functionality such as WiFi settings and airplane mode that can allow them to intentionally avoid contact with their officer. Further, it can be difficult to control what other applications, including location spoofing or other conflicting software the client might be downloading on the smartphone. Services associated with "corporate-owned" smartphones, on the other hand, are generally more costly; however, they offer far greater security and are capable of monitoring all phone activity and restricting the individual's access to particular functionality as determined by the officer. For example, access to the Internet may be restricted or limited, based on risk level and/or compliance with conditions of supervision. Conversely, positive behavior may be rewarded by removing restrictions or increasing accessible functionality on the smartphone. Further, the officer has the capability to limit the individual's ability to call or text certain individuals or restrict activity based on a schedule. Note that some vendors who provide "corporate-owned" smartphones intend that the justice involved individual use this device exclusively (i.e., use of another smartphone is prohibited) in order to better control activity. While this may be desirable from a supervision perspective, it may be difficult to enforce in practice.

LINKING THE SMARTPHONE TO THE INDIVIDUAL

Smartphone applications have the potential to support the supervision process, however, in order for these benefits to be fully realized, the client must be in possession of - and be the person actually using - the smartphone. Vendors generally take three approaches to the problem of confirming identity and proximity to the smartphone: periodic confirmation, continuous confirmation, and a hybrid method. Periodic confirmation typically consists of an automated biometric (e.g., fingerprint, voice verification) and/or credential/password to validate identity at points where key information (e.g., location) is collected. Due to the nature of this approach it might be expected that the client may intentionally or unintentionally separate from the smartphone and "lose" contact with the officer. In these cases, extended separation would be detected when the client misses the next scheduled or random check-in or other contact. Due to the requirement for active participation on the part of the client, contacts during normal sleep hours are problematic. Therefore, this approach may be more suitable for lower-risk individuals who may not require "on-demand" contact/monitoring.

> ***One study revealed that drug-involved probationers who volunteered to receive text or email reminders about treatment goals participated in more days of treatment and had fewer days of substance use than their counterparts who chose not to receive electronic reminders.***

The continuous confirmation approach generally employs a secure, body-worn tether linked via radio frequency, with the smartphone. In this configuration, an alert may be generated if the two devices are separated or if the tether is

removed. This provides a much higher level of confidence that the client is with the smartphone and may be more suitable for moderate to high risk individuals or those who have trouble keeping the smartphone within proximity.

The hybrid approach offers multiple layers of confirmation, for example a tether combined with a biometric validation to operate the smartphone. These configurations are highly flexible and can be modified as needed based on risk level, compliance, or other considerations.

CapabilitieAs discussed, smartphones are extremely powerful and flexible computers. The community supervision applications that have been developed offer a broad range of functionality too numerous to detail here, however, below is a description of some of the more common features.

LOCATION MONITORING

By leveraging the technologies built into devices (e.g., GNSS, WiFi, cell tower trilateration), smartphone applications can be useful in determining the location of the device and the client. The location approach used is dependent upon the chipset chosen by the smartphone manufacturer, and to a lesser extent, the cellular network that the device uses. The accuracy of smartphone location services can vary due to a number of hardware and environmental factors. The quality of the chipset along with the choice and placement of the antenna within the phone are variables that are controlled by the smartphone manufacturer. Vendors that offer software applications that can be downloaded to a variety of phones (BYOD) may therefore have less control over accuracy as opposed to “corporate-owned” smartphones, though actual differences in accuracy may be minimal.

The accuracy of location data is irrelevant if there is no confidence that the client is in possession of the smartphone when the location points are taken. The frequency at which this proximity confirmation occurs constitutes the distinction between continuous tracking capabilities and periodic location sampling. Agencies will need to determine which approach best fits their needs.

CONTINUOUS TRACKING

When location information is combined with a continuous means of validating the client is with the phone (e.g., tether), much of the functionality of traditional tracking systems can be realized without the stigmatization associated with bulky ankle bracelets. In this approach, a secure, body-worn tether is connected via Bluetooth to the smartphone. The result is similar to the traditional two-piece offender tracking system, however the components are much smaller than those currently offered by manufacturers. Much like offender tracking systems, location points are gathered continuously and an alert is generated if the two devices (smartphone and tether) are separated indicating that the integrity of the location points has been compromised.

PERIODIC LOCATION SAMPLING

Solutions that periodically (i.e., no tether) confirm client identity/proximity to the smartphone are generally not as comparable to traditional tracking systems. In this configuration, the client may be prompted, by a message on the application, to conduct a check-in to confirm identity/proximity while the device's location point is captured. These check-ins can be programmed to be random, on demand, or scheduled at specific times of the day to determine, for example, whether the client has arrived at work on time or is attending a counseling session. Note, these applications may be gathering location data throughout the day; however, only those location points associated with an identity/proximity confirmation should be considered reliable. Again, because non-tethered approaches rely on a client's active participation to confirm identity/proximity to the smartphone, these check-ins are typically not scheduled during the hours the client is sleeping, creating a gap in monitoring capability. This may or may not be a major concern depending on the risk level of the client; however, agencies should understand the difference between continuous tracking and periodic location sampling.

As part of this functionality, many smartphone applications allow officers to create and monitor inclusion and exclusion zones. It should be noted that systems that use the periodic proximity verification approach appear to be much less suited to zone monitoring as compared to the tether approach. This is primarily because the client can intentionally separate from the smartphone prior to entering an exclusion zone and, in all likelihood, return and retrieve the device without detection.

Remote Reporting and Supervision

Many smartphone applications allow the client to remotely submit reports to their officer with updates of employment status, living arrangements, contact information and other important data. These reports can be scheduled by the officer on a regular basis, randomly, or the officer may initiate an immediate prompt. Further, leveraging the smartphone's camera, an officer can virtually interact with the client to conduct a "face-to-face" interview or a walk-through of the client's home, inspecting the contents of drawers, cabinets and the refrigerator.

Calendar Event Management

Clients often lead chaotic lives and can struggle to keep up with daily activities. For example, they often miss important events (e.g., court appearances, drug tests, programming) and negative consequences can ensue. In some cases, a bench warrant may be issued, and the client could be jailed until a hearing can be scheduled. Reminders can help avoid this situation; some studies have demonstrated a reduction in failure to appear rates by as much as 30 percent (National Center for State Courts, 2018). Smartphone applications can automate the reminder process. For example, an officer can populate the client's calendar with important appointments. Once on the calendar, these systems can be programmed to generate a series of reminders to the client, via the application, in an effort to improve compliance. Further, calendar events can be linked with the smartphone's location-based services to provide the supervising officer with an alert if the individual failed to appear as scheduled.

Positive Reinforcement Tool

Electronic supervision technologies (e.g., ankle bracelets) are often viewed in a negative context - as tools of surveillance and control. Smartphone applications, on the other hand, have the power and flexibility to be used to deliver positive reinforcements to the client. This can be accomplished by using instant communications (e.g., text) between the officer and the client; however, some applications can be programmed to deliver automated positive affirmations in response to desired behaviors (e.g., meeting curfew, negative drug test). One study revealed that drug-involved probationers who volunteered to receive text or email reminders about treatment goals participated in more days of treatment and had fewer days of substance use than their counterparts who chose not to receive electronic reminders (Spohr, Taxman, and Walters, 2015). Further, these applications are capable of leveraging gamification theory to incentivize client engagement. Points can be earned by the client for positive behaviors and deducted for negative behaviors, and the applications can track points and provide the client with a graphic representation of progress, tying daily actions to specific goals and milestones. Points can be redeemed for tangible rewards that are meaningful to the client such as a bus pass, movie tickets, or expanded curfew.

Connecting Clients with Resources

Smartphones can be used to connect clients to resources in a variety of ways. Any smartphone, via internet connectivity, can access existing resources such as websites that post job opportunities, information about health care, addiction treatment, mental illness, etc. Further, the client can use the smartphone to access a growing number of free or low-cost third-party applications specifically designed to deliver evidence-based interventions (e.g., cognitive behavioral therapy) to address criminogenic need areas. Research conducted on general populations have found that mobile applications have demonstrated effectiveness as interventions for issues such as substance misuse and mental disorders (Bush, Armstrong, and Hoyt, 2019).

Some smartphone applications for community supervision aggregate existing resources that are most relevant to the client (e.g., the conditions of supervision, cognitive behavioral or life-skills training materials and exercises). Other solutions go even further and offer direct support to the client through the development of new content delivered through the application or creation of support groups made up of people in the client's life who can help him/her stay on the path to success.

Regardless of whether the intervention is part of the community supervision application or stand-alone, the smartphone's camera can be leveraged to facilitate telepresence interactions with officers and treatment providers when and where the need arises.

Other Functionality

Some smartphone application solutions can be linked with a portable breathalyzer for remote alcohol testing. In this configuration, the officer can send a prompt to the client to confirm his/her identity and video record themselves

taking the breath test. Identity confirmation and test results are recorded and alerts are sent to the officer per established protocols. Smartphone applications can also be linked with third-party drug testing services to forward notification to the client that he/she is to report to submit a urinalysis sample. Finally, mobile wallet technology allows the client to securely link the smartphone to his/her bank accounts or credit cards to transfer funds to pay fees, fines or treatment costs.

CHOOSING THE TARGET POPULATION

Smartphone applications can be an extremely flexible, yet powerful, tool for community supervision. Just as with any technology or intervention, agencies will need to determine how to best leverage these new tools to achieve desired objectives. Among the key considerations are determining the client groups that would most benefit from these applications and which features should be emphasized. These decisions should be based on evidence-based practices, and in particular, client risk/needs. For example, lower risk populations or those clients who have successfully completed traditional location tracking may be well suited for the periodic or untethered location monitoring approach, whereas higher-risk clients may be more appropriate for the tethered approach. With respect to use of these applications to support behavioral change objectives, agencies should resist the temptation to over-supervise low risk clients by creating new pitfalls or opportunities to fail. Integration of smartphone applications into operations should, therefore, be in alignment with evidence-based practices.

VULNERABILITY TO CIRCUMVENTION

As with any technology, smartphone applications may be circumvented in a number of ways. A determined client can cut, remove, or electronically manipulate the tether; physically separate from the smartphone; shield or jam GPS or cellular signals; or simply fail to charge the device battery. In the case of BYOD, a client can simply turn the smartphone off, remove the battery, or disable functionality such as WiFi. In contrast, corporate-owned devices can be locked down, mitigating these risks. Further, lower quality biometric sensors (e.g., fingerprints, facial recognition) found in BYOD may be susceptible to spoofing. While these solutions are designed to alert authorities when these attempts are detected, it may be difficult to address the issues in real time. Corporate-owned devices may include advanced sensors, built for purpose and more resistant to circumvention. Agencies should consider the robustness of the solution through the lens of the risk level of the individual under supervision and the case objectives. For example, if the main objective is providing a tool to support behavioral change, these concerns may be less relevant.

Technical Issues

Smartphone applications present a variety of technical considerations that agencies should be aware of and consider. The specific issues will vary depending on whether the device is corporate-owned or BYOD. For example, connectivity is dependent upon the cellular service provider's coverage area. Insufficient coverage will result in

lapses in service. If using a corporate-owned device solution, agencies should determine whether the vendor is leveraging the cellular provider(s) that provides the best coverage in their area. Coverage areas associated with BYOD applications are more variable since the agency can't control what cellular provider is used by the client. BYOD solutions rely on the client's data plan to support the supervision related activity. When minutes or data limits are exhausted, the service may terminate.

BYOD solutions can't control for the quality of the smartphone; therefore, the performance of the hardware components (e.g., battery, camera, GPS chipset) will vary by device. This means each client using a different device will have a slightly different experience. Corporate-owned smartphone approaches will not only have more consistent coverage and hardware level control features but can also be customized to the requirements of community supervision agencies as needed.

Whether a BYOD or a corporate-owned solution is used, agencies should be aware that application can significantly impact device battery life, particularly in the case of location monitoring. Generally speaking, the device battery will discharge more rapidly as the frequency of location data points collected increases. Agencies should evaluate the impact of frequent location monitoring or sampling on device battery life in realistic operational scenarios and be aware of any methods the vendor uses to preserve battery life (e.g., the use of beacons or movement sensors) that limit location point collection when the device is at rest.

DATA MANAGEMENT ISSUES

Since smartphones are effectively mobile computers with immense processing power and ever-smaller sensors, the amount of data that can be collected is almost endless. Agencies should consider how these data will be managed and used. For example, are the reporting data a client enters via the application automatically integrated with an agency's existing case management system or does this information reside in separate silos creating additional work for the officer?

Officers may have access to unprecedented amounts of data about their clients and the ability to collect behavioral data that may allow for a systematic approach to identifying promising practice that will lead to future evidence-based practices. While this is a worthwhile goal, there is a real risk of information overload. Agencies will need to identify the data of immediate concern that are central to the supervision process and partition it from data that may be more important in research endeavors. Solutions that leverage dashboards that quickly identify and prioritize action items can assist officers manage workloads.

DATA PRIVACY AND SECURITY

Smartphones/applications have the potential to capture information about the client's medical or behavioral health. Agencies should consider how this data may be captured, transmitted and stored and create policy to

ensure they are in compliance with all relevant privacy regulations (e.g., HIPPA). Further, as sensitive information may be transmitted between the officer's device and the client's device, agencies should evaluate each solution to determine vulnerabilities to attack (e.g., hacking, spoofing, data denial) and what information security measures are in place to mitigate these risks.

LEGAL AND ETHICAL ISSUES

Smartphone applications that are used to locate and track clients may be considered a form of electronic monitoring in some jurisdictions. Agencies should therefore determine whether permission is required by a sentencing court or parole board prior to using this particular functionality. Similarly, some issues arise with respect to solutions that use the corporate-owned model. One advantage of this approach is that officers can control when and how the client uses the device (e.g., blocking certain websites, limiting who the client can call or text, denying access to device functionality during school hours). While this may be appropriate to achieve supervision objectives, agencies will need to consider potential ethical concerns such as remotely turning on camera or voice recorder functions. Further, agencies should consider whether it is possible or practical to mandate that clients use only the phone provided for supervision purposes and no other device. Finally, agencies should be cognizant of how smartphone applications, particularly those installed on the client's personal device, may impact the client's right to privacy. It is particularly important that agencies consider situations in which the device may be subject to search and seizure, thereby potentially inadvertently exposing the client to increased liability for activity that may not be related to the application. These situations should be anticipated, and clear policies should be developed to guide appropriate responses.

Implemented properly, smartphone applications can be an important community supervision tool. Smartphones and applications are ubiquitous and powerful. Further, they are extremely flexible. Agencies can determine exactly how they want to leverage the technology depending on the risk/needs of a particular case. For example, some clients may only need an easy and reliable way to remotely submit status reports to their supervision officer. Other clients may require location monitoring and remote breath tests, while still others may benefit from the telepresence functionality to participate in remote counseling sessions with treatment providers. Further, with the rapid development of applications and integrated and compatible sensors, the capabilities of smartphones are constantly evolving. These advances promise flexibility and expandability that community corrections has not yet experienced with any other tool, and it is anticipated that smartphones will play a very prominent role in community supervision moving forward.

Agencies should educate themselves on the capabilities and limitations of smartphone applications in general as well as the pros and cons of corporate-owned vs. BYOD approaches and tethered vs. non-tethered approaches. These solutions, like any other, should be implemented in alignment with evidence-based practices, focusing on the risk/needs of each case.

REFERENCES

Bush, Nigel, E., Christina, M. Armstrong, Timothy V. Hoyt, "Smartphone Apps for Psychological Health: A Brief State of the Science Review", Psychological Services, Vol. 16, No. 2, 2019.

Kaeble, Danielle and Mary Cowhig, "Correctional Populations in the United States, 2016", Bureau of Justice Statistics, April, 2018.

National Center on State Courts, "Hennepin County MN District Court eReminder System Cuts Failures to Appear", February 10, 2018.

Pew Center on the States, "One in 31 – The Long Reach of Corrections", March, 2009.

Pew Research Center, Global Attitudes & Trends, "Smartphone Ownership is Growing Rapidly Around the World, But Not Always Equally", February 4, 2019.

Russo, Joe and George Drake, "Monitoring with Smartphones: A Survey of Applications", Journal of Offender Monitoring, Vol. 30, No. 1, Spring/Summer, 2017.

Spohr, S.A., F.S. Taxman, and S.T. Walters, The Relationship Between Electronic Goal Reminders and Subsequent Drug Use and Treatment Initiation in a Criminal Justice Setting, Addictive Behaviors, December, 2015.