Pennsylvania Board of Probation and Parole Offender Management Software Pilot:

FEASIBILITY EVALUATION REPORT

September 2, 2014

Ian A. Elliott, Ph.D.

University of Massachusetts Lowell

Email: ian_elliott@uml.edu; Tel: (978) 934-4109

Gary Zajac, Ph.D.

The Pennsylvania State University

Email: gxz3@psu.edu; Tel: (814) 863-0786

Contents

Executive Summary

Ensuring effective supervision of sex offenders in the community remains of considerable concern for both criminal justice agencies and the general public alike. Law enforcement agencies are required to balance public protection, community safety, and accountability for victims with encouragement and support to promote successful reentry into the community for sex offender clients. Along with mandated registration, notification and residence restrictions, sex offenders can also be placed under further legal conditions, which can include limiting or revoking the offender's access to communications technologies (e.g., the internet).

Recent legal scrutiny has noted that limitations on internet access for sex offenders may be overbroad and unconstitutional and/or constitutionally vague (e.g., *Doe v. Jindal et al.*, 2012), and a possibility exists that all-inclusive restrictions may be themselves limited or abolished. Consequently, an approach to the supervision of computer-use is needed in which registered sex offenders can be provided with full access to communications technologies, but in a way that provides adequate monitoring. A recent series of demonstration projects in the United Kingdom evaluated the use of offender management software (OMS) as a management strategy. This approach has now been implemented in a number of regional police forces across the U.K. (e.g., London Metropolitan Police).

In light of this, a U.S.-based demonstration project was designed to investigate the possibility of a similar implementation of OMS by the Pennsylvania Board of Probation and Parole (PBPP) using technology provided by a U.K.-based software company, Securus Software Ltd. Securus OMS monitors computers for pre-defined prohibited words and phrases. When the software detects a match between a word/phrase, typed or viewed, with one from any of its active libraries it captures an image of the user's screen at that moment. These captured images can then be viewed remotely

by the monitoring agent by remotely logging into the secure server, via a management console, from any computer with internet access. The report that follows outlines a feasibility study that aimed to evaluate the success with which the PBPP was able to implement Securus OMS for registered sex offenders in targeted areas within Pennsylvania and allowed supervising agents to remotely monitor potential violations of acceptable use. The feasibility study also developed a program logic model, to clarify the expected theory of change, and a process model that outlined the various stages of implementation.

Participants were four agents from the PBPP Pittsburgh District Office, each with a current caseload of sex offender clients and the technical capability to use OMS, and seven adult male registered sex offender clients (average age = 44 years) with prior agent-imposed restrictions on access to personal computers, laptops, smartphones, and/or communications technology. Client's machines were monitored for an average duration of approximately 4.4 months. For the feasibility study, data on the captures from the OMS server were collected and analyzed and data on implementation were collected via semi-structured interviews with various individual stakeholders and via feedback questionnaires completed by client participants.

The server data provided 1796 captures from a total of 9 monitored machines - an average of 13.1 captures per day and 256.6 captures per offender - equating to 3.3 captures per day, per agent. Extrapolating frequencies at this rate estimates that an agent supervising 30 sex offenders clients using OMS would be receiving an average of almost 100 (98.2) captures per day.

Although agents remain skeptical about sex offender clients being allowed to own a computer, they reported a sense of inevitability that restricting sex offender clients' access to communications technology would become increasingly difficult and that the OMS approach had a positive impact on

their work and would be of benefit to the ongoing community management of sex offender clients. As anticipated, some problems in operational implementation were raised. These included issues around availability and attendance in training and its relationship with agents' opinions about the user-friendliness of the software, and the apparent lack of enforcement of the intended frequency and duration of monitoring and a lack of uniformity in levels of monitoring between agents. Due to OMS not capturing any new offenses during the demonstration project, it was not possible to implement or assess the procedures that would follow. Nonetheless, this feasibility study found that this OMS approach was sound and implementable in theory and those difficulties in implementation are such that we anticipate that they could be resolved through realistic changes to implementation and better communication between the various stakeholders.

Seven recommendations are made: (1) refine training methods and enforce attendance; (2) refine the libraries and make them more specific to the PBPP context; (3) establish policies and standardize practice relating to the frequency and regularity of monitoring by agents; (4) develop processes for presenting OMS evidence to provide a rationale for further investigative action; (5) seek ways in which to increase the numbers of participating agents and clients; (6) collect workload data as standard practice to examine the effects of OMS on workload; and (7) establish a future funding strategy in order to make OMS as cost-effective as possible.

It is concluded that with targeted modifications in practical implementation of the approach, the PBPP can achieve the goal of incorporating OMS into supervisory practice and to provide PBPP agents with an extra tool with which to ensure public safety – one that also has potential important pro-social benefits for the client - and thus make a valuable contribution to established methods for the supervision of sex offenders in Pennsylvania.

Introduction

Ensuring the safe and effective supervision of sex offenders in the community is of considerable concern for both criminal justice agencies and the general public alike. Sexual crimes have been linked with a series of potential long-term negative consequences for victims (Andersen, Tomada, Vincow, Valente, Polcari, & Teicher, 2008; Chen, Murad, Paras, Colbenson, Sattler, Goranson, et al., 2010) and preventing recidivism is one method by which criminal justice agencies seek to reduce sexual victimization overall. Consequently, sexual offenses typically carry substantial sanctions. In many U.S. jurisdictions, a variety of policies have been implemented to protect communities from further sexual victimization (Levenson & Hern, 2007; Mercado et al., 2008). These policies include stringent notification and registration laws and restrictions over where sex offenders can reside within the communities into which they are released (Levensen & Hern, 2007; Nieto & Jung, 2006).

In the state of Pennsylvania, the supervision of registered sex offenders on probation or parole in the community is the responsibility of the Pennsylvania Board of Probation and Parole (PBPP) or county probation/parole departments, depending on jurisdiction. Along with notification and registration conditions, sex offenders can also be placed under further restrictions based on perceived risks some specific offense-related behaviors might create. These additional restrictions can be legally mandated at a court level, at a Board level, or at an individual agent level. Under certain circumstances these restrictions can include limiting or revoking in full an offender's access to communications technologies, such as the internet.

In the midst of the recent increase in sanctions for convicted sex offenders, some commentators (e.g. Vess, 2008; Ward, Gannon & Vess, 2009) have advocated for greater consideration of the implications and consequences of those restrictions and that agencies ensure that such restrictions are proportionate to the level of risk the individual is judged to pose to commit further offenses.

Recent estimates find the base rate of recidivism for sex offenders to be low relative to other offender populations, with meta-analysis data reporting an observed overall recidivism rate of 33.2% for any new offense (*n* = 23,343; 65 samples), and a sexual recidivism rate of 11.5% (*n* = 28,757; 100 samples) (Hanson & Morton-Bourgon, 2009). Those advocating for proportionality suggest that the management of registered sex offenders should not only focus on risk reduction but also the promotion of pro-social behavior, and cite the utility of approaches that incorporate elements of positive psychology in offender management (Ward & Stewart, 2003). These approaches are concerned with the enhancement of innate capabilities and aim to reduce the likelihood of an individual committing new offenses by increasing that person's ability to improve their own life circumstances (Ward & Stewart, 2003).

Such legally-mandated restrictions on internet use for registered sex offenders have recently faced legal scrutiny, most notably in Louisiana. On August 15, 2011, an Act (LSA-R.S.14:91.5) "Unlawful use or access of social media", signed into Law by Louisiana Governor Bobby Jindal, came into effect prohibiting sex offenders from using or accessing social networking sites, chat-rooms, or peer-to-peer networks. In a civil action (*Doe v. Jindal et al.*, 2012), two Louisiana-based registered sex offenders filed a suit against the state alleging that the Act was facially overbroad and unconstitutional in that in addition to restricting behaviors that constitute criminal activity, it criminalized substantial amounts of speech protected by the 1st Amendment. They argued that the Act not only banned registered sex offenders from accessing social networking sites directly, but also made it a felony to browse websites with social networking features (i.e., comment sections, bulletin-board features, content forwarding, etc). This included sites such as NOLA.com (a Louisiana news agency), getagameplan.com (Louisiana's official hurricane preparedness site), USAJOBS.gov (the federal government's employment database), and - as noted during the trial - the website of the Court in which the case was heard. It was also argued that the Act was

unconstitutionally vague (i.e., lacks fair intelligible notice of what conduct is and is not permitted under that legislation). Federal District Judge Brian Jackson, ruled in favor of the plaintiffs and concluded that the Act was "unconstitutionally overbroad and void for vagueness".

Many states are now facing a potential scenario in which it is likely to become more difficult to apply mandated blanket restrictions on internet access for convicted sex offenders in their jurisdictions. This is based on the fact that so many facets of the internet are no longer simply static archives of information to be passively viewed, but an interactive and collaborative social environment in which to consume information and media (the so-called 'Web 2.0') (Fuchs, Boersma, Albrechtslund, & Sandoval, 2012). In his concluding remarks on the Louisiana case, Judge Jackson[1] stated that, "[more] focused restrictions that are narrowly tailored to address the specific conduct sough to be proscribed should be pursued". This can be read as a requirement for more nuanced mechanisms for sex offender supervision than all-inclusive restrictions.

Criminal justice agencies find themselves increasingly required to balance two seemingly-conflicting management principles. On one hand (and perhaps foremost), they are required to monitor and manage the conduct of sex offenders in the community in the interests of public protection and community safety, and to provide accountability for victims. This necessitates preventative measures and constraints to ensure that sex offenders cannot access potential new or previous victims, which has included revoking or restricting access to communications technologies (e.g., where there is a risk of online 'grooming'[2]). On the other hand, agencies also have a

[1] In ruling against the Act in *Doe v. Jindal*, Judge Jackson wrote, "Although the act is intended to promote the legitimate and compelling state interest of protecting minors from Internet predators, the near total ban on Internet access imposed by the act unreasonably restricts many ordinary activities that have become important to everyday life in today's world."

[2] "[A] process by which a person prepares a child, significant adults and the environment for the abuse of this child. Specific goals include gaining access to the child, gaining the child's compliance and maintaining the child's secrecy to avoid disclosure" (Craven, Brown, and Gilchrist, 2007: p. 297).

responsibility for successful reentry into the community for sex offenders. This reflects the growing view within the criminal justice system that the management and treatment of registered sex offenders should make provision for the individual's attempts to lead an offence-free life and achieve personal goals such as education and employment that may be hindered by restricted access to communications technologies.

Hence, for the supervision of computer use there is a need for a solution through which registered sex offenders can be provided with full access to communications technologies, but that simultaneously provides adequate monitoring that eliminates the perception of anonymity and provides sex offender clients with a sense of guardianship over, and accountability for, their computer use. The desired outcome of this is that it helps facilitate both the prevention of previously illegal behaviors and the development of pro-social computer user. Furthermore, it is inevitable that most sex offender clients will eventually complete their sentence and be able to obtain unrestricted, unsupervised access to the internet. So, it is hoped that any such approach would also increase supervising agents' confidence that their clients have been given every opportunity to learn and demonstrate the skills, the appreciation, and the motivation to use communications technologies appropriately beyond their formal supervision period.

Offender Management Software

Over the past five years, a series of demonstration projects based in the United Kingdom sought to develop a solution that bridges the two offender management responsibilities described above, through the use of offender management software (OMS) provided by a commercial entity, *Securus Software Ltd.* (see Elliott, Hughes, & Findlater, 2010). Registered sex offenders in the U.K. with prior internet-related offenses were given unrestricted access to the internet, but on a court-mandated condition that any machine that they possessed must have Police-approved OMS installed. A pilot

evaluation of implementation concluded that OMS could be used to successfully augment offender management strategies and that the approach "appeared to promote a positive, cooperative relationship between registered sex offenders and their monitoring officers… creating conditions where computer use can be reintegrated into the lives of individuals about whom the police would naturally be concerned" (Elliott et al., 2010: p. 245).

Securus Offender Management Software

Securus Software's OMS was developed from a product originally intended for school networks to counter issues such as exposure to pornography, cyberbullying, and the potential solicitation of children by adults, on schools' internal and external computer networks. In brief, Securus OMS, when installed on a machine, monitors that machine for prohibited words and phrases, both online and offline, and regardless of source. It alerts network monitors to violations of pre-defined acceptable use policies. When the software detects a match between a word/phrase typed or viewed with one from any of its active libraries, held externally on a server, it captures an image of the user's screen at that moment and records it together with other evidential information (e.g., computer name, user name, date, time, etc.). These captured images can then be viewed remotely by the monitoring agent by logging into the secure server, via a management console, from any computer with internet access.

How Securus OMS works

Securus OMS consists of three elements: (1) cloud/server storage; (2) client software; and (3) a web-based management console (see Figure 1).

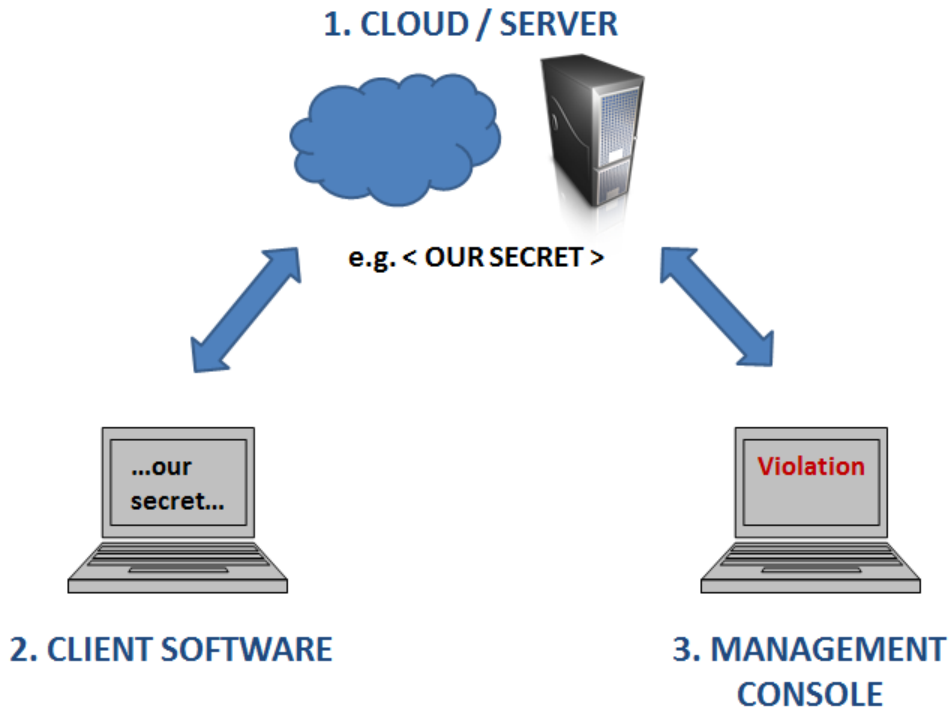


Figure 1. A schematic map of Securus Offender Management Software.

The **server** (or cloud computing[3]) provides the central monitoring and control database and receives data from the client software. The server contains various databases (referred to as 'libraries') of key terms and phrases that are to be considered to be exemplars of inappropriate behavior and constitute violations of the monitoring organization's pre-defined acceptable use policies for their computers. Figure 1 shows the example of "our secret" from the library related to 'Grooming' behaviors. The server also simultaneously holds data collected from any machines on which the client software is installed and makes that data accessible to appointed monitors via the online management console (both described below). All servers were hosted in a secure data center, therefore no data is accessible and cannot be altered or deleted, including during transmission.

[3] Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction (Mell & Grance, 2011)

The **client software** is installed directly onto any machine that is to be monitored. The software monitors that machine for any the terms or phrases that are contained in the libraries held on the server and considered unacceptable use. The software also monitors all sources for these violations of acceptable use, both online (e.g., chat-rooms, websites, emails, and any other online resource) or offline (Microsoft Office programs, CD-ROMs, USB memory sticks, etc.). When the client software detects a match with a word or phrase in any active libraries, it captures an image of the user's screen at the time of the event and records it together with the user name, machine name, date/time, and other evidential information, all of which is then transmitted back to the secure server (or cloud). The software also alerts monitors to any access to 'proxy anonymizer' sites that can be used to bypass traditional security such as internet filtering and blocking solutions.
In addition, the software records usage statistics, which include a log of time and duration of access, as well as a log of websites visited.

The **online management console** is a web-based user interface that allows those who manage the network (in this case the PBPP Probation/Parole Agents) to securely access the data on the server by logging-in from any computer with internet access, regardless of their location or machine. Via the console, network monitors are able to view directly images of any captures (and related evidential data) generated by each machine, access internet histories and sites visited, and generate reports of trends in the data.

Databases/Libraries

Securus OMS is reliant on the libraries on which it operates for operational success. Operationally-useful monitoring is dependent on high levels of both *sensitivity* and *specificity*. For Securus OMS, the sensitivity of the libraries is dependent on correctly including terms and phrases that *are* violations of acceptable use policies, ensuring that agents are being alerted to behaviors that are

relevant to risk management (a high *true positive* rate). The specificity of the libraries is dependent on correctly excluding terms and phrases that *are not* violations of acceptable use policies, and thus ensuring that agents are not being alerted to behaviors that are irrelevant to risk management (a low false positive rate). The aim is to produce libraries with the highest possible levels of sensitivity and specificity.

Securus OMS's libraries are under constant review, having been initially developed for use in schools in collaboration with the Internet Watch Foundation[4] (IWF), the Lucy Faithfull Foundation[5], and U.K. law enforcement agencies. They are not available in the public domain. As part of this demonstration project (following the implementation used in the U.K. pilots) the following sex offender-specific libraries, along with Securus' general libraries (i.e., 'Hacking', 'Swearing' [profanity], 'Drugs', 'Weapons', etc.), were utilized (see Table 1 for examples of words and phrases in these libraries):

1. **Grooming** – capturing phrases relating to the potential grooming of children on the internet;
2. **Pornography** – capturing popular search terms for both adult and child pornography;
3. **SMS/text language** – capturing the use of slang words that could indicate grooming or pornography.

These libraries were chosen with the specific intention to generate a greater volume of captures that would allow agents to experience and identify potentially-relevant and potentially-non-

[4] A U.K.-based non-profit internet 'watchdog' organization (https://www.iwf.org.uk/).
[5] A U.K.-based non-profit child protection organization, who specialize in online protection of children and working with individuals who have been charged with internet-related sex offenses (http://lucyfaithfull.org/).

relevant information, and thus judge sensitivity and specificity, with an aim to making the system more efficient in the future[6].

The Securus OMS system also incorporates the *Image Analyzer* tool, an independently-developed software engine that scans the composition of media content to identify attributes that indicate the content may be pornographic. Images that Image Analyzer has identified as potentially pornographic are also captured by the client software and provided to network monitors via the online management console.

Data collection and handling (software)

The software records usage statistics, which include a log of time and duration of access, as well as a log of websites visited. This data is held on a secure, tamper-proof, and encrypted server and violations can only be accessed by participating PBPP agents. In 2012, successful security tests were conducted by a separate independent U.K. Police Force as part of the second OMS management pilot with the Hampshire Police Force in the U.K. and found it to be sufficiently secure as for the data held within to be considered evidential in legal proceedings (in the U.K.). A copy of all data held on the server was provided to the evaluation team at the end of the pilot project period. The PBPP works under confidentiality regulations that they do not release any information specific to individual clients – although it was recognized that this could be possible given the nature of what Securus OMS does.

[6] In the U.K. OMS terms and phrases are now being incorporated into one 'Public Protection' library.

Feasibility evaluation

Feasibility evaluations are an integral part of project development. Developing new interventions, particularly in the context of criminal justice, from an idea to full operational status is a challenging, resource-intensive, and costly undertaking. New interventions can include operations that differ from standard practice and are unfamiliar to management, staff, and clients. Pilot projects and feasibility evaluations allow organizations to preview and assess potential implementation and outcomes for promising interventions and assist decision-makers in considering strategic goals, methods of operation, practical utility, potential for success, and possibilities for expansion. Feasibility studies can be theoretical or practical in nature - evaluating either hypothetical or small-scale operations in advance of implementation – but essentially represent a performance assessment of the initial assembly of all of the elements of an intervention when drawn together for the first time.

The following sections describe a feasibility evaluation of the PBPP's demonstration project into the use of Securus OMS to monitor the computer use of registered sex offenders in Pennsylvania. In September, 2012 a delegation from Securus presented the concept of their OMS approach to the PBPP in Harrisburg. The same month the PBPP received authorization to develop a pilot project of OMS with PBPP agents and sex offender clients. A memorandum of understanding was signed between the two parties and in late November, 2012 preliminary testing of the OMS server was conducted. Two sections of training of PBPP management and agents took place in early February, 2013. The first client participants had OMS installed onto their machines in April/May, 2013. The duration of the pilot study was such that each participant was placed on OMS for approximately 5 months (between May and November, 2013).

Aims and objectives

The overall aims of this feasibility evaluation are: (1) to appraise the viability and practicality of installing Securus OMS on the machines of registered sex offenders in targeted areas within Pennsylvania and of allowing supervising agents to remotely monitor subsequent potential violations of acceptable use; (2) to assess whether the use of Securus OMS has the potential to augment and enhance both the agents' ability to supervise registered sex offenders and the client's attempts to develop positive online behaviors; and (3) to provide a model for the theory and implementation of Securus OMS and the ways in which data can be derived to assess its utility in this context.

Feasibility evaluation objectives

1. Map aims and objectives of the Securus OMS approach and formulate a program logic model (identify *intended* implementation);
2. Assess legal, operational, technical, and resource/schedule feasibility (identify *operational* implementation);
3. Examine the outcomes (i.e., captures) related to clients who participate in Securus OMS monitoring;
4. Combine (1) and (2) to assess the congruence between the logic model and initial program operations, deriving initial conclusions about the success of implementation;
5. Make recommendations for future development of implementation and best-practice.

This feasibility evaluation and its methods were approved by the Institutional Review Boards of both the Pennsylvania State University and the University of Massachusetts Lowell.

Stakeholders

There were three main stakeholder groups identified in this feasibility evaluation. They are listed as follows, in no particular order or hierarchy between departments, with the titles of those individuals directly involved in parentheses:

1. **Pennsylvania Board of Probation and Parole**
    - Central offices
        - Re-entry & Quality Assurance (Deputy Executive Director)
            - Transition Services and Staff Liaison Division (Director)
        - Evidence-Based Program Evaluation Office (Director)
        - Probation & Parole Field Supervision (Director)
    - Pittsburgh Regional Office (Deputy Executive Director)
        - Special Needs Unit (Supervisor; individual agents)
2. **Securus Software Ltd.**
    - Senior Management (General Manager and Operations Manager)
    - Safeguarding Consultants (both ex-law enforcement officers)
    - Technical Support Team
3. **Sex offender clients**.

The PBPP management and Securus Software Ltd. are considered to be service *providers*, who supply the people, the financial resources, the range and wealth of expertise, and the technology and equipment that the demonstration project required. Much of the communication in terms of implementing the demonstration project appeared to flow between the Transition Services and Staff Liaison Division at the PBPP Central Offices, the Securus Safeguarding Consultants at Securus Software Ltd., and the Special Needs Unit at the Pittsburgh District Office. The agents and clients

were considered to be service *users*, as they were those who materially interacted with the technology and were the intended recipients of program operations.

It is worth noting that the communities in which the sex offender clients reside could also be considered a potential fourth stakeholder group, and considered to be service *beneficiaries*, as they provide the environment in which the service was operated and may experience incidental effects from any observed outcomes for clients and PBPP agents.

Participants

For the purpose of this feasibility evaluation, the 'participants' in the demonstration project were deemed to be: (1) the agents who would be using the software to monitor their clients; and (2) the sex offender clients themselves.

PBPP agents

Agent participants were four PBPP agents that were determined to meet the criteria for inclusion (i.e., those that had a current caseload that includes sex offender clients, had enough offenders who qualify for inclusion, and had the technical capability) who agreed to participate in the project. These agents were based at the PBPP Pittsburgh District Office, who hold jurisdiction over a major metropolitan area. This was deemed suitable to provide the greatest potential number of client participants. Because there existed a possibility that agents may be exposed to material that can be distressing (e.g., bad language, pornography, child pornography), it was ensured that agents who participate have experience working on cases related to sex offenders.

Sex offender clients

Client participants were recruited on a voluntary basis and comprised seven adult male registered sex offenders all of whom had prior agent-imposed (as opposed to Board-imposed or court-imposed[7]) restrictions on access to personal computers, laptops, smartphones - particularly those with internet access or a built-in camera - and/or communications technology (see Table 1 for demographic information). Clients were selected by the participating PBPP agents from their caseloads. The demonstration project was promoted in a variety of sex offender treatment groups and moderate estimates were that approximately 100 offenders were made aware of the possibility of participating.

Clients chosen were those that had an agent-imposed condition restricting internet use, and having an internet-related sexual offense was not a necessary criterion for participation. The average age of client participants was 44 years of age, the majority was judged to be low risk on the Level of Service Inventory – Revised[8] (LSI-R) risk assessment tool, and participants were under PBPP supervision for a range of sexual offenses. Client participant's machines were monitored for an average duration of 137 days (approximately 4.4 months).

For the demonstration project, participants were required to sign a release form stating that they formally agree to have Securus software on their computer and that they were aware that this software would monitor all and any computer use for the duration of the demonstration project. Clients were informed at that time that personal data and information may be collected by the software and held on servers hosted by a third-party in the U.S. (funded by Securus). Client

[7] It was decided early in the pilot project development process that including those with court-imposed or Board-imposed restrictions would be difficult as these would require the PBPP to request a court or Board decision.

[8] The LSI–R is a quantitative actuarial assessment that measures offender attributes and situations relevant to level of supervision and treatment decisions, and is designed to predict parole outcome, success in correctional halfway houses, institutional misconducts, and recidivism.

participants were informed that they had the right to withdraw from the demonstration study, to have the software removed, to have their data destroyed, and that they could return to their original probation/parole conditions relating to their internet use. It was also made clear that neither their decision to take part, nor any later decision to withdraw, would affect their relationship with any of the institutions involved in the pilot study and would not affect their legal circumstances.

Table 1. Demographic details for client participants.

Code	Gender	Age	Offense	LSI-R grade	# Home Visits
1	Male	30	Involuntary Deviate Sexual Intercourse	Low	3
2	Male	76	Indecent Assault	Low	4
3	Male	48	Indecent Assault	Low	1
4	Male	27	Obscenity	Low	2
5	Male	46	Involuntary Deviate Sexual Intercourse	Low	3
6	Male	51	Involuntary Deviate Sexual Intercourse	Medium	2
7	Male	32	Rape	Medium	0

For this feasibility evaluation, again, each client participant was required to sign a written consent form that outlined the purpose of the evaluation and the procedures that would take place. Each client participant was informed that they had the right to withdraw from the evaluation segment of the demonstration project, to have their data destroyed. It was similarly made clear that neither their decision to take part, nor any later decision to withdraw, would affect their relationship with any of the institutions involved in the evaluation. It was also made clear that any data that was to be collated would be anonymized so that they would not be personally identified, but that this meant

that they would no longer be able to personally withdraw once their data could no longer be identified.

Data collection strategy

Members of each of the groups of stakeholders were invited to provide data for this feasibility evaluation. Semi-structured interviews were conducted, the key elements of which can be described thusly (the questionnaires are available as Appendices 1 and 2):

- What are the aims, objectives, and intended outcomes of this project and how effectively were the communicated to service users?
- What were the short-term and long-term benefits of OMS to policy and procedure at PBPP?
- What policies and procedures were developed and how effectively were they followed by service users?
- How user-friendly was the OMS and were service users able to use it effectively?
- What measurable outcomes did OMS generate and what utility did these outcomes provide to augment traditional management for PBPP clients?
- Was there a perceived future demand for OMS and how might it be improved in order to ensure best-practice?

Interviews were conducted with senior management (n = 2), participating agents (n = 4); and a legal representative (n = 1). Client participant feedback forms (See Appendix 3) were supplied to all clients involved in the pilot project. Two separate waves of forms, all supplied with a pre-paid, addressed envelopes were delivered to clients via the PBPP office.

Data collection and handling (participant information)

All hard copy data collected as part of the feasibility study (e.g., surveys, forms, etc.) were stored in a locked cabinet at the University of Massachusetts Lowell. All digital data were held on a secure encrypted laptop computer at the University of Massachusetts Lowell. These data was considered to be confidential, but not anonymous as it was necessary to link data to the user/computer name of the client participant and their respective supervising agents. Only individuals listed as principal or co-investigators had access to either the hard or digital data.

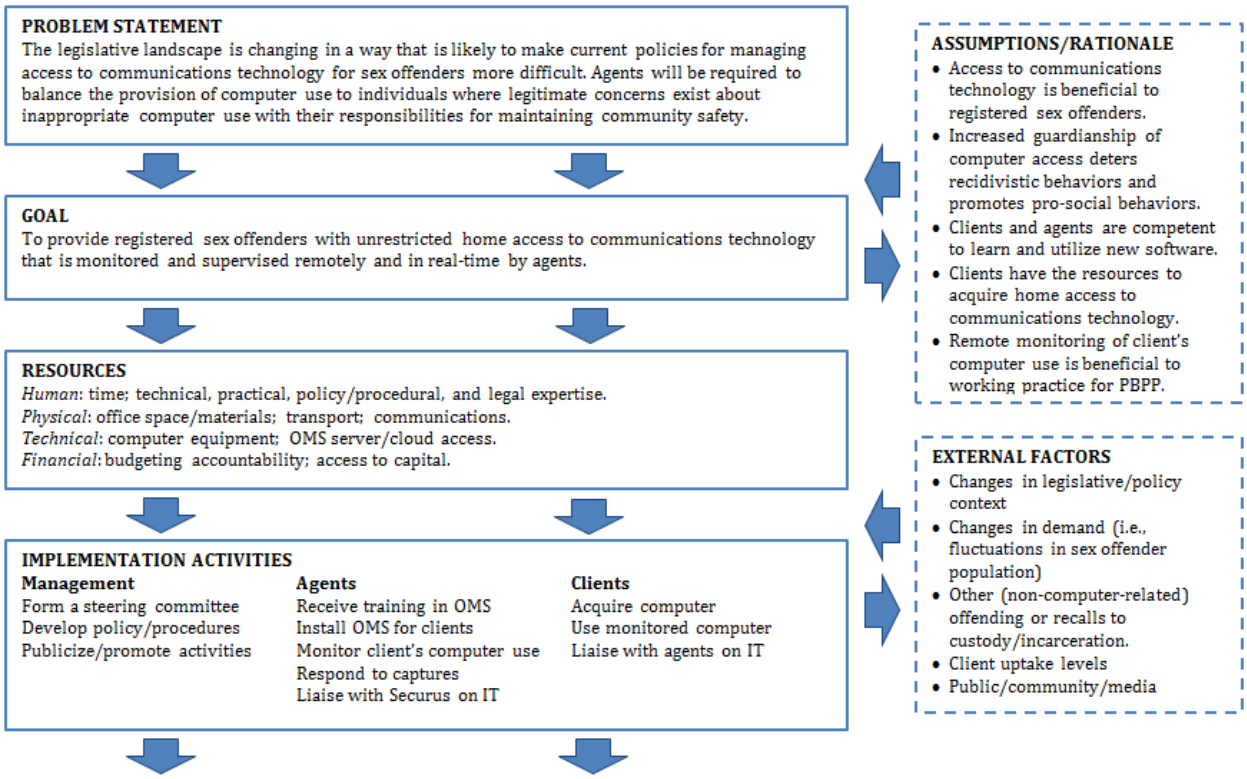
Intended OMS theory

The following sections outline an intended theory for the implementation of Securus OMS as a means to augment traditional supervision of sex offenders and their computer use. These sections outline the management structure that was put in place, the logic model (i.e., the theory of how the service should affect the behavior of the service users and the outcomes that should be expected), and a process model of the procedures by which the service should operate.

Logic model

Assessing the feasibility of an intervention requires clear definitions of the target population, definitions of the problems and outcomes that are to be the focus, clear presentations of the theoretical assumptions that guide decision-making, and the provision of a systematic framework for future evaluation (Savaya & Waysman, 2008). Logic models provide a clear and concise systematic visualization of the various elements of an intervention: the relationships between the means with which you operate your intervention, the activities you plan to engage in, and the changes and results you hope to achieve (W.K. Kellogg Foundation, 2006). The purpose of a logic model is to provide stakeholders with a theoretical framework to understand how the intervention functions and how these functions generate solutions to the problem being addressed.

Figure 2 below outlines a basic logic model for the use of Securus OMS to monitor the computer use of sex offenders. This logic model outlines: (1) a statement of the problem that the OMS approach seeks to solve; (2) the overall goal of OMS monitoring for sex offenders; (3) the assumptions made in applying this solution; (4) the external factors that have the potential to affect implementation; (5) available resources and intervention activities; (6) the intended results, describing the anticipated short-, medium-, and long-term outcomes.



OUTCOMES		SHORT TERM	MEDIUM TERM	LONG TERM
AGENTS	KNOWLEDGE	Increased awareness/exposure to risks related to computer use.	Greater nuance in understanding of risks related to computer use.	Comprehensive understanding of risks related to computer use.
	PRACTICE	Ability to *identify* risk. Reactively respond to new offending.	Ability to identify *changes* in risk over time. Reactively respond to risky behavior.	Ability to identify *antecedents* to risk. Proactively respond to risk antecedents/changes over time.
	WORKLOAD	Remote monitoring of clients and access to data.	Ability to manage tasks (e.g., home visits) where appropriate.	Increased efficiency in use of workload and resources.
	ATTITUDES	Shared accountability/ responsibility for risk related to computer use.	Improved communication of risk decisions to/from clients.	More inclusive professional relationships with clients.
	SKILLS	Improved engagement with technology.	Customization of technology and generation of reports.	Comprehensive incorporation of technology into everyday practice.
CLIENTS	ACCESS	Access to immediately beneficial services (housing, communication, treatment).	Access to medium-term beneficial services (education, training, employment).	Increased economic/pro-social activity; reduced dependence on government services.
	KNOWLEDGE	Awareness of own risk perception.	Understanding own risk and identifies recidivistic behaviors.	Reduction in recidivistic behaviors (and reoffending).
	BEHAVIOR	Increased guardianship; reduction in anonymity in computer use.	Development and demonstration of pro-social computer use.	Increased pro-social computer use.
	ASPIRATIONS	Shared accountability/responsibility for risk related to computer use.	Increased perception of self-efficacy and agency in risk related to computer use.	Increased self-esteem and responsibility for computer use.

Figure 2. A proposed logic model for OMS implementation at PBPP (see Appendix 4 for a larger-text version of this figure).

Process model

The 'Implementation Activities' section in the logic model above differentiates between management, agent, and client activities, but in practical terms the stakeholders were part of a series of interactive processes. Seven separate consecutive implementation processes were identified in the demonstration project: (1) establishing the OMS approach; (2) identification and selection of agents; (3) agent training; (4) selection of sex offender clients; (5) software installation; (6) ongoing monitoring and responses; (7) termination. These are described in greater detail, and in the order in which they occur, below.

Establishing the OMS approach

1. An informal steering committee is formed that included.
2. The steering committee develops links with OMS provider (in this instance Securus OMS) to develops and sign a memorandum of understanding (MOU).
3. Members of the steering committee promote the approach to management in regional field divisions.

Identification and selection of agents

4. Management in regional field divisions identify field agents in their division who:
    a. have current caseloads that include sex offender clients;
    b. have clients whose supervision terms are of a sufficient duration for them to participate in Securus OMS monitoring;
    c. have clients with the resources to acquire home access to communications technology.
5. Agents who meet the criteria for inclusion are given an introduction to the aims and objectives of the Securus OMS approach and are invited to participate.

Agent training

6. Participating agents receive training on the use of Securus OMS, via an online webinar delivered by the Securus' training provider, in two sections:
    a. Section 1: Awareness of the software; training on the installation of the client software; familiarization with the captures console.
    b. Section 2: Managing captures; practical case studies from law enforcement officers who use the system to manage offenders.

Selection of sex offender clients

7. Agents select clients on their caseload who meet the selection criteria. The basic criteria in the demonstration project were that clients should:
    a. have current agent-imposed restrictions on computer and/or communications technology use;
    b. have requested access to communications technologies or have stated their wish to acquire a computer for home use;
    c. have the means to acquire the required hardware and technology;
    d. be willing to consent to having Securus OMS installed on any computer to which they have personal access.

Software installation

8. Agents install the software on machines of selected sex offender clients on their caseload. Installation of the software was carried out using a USB drive containing an executable installation file. The Securus Support Team should be on hand to assist with installation should any problems or issues occur.

Ongoing monitoring and responses

9. Agents access the online management console to assess captures on a daily basis (at least) to allow agents to respond to violations of acceptable use with swiftness and certainty. Assessing captures should not take any longer than 30 minutes per session at the most.
10. Agents are encouraged to maintain a log to record the amounts of time spent accessing the console, dealing with issues arising, and to record how many captures were marked as serious, minor, or are saved.
11. If a client is detected as having committed either a new offense or a violation of license conditions, agents follow established protocol and chain of command and investigate and obtain any necessary information in order to pursue the matter further.

Termination

12. If a client is returned to custody/incarceration, has completed their license, or is no longer considered suitable for OMS monitoring (e.g., no longer requires/has the means to own a computer, is re-incarcerated, has health problems, etc.), the supervising agent will uninstall the software from the client's machine.

Legal context

The legal departments at PBPP found no legal constraints on the Board's use of OMS to monitor the computer use of its sex offender clients. The PBPP's legal representatives noted that any OMS monitoring would need to comply with 4th Amendment rights to privacy and freedom from unreasonable searches and seizures of individuals or property by law enforcement officials. They advised that Securus OMS would not be restricted by 4th Amendment rights on the basis that that supervised offenders have a reduced expectation of privacy in their actions and behaviors and since (a) Securus OMS does not represent clients being under constant supervision by PBPP agents –

agents only receive data when unacceptable use occurs and (b) that the participants provided their consent to be monitored by Securus OMS. The PBPP legal representatives also advised that Securus did not violate either HIPAA (Health Insurance Portability and Accountability Act) or CHRIA (Criminal History Records Information Act) regulations, as the PBPP is not *providing* personal data to another agency (i.e., Securus) and any personally-identifiable data captured by OMS is accessible only to PBPP agents. The PBPP legal representatives also noted that their MOU with Securus Software Ltd. ensured that if there were any litigation (i.e., civil or legal action) between the PBPP or Securus pertaining to the use of OMS that this litigation would be handled in the U.S and under U.S. law.

Securus OMS does create a potential for third-party monitoring (i.e., the incidental monitoring of others who use the monitored machine or others who have communicated with the monitored individual). Securus OMS monitors 'the machine' not the individual; therefore signed informed consent was obtained from other household/family members who may be at risk of having their computer use inadvertently monitored by PBPP agents. It is important that the scope of monitoring remains focused on the client and does not place undue restrictions or burdens on other individuals within the client's life (i.e., family and friends). A balance is required where non-client individuals need to be made aware that the machine is being monitored, but in a way that does not advertise the fact that the client is a registered sex offender.

Data capacity (captures)

The PBPP capture database from Securus provided data on 1796 captures from a total of 9 monitored machines for 7 sex offender clients. This calculates as an average of 13.1 captures per day and 256.6 captures per offender overall. Across four participating agents this also equates to

3.3 captures per day per agent. Although these numbers appear small, it should be noted that this is for a very small sample of offenders (*n* = 7) and extrapolating frequencies at this rate it could be estimated that an agent supervising 30 sex offenders clients on Securus OMS would be viewing an average of almost 100 (98.2 to be precise) captures per day across their caseload.

Table 2. Proportions of captures by Securus OMS library.

Library	**Frequency**	**Proportion**
Bullying	23	1.3%
Drugs	90	5.0%
Gambling	17	0.9%
Grooming	173	9.6%
Hacking	898	50.0%
Porn	86	4.8%
Porn Image	15	0.8%
Racism	75	4.2%
Swearing	219	12.2%
Terrorism	6	0.3%
Weapons	194	10.8%
Grand Total	**1796**	

It should, however, also be noted that proportions of captures were not uniform across machines. One machine was responsible for 54.6% (980) of all captures, and other machine responsible for 24.2% (435) and supervising these two clients alone would equate to an average of 10.3 captures per day. If it were the case that one agent was supervising 30 clients creating captures at these rates, they would be viewing an estimated 154 captures per day. Furthermore, if this scenario

happened to be two machines owned by the same client and the agent was supervising 30 clients creating captures at this rate, they would be viewing an estimated *308* captures per day.

As can be seen in Table 2 the majority of captures were related to the 'Hacking' library. In fact, 73% of all captures were related to one of the 'Hacking', 'Swearing', or 'Weapons' libraries. It should be noted that these libraries may not be specifically relevant to sex offender management. However, that almost 10% of captures were related to the 'Grooming' library suggests that the system is capturing sex offender-relevant behaviors (although, this is not to assume that these captures are evidence of 'risky' or recidivistic behaviors).

Table 3. Proportions of captures by source.

Source	**Frequency**	**Proportion**
Keyboard	30	1.7%
Application	1751	97.5%
Image Analyzer	15	0.8%
Total	**1796**	

Table 3 shows that the overwhelming majority of captures were taken from applications (i.e., internet browser, word processor, game consoles, Skype, etc.) as opposed to being typed in to the computer. This has implications for legislative issues of 'overbroad' supervision as, for example, the data shows that none of the captures from the 'Grooming' library has a keyboard source. If the rationale for the inclusion of that library is to detect clients who are using their computer to solicit

potential victims online, then these captures should reasonably be expected to occur via keystrokes.

As shown in Table 4, the majority of the captures were of a severity level between 51 and 100[9].

Table 4. Proportions of captures by severity level.

Severity level	**Frequency**	**Proportion**
0-50	416	23.2%
51-100	1363	75.9%
101-150	9	0.5%
150-180	8	0.4%
Total	**1796**	

[9] Examples of terms and phrases at these security levels were 'asshole', 'gonna get you', 'touch me', and 'stop program'.

Operational feasibility

Although many of the agents remained skeptical that sex offender clients should be allowed access to computers, there appeared to be a sense of inevitability among stakeholders that revoking or limiting access to communications technology for sex offender clients will become increasingly difficult. Stakeholders noted that access to the internet has become a prerequisite to modern life in the U.S. and that communications technology is a ubiquitous feature in people's lives. Thus, many stated that novel methods for dealing with clients' computer use would become increasingly necessary and that therefore having an opportunity to monitor that computer use for those clients with the means to acquire machines was viewed positively.

The vast majority of the PBPP management and agents that we spoke to were enthusiastic about the OMS approach, believed that it did have a positive impact on their work, and felt that it would be of benefit to consider in the future in the ongoing community management of sex offenders. There were, however, some practical issues in implementation that were raised by stakeholders who volunteered feedback. The issues related to operational practice, including both aspects that found to be positive and areas where improvements could be made, are outlined and discussed in the sections below.

Agent training

Those agents who attended the training considered it to be comprehensive and adequate to allow them to install the software and appropriately and successfully use the online management console. However, not all PBPP agents with clients being monitored by Securus OMS were able to attend the formal training webinar (mostly due to work commitments). Some of these agents were essentially trained by other PBPP staff who had attended the webinar, while others participated in the

demonstration project with no training. It was of note that those agents that were able to attend the training webinar were also those who found that the management console to be particularly user-friendly in terms of getting access to the data and information that was of interest to them. Thus, dissatisfaction with OMS on an operational level was likely to be a result of a lack of training.

Not ensuring that all agents participating in the demonstration project attend training would likely have serious implications for successful implementation. It appears that the PBPP did not stipulate or enforce mandatory attendance for OMS training. However, it is also the case that, presumably for legitimate financial and resource reasons, Securus provided that training from the U.K. via webinar rather than in-person in the U.S., and that only one occasion of each of the two sessions was provided (although additional training was offered if individual agents felt they required it). In this instance the webinar format was preferred by Securus for its flexibility and timing. However, it may still have been difficult for participating agents to attend specific sessions. Also the remote nature of the training meant that agents were not assessed or advised while applying, under working conditions, their understanding of the functions and features of the software (although it could be argued that this is a limitation to many training formats in general).

Software installation

Agents found that the software was easy to install on clients machines, and in the few circumstances where agents had problems with installation they reported that they were able to contact the Securus Support Team and these issues were dealt with promptly and successfully. Agents also reported that in the earlier cases OMS-trained PBPP management were available to go with them and assist in the installation the software.

Ongoing monitoring

Most agents reported successfully using the management console to access captures and other related information. The interface was described by agents as excellent and the ability to view screenshots was highlighted as a useful feature. There were, however, some practical issues. Some agents reported finding the use of the management console difficult and were not familiar with the features available to them – although, as noted above, this was usually linked to non-attendance in training and those who reported non-attendance highlighted this as a hindrance to their ability to use the software more effectively. Some agents reported that they found it difficult to clarify what information they were being presented with, which data were related to which client, and where and how to access the information that would be relevant to them in terms of providing supervision – either more generally (e.g., pornography use) or specifically (e.g., offenders with minor victims accessing websites for toy stores).

Furthermore, the intended frequency and duration of monitoring did not seem to be enforced. Some agents reported logging-on to the management console frequently and regularly, whereas others reported logging-on infrequently and sporadically. It was apparent that agents were not accessing the management console on a daily basis. Some agents reported that they began the demonstration project logging-on regularly (although, even then around once a week for 30 minutes to one hour) but that this regularity waned as agents encountered large volumes of data and found it difficult to differentiate between clients and/or relevant and irrelevant data.

The implications of any pliability in the consistency of monitoring depend on who is responsible for setting the criteria and boundaries for monitoring. One viewpoint is that OMS is regarded by the PBPP as a formal responsibility for participating agents and a required element of their supervisory practice. If the PBPP takes this viewpoint for OMS, then a failure in the enforcement of regular

monitoring of captures by agents occurred in this demonstration project and there needs to be put in place a clear policy for frequent and regular use (e.g., a specific, realistic number of minutes per day) and agents should be held accountable for adhering to the conditions of this policy. A second viewpoint is that OMS is regarded by the PBPP as a flexible tool available for participating agents to incorporate into their supervisory practices as they see fit. If the PBPP had this latter approach in mind for OMS, then there was no issue of regular monitoring in this demonstration project. In this case, however, that viewpoint should still be formally recognized and agents should be made aware that they are responsible for setting their own criteria and boundaries.

Responding to violations

Agents noted that the key practical priority for them in terms of violations was to be able to view captures and be provided with *immediately-actionable intelligence*. There were, however, no violations of acceptable use demonstrated on any of the machines of clients who participated in the demonstration project, meaning that it was not possible in this feasibility evaluation to determine how agents would be likely to respond to violations of acceptable use. Nonetheless, the knowledge that clients are not (or at least appear not to be) accessing sites that might concern their supervising agents remains valuable knowledge and potentially a positive outcome for the demonstration project (although it should be noted that this was not an outcome evaluation).

The agents stated that although it is actually unlikely that Securus OMS would change their overall assessments of clients' risk levels, that both participation and particularly *successful* participation was evidence of compliance with supervision, which is an important component in assessments of offender risk. It was also noted that if clients who have agreed to participate in OMS monitoring are found to have computers (or smartphones) that are not being monitored, then agents may feel the more comfortable assuming that these machines are possibly being used for unacceptable activity.

One agent noted that currently, should they have some suspicion that a client is engaging in illegal online behavior – perhaps based on items within their web history – the computer would be sent to the Attorney General's office who have approximately 4 technicians for forensic analysis for the Western PA region (covering around 10-15 counties) and it can take months before they receive any information on what online data were being accessed. The ability to be able to generate and present evidence immediately that would allow agents to request further investigative activity would be highly beneficial. It also creates a scenario in which clients are aware that their behavior is instantly actionable – and that simply deleting their internet history in the anticipation of a home visit will no longer conceal unacceptable computer use.

In terms of actionable intelligence, the agents feedback suggested that there were too many false-positives, which not only took time to examine, but also constituted 'noise' that obscured the context as a whole and made it increasingly difficult to identify relevant material. As outlined above, false-positives are a marker of the *sensitivity* and *specificity* of the OMS system and it is apparent that the libraries were neither sensitive nor specific enough to maximize the benefits for PBPP agents. It is noted that for this pilot the sensitivity and specificity were set lower, in order to generate data, as was the case in the U.K pilots – the assumption being that it is easier to refine a larger quantity of data (reduce irrelevant data) than to generate less data and miss relevant data, particularly data the relevancy of which may not be known until it is experienced (i.e., the 'unknown unknowns'). Thus, refinement of the libraries specifically for the PBPP would be needed for any future implementation.

Client feedback

Only one client participant provided feedback. Thus, in order to maintain a level of anonymity, we provide here simply the 5 key points that permeated the responses: (1) that there was little

communication of the project's rationale, aims, and the data it collects - and that boundaries of appropriate and inappropriate behavior were not explained (but seemed to be reasonably easily assumed); (2) that the software was unobtrusive and operated correctly; (3) that the positive outcome of getting internet access and potentially reducing home visits outweighed the somewhat negative effects on privacy and feelings of obligation to take part; (4) that it did appear to have some deterrent effect against inappropriate computer use; and (5) that although this approach may be a relevant one for most sex offenders, assessment in selection should be a major component.

Other feasibility issues

The following section outlines a number of issues that were not directly related to the implementation process within OMS intended theory and processes could have a significant impact on the ability to implement OMS in the future.

Deception

The OMS system relies on the client only using machines known to the PBPP and that have had OMS installed on them. As such, the potential that clients may have attempted to disengage or circumvent the software could not (and cannot in the future) be ruled out. Offenders could seek to bypass Securus OMS monitoring through one of (or a combination of) two principal methods. First, *technical* methods can be used, that involve changes to hardware or software on the machine to circumvent the scope of OMS or by limiting the ability of OMS to identify data as text. To counteract technical methods Securus training includes the identification of, for example, hardware changes. Secondly, *physical* methods can be utilized, for example by using an unrelated machine that does not have the software installed to engage in inappropriate behaviors, without the knowledge of

monitoring officers. To counteract the suspicion of the use of machines without OMS installed, a handheld electronic device can be used to identify how many devices are connected to a wireless network (a common networking configuration) in order to detect potential alternative machines using the offender's network.

There are, and always will be, methods by which offenders can circumvent monitoring in any form and thus these are issues for the supervision of sex offenders in general. For those individuals that are motivated to continue engaging in criminal behavior undetected, the above methods could be implemented to circumvent any form of computer monitoring. This should not detract from efforts to find balanced and positive methods for supervising offenders' computer-related activities, especially given that base rates of recidivism are low and that many offenders are attempting to lead law-abiding lives. OMS represents another tool for effective offender supervision: it is not a panacea for all supervisory issues and will not be appropriate for all clients.

Legal/ethical considerations

In addition to the legal context outlined in the legal context section above, a further legal/ethical issue became apparent in the implementation of Securus OMS at the PBPP. Specific acceptable use policies should be developed by the PBPP for the purpose of computer monitoring and these policies should be made available to monitored clients. As outlined in the *Doe vs. Jindal* case described in the introduction to this report, the client has a constitutional right to expect conditions of supervision and legislation related to supervision to be transparent and understandable to the average person. Therefore, it is likely that in this context they have a right to have an understanding of how 'acceptable use' is being judged by the PBPP. Thus, a written acceptable use policy should be developed and this document should be available to management, agents, and clients alike. This would allow the PBPP to ensure that monitoring policies are not unconstitutionally vague and that

clients have well-defined boundaries in which to act. This document would not need to infringe on commercially-sensitive information (i.e., would not need to include Securus' lists of words) – they would simply need to outline what libraries are switched on and why the content of these libraries constitute unacceptable use for sex offender clients It should also include information on other aspects of monitoring, such as the fact that the software allows agents to access browser histories, and that they can detect attempts to circumvent the system or use evidence eliminating software.

Issues for future evaluation

The following sections outline some implementation issues that were noted that could have the potential to hinder successful evaluation of the OMS approach in the future. Well-implemented programs structure future evaluation into the development of policies and procedures from the outset, in order to incorporate data collection and performance assessment into basic program operations, and it would be beneficial if these issues were addressed *a priori* as part of further development of OMS implementation.

It should be noted that recidivism is *not* the only relevant measurable outcome for an OMS approach. In fact, given the focus on better *detection* of recidivism and/or inappropriate computer use it might be argued that a greater number of reconvictions or parole violations could be an indicator of program success for OMS. However, the overall aim of OMS appears to be a combination of deterrence, accountability, and support, and thus the following sections focus on the potential for the use of experimental methodology to evaluate the success of OMS based on the reductions in recidivism and anticipated changes in behavior and necessary resources.

Corroboration of captures

In evaluating the effectiveness of Securus in terms of outcomes and its ability to alert agents to violations of unacceptable use it would be beneficial if any future evaluation were to be able to compare the data collected and reported by OMS with the data scanned directly from offenders' machines during home visits. As PBPP management pointed out, this may be a useful independent method by which to assess performance in terms of whether or not OMS is capturing all of the relevant computer use that would concern the PBPP.

Capacity

Limited sample sizes are an issue for successful evaluation. The size of the expected effect of a program is the key determinant of the sample size needed to conduct a successful RCT and the smaller the expected effect of the program the larger the sample size required for evaluators to be able to conclude, with enough power, that observed differences are unlikely to be due to chance (Rice & Harris, 2003; Stolberg, Normal, & Trop, 2004). It is recognized that this was a small-scale demonstration project and that low participation was to be expected – however, the stated difficulties in identifying and recruiting eligible clients (e.g., lack of motivation, lack of resources to acquire technology, etc.) would be of concern to evaluators seeking to evaluate effectiveness of OMS monitoring. It is worth reiterating that there are genuine reasons why some sex offender clients may choose to decline to take part –they simply may not have the resources to participate, or may have their own concerns about their behavior should they have access to the internet – and so participation rates may be naturally low. If any form of experimental or quasi-experimental methodology is desired there would need to be a substantial increase in capacity.

There is also likely to be an effect of the low baseline rates of recidivism in sex offenders (noted in the introduction) in the ability to provide evaluators with enough statistical power to detect genuine effects of OMS. Thus, given the low capacity, combined with the low rates of recidivism anticipated for both OMS clients and controls, any expected observable effect of OMS monitoring will be small. The degree to which capacity might impact successful evaluation, however, is dependent on what exactly the PBPP (or any agency who evaluates an OMS approach) expects OMS to detect. If OMS is specifically designed to detect *sexual* recidivism - and it should be noted that restrictions on access to computers and communications technology are presumably the result of a particular criminal justice concerns specifically about the behavior of *sex offenders* online - then the low sexual recidivism rate of approximately 12% for sex offenders (Hanson & Morton-Bourgon,

2009) may necessitate a substantial increase in capacity in order to detect effects. If OMS is designed to detect *any* recidivism by sex offenders, then the higher general recidivism rate of 33% for sex offenders (Hanson & Morton-Bourgon, 2009) would mitigate the issue of low sample size somewhat. Similarly, it could the detection of genuine effects would be affected if any samples contained a skewed proportion of individuals assessed as being at the lowest risk of recidivism[10].

As St. Pierre (2004) noted, although studies based on large sample sizes yield the greater statistical power, it may be possible for studies with smaller sample sizes to increase the precision of impact in other ways, such as by controlling more carefully any differences in variables that are related to the outcome (e.g., prior treatment provision and success, intensity of supervision, risk scores, social capital, and psychological characteristics). However, as noted above, there are currently some implementation issues that would need to be resolved (e.g., the issue of monitoring frequency/duration, risk assessment, etc.) before these variables can be successfully controlled. Nonetheless, the implementation of OMS as observed during this feasibility evaluation suggests that it is conceivable that with careful control of key variables and clarification on whether sexual recidivism is the key focus, the detrimental effects related to a low sample size issue could be mitigated.

Alternative measures

As noted at the beginning of this section, reductions in recidivism and reconvictions are not the only variables that should be considered. The OMS logic model outlines a theory of change that assumes changes in behavior for both clients and agents as a result of OMS monitoring.

[10] It is worth noting here that in the demonstration project the criteria for participation was simply that the client be a registered sex offender with the aspiration and means to obtain a computer and access to the internet, regardless of risk level.

For the clients, the logic model outlines a number of variables on which change is anticipated. First, clients are expected to obtain greater access to public and community services - therefore, some measures of whether OMS leads to positive outcomes in terms of access to housing, treatment, education, training, and employment, and a general reduction in reliance on public and community services over time would be recommended. Second, clients are expected to develop and understanding of their own 'risky' behavior and develop pro-social behaviors - therefore, measures related to relapse prevention perhaps, or problematic internet use, would be recommended. Lastly, clients are expected to improve in areas of socio-affective functioning, such as self-efficacy and self-esteem, as a result of the increasingly shared personal accountability and responsibility afforded to clients - therefore, some measures of these socio-affective variables would also be recommended.

For the agents, one of the key assumptions of the OMS approach is that the ability to remotely monitor computer use should allow PBPP agents to manage their workload and work more efficiently. In the current implementation it was difficult to see how the success of this aim could be evaluated. In the implementation phase, it was suggested (as occurred in one of the U.K. pilots) that agents maintain a simple log of their monitoring activities. However, this did not form part of implementation at PBPP. These logs would not need to be detailed or resource-intensive, simply a log of time spent viewing captures and a decision-log for any further action taken - i.e., if a capture was considered a *minor* violation of acceptable use (an example of *risky* behavior that perhaps led to a home visit or a conversation with their supervising agent) or a major violation of acceptable use (and led to further legal sanctions). These logs would allow future evaluators to measure: (a) the time spent by agents monitoring offenders; and (b) the time spent engaging in activities generated by captures. This in turn would allow evaluators to establish the proportion of captures that were considered to be, in this context, true-positives or false-positives.

Recommendations

It was established that many of the elements of implementation were successful, but that some alterations should be made to improve implementation in the future. The following section outlines a series of recommendations based on the findings above. When reading these recommendations it should be acknowledged that this was a demonstration project that was internally funded with the respective resources being provided either free of charge or at the cost of both the PBPP (agent time, etc.) and Securus (equipment, technology, hosting, etc.), and that some of the identified issues were a result of the reduced-cost nature of these types of exploratory implementation projects.

1. Refine training methods and enforce attendance

Training practices should be refined. If it is to develop an ongoing program of providing OMS monitoring in the U.S., Securus should consider having trainers that are located in the U.S. and making training available in-person for U.S. organizations. This would allow organizations to schedule longer sessions on multiple occasions and with trainers on-hand to guide staff through the process of using the functions and features of the management console, and ensure that those with a more kinesthetic learning style are catered for. It is worth noting that the stakeholders did consider this issue in advance and this was an anticipated potential outcome for implementation. Furthermore, it may be beneficial to provide training in two tiers: (1) an initial 'core' training program that outlines the very basic functions of OMS; followed by (2) an 'advanced' training program that builds upon core training and explains the more sophisticated elements of OMS.

2. Refine the libraries for the PBPP context

Refinement of the libraries is needed to make them specific to the needs of the PBPP. In the context of Securus OMS, agents described a desire to have a system that is highly-customizable for both sex offenders in Pennsylvania in general and for individual clients that allow agents to know if their

clients are "stepping off the reservation" in terms of violating defined boundaries of computer use. This may require collaboration between all stakeholders to find a balance that ensures that proprietary content is protected but ensures sensitivity and specificity in operational use of OMS.

In the U.K. police officers were keen on the 'soft intelligence' that Securus OMS provided and the risk context it allowed them to build (see Elliott et al., 2010). In contrast, the feedback received in this evaluation is that PBPP agents want to be provided with (and alerted to) highly-specific information related to new offending and possible breaches of license conditions, with the added benefits of being able to view internet browsing histories. One agent described an apt analogy to the Board's use of GPS monitoring. It described how the agent had a knowledge of the client's prior victims, their families, and their client's behavior such that by using GPS technology they were able to develop 'zones of exclusion' that are specifically tailored to that client, based on the specific locations of victims and family members relevant to past (and potentially future) offending, and that the agent was then immediately alerted to any breach of those zones and is able to react.

3. Establish policies relating to the frequency and regularity of monitoring

Aims and objectives related to the frequency and regularity of monitoring should be formally established. The PBPP needs to establish whether they wish to incorporate OMS into its supervisory practices as a requirement of participating agents and set either rigid or flexible rules on frequency and duration of monitoring, or if they wish to simply provide the service to participating agents, who may utilize the service as they best see fit, and provide only guidelines on recommended practice. This is not to say that one approach is better than the other (we have no outcome data on which to make claims about effectiveness and effective practice) – however, clarification will be required for future implementation. In addition, it may also be beneficial for

management to receive specific training on the online management system to learn how to generate performance reports that indicate how often agents are monitoring captures.

4. Develop processes for presenting OMS evidence

The PBPP should produce *pro forma* documents that can be used to present evidence collected via OMS. In this demonstration project, agents were instructed to use knowledge gleaned from OMS to instigate further investigative action (following established practice). It would be recommended that the PBPP liaise with agencies using OMS in the U.K. to learn from how they present and utilize the specific information OMS provides in order to justify further investigative activity.

5. Seek ways in which to increase capacity

In order to present Securus OMS as evidence-based practice, an evaluation of effectiveness would need to be carried out. As outlined above, this will require an increase in participation in the problem to levels that would allow for meaningful outcome statistics to be derived. Both the PBPP and Securus have an interest in establishing an evidence-base for OMS implementation in the U.S. and should work together to develop methods by which to both make Securus available to a greater number of clients and to promote the benefits of Securus to those clients in order to improve levels of uptake.

6. Collect workload data

It would be recommended that the PBPP develop some form of workload log that would allow agents to log time spent using the system – or if this is already an option within Securus OMS, better promote these features during training. If such logs could be automated within the software, it would reduce the burden of hard-copy record-keeping from agents and allow agents, management, and evaluators to generate workload reports that could be used to assess, modify, and improve

ongoing implementation. Alternatively, some agents noted that the PBPP has IT systems for maintaining case notes and perhaps these systems could be adapted to maintain workload data. It would also be recommended that this system be promoted as a means by which to record data on what responses (and what level of response) were made to violations captured by Securus OMS.

7. Establish a future funding strategy

This demonstration project was established as a no-cost opportunity in which the PBPP would be able to test implementation feasibility and Securus would be able to establish their credentials with a large U.S. State-level criminal justice organization. If the approach were to be implemented in the future the PBPP would need to develop a strategy for funding implementation (i.e., purchasing server or cloud computing space, purchasing software licenses, etc.) This may involve sourcing centralized funding, but it may also be worth the PBPP engaging in some reconnaissance with organizations using OMS in the U.K. who have had success in implementing a funding model based on client subscriptions where clients contribute to costs – although, this may further limit uptake of participation and place further financial burden on a population for whom it has been established above often struggle to find the resources to get online.

Conclusions

This feasibility evaluation found that the Securus OMS approach was sound and implementable in theory. The PBPP was able to create an effective partnership with Securus and successfully draw together various relevant departments to set up a team with the abilities and scope to implement this approach. Despite the communication issues related to having stakeholders in various locations (Harrisburg and Pittsburgh in the U.S. and Leatherhead in the U.K.), on the whole management and agents at the PBPP welcomed the approach, embraced the technology, and had positive experiences of participation. However, the practical implementation of OMS in some areas was inconsistent and there were some legitimate concerns about ensuring that agents received the highest proportion of relevant and actionable data possible from the software.

This highlights the benefit of utilizing feasibility evaluations in the early stages of implementation – problems in implementing new and novel practices are to be expected and it is beneficial to identify limitations to implementation early in development where modifications are likely to have the greatest effect in the long-term. It is of note that the majority of the issues that were uncovered in implementation were not related to the intended theory but to issues the practical application of that theory. Thus, all have the potential to be resolved through realistic changes to implementation and better communication between the various stakeholders and refinement of the management structure.

If it is found to be possible to increase capacity in terms of participation and scope, it is highly recommended that the stakeholders consider engaging in further evaluative effort. Given the current legislative landscape it seems that there would be few practical or ethical obstacles to developing an experimental evaluation of the effectiveness of the OMS approach (including randomized allocation to OMS or supervision-as-usual groups). It would be to the benefit of all

stakeholders involved to determine if this is simply an additional aid to supervision or if it has an independent tangible effect on in reducing reoffending, and to what extent this effect is a result of changes in client behavior and/or an increased ability to detect new offenses.

This feasibility evaluation concludes that with some targeted modifications in the practical implementation of OMS, the PBPP can achieve the goal of incorporating the approach into supervisory practice. OMS has the potential to provide PBPP agents with an extra tool with which to ensure public safety – one that also has potential important pro-social benefits for the client - and thus OMS can make a valuable contribution to established methods for the supervision of sex offenders in Pennsylvania.

References

Andersen, S. L., Tomada, A., Vincow, E. S., Valente, E., Polcari, A., & Teicher, M. H. (2008). Preliminary evidence for sensitive periods in the effect of childhood sexual abuse on regional brain development. *The Journal of Neuropsychiatry and Clinical Neurosciences*, *20*, 292–301.

Chen, L. P., Murad, M. H., Paras, M. L., Colbenson, K. M., Sattler, A. L., Goranson, E. N., et al. (2010). Sexual Abuse and Lifetime Diagnosis of Psychiatric Disorders: Systematic Review and Meta-analysis. *Mayo Clinic Proceedings*, *85*, 618–629.

Craven, S., Brown, S., & Gilchrist, E. (2007). Current responses to sexual grooming: Implications for prevention. *The Howard Journal*, *46*, 60–71.

Elliott, I. A., Findlater, D., & Hughes, T. (2010). Practice report: A review of e-Safety remote monitoring for U.K. sex offenders. *Journal of Sexual Aggression*, *16*, 237-248.

Fuchs, C., Boersma, K., Albrechtslund, A., & Sandoval, M. (2012). Introduction: Internet and surveillance. In C. Fuchs, K. Boersma, A. Albrechtslund, & M. Sandoval (Eds.), *Internet and surveillance: The challenges of Web 2.0 and social media* (p. 1-30). New York, NY: Routledge.

Hanson, R. K., & Morton-Bourgon, K. E. (2009). The accuracy of recidivism risk assessments for sexual offenders: A meta-analysis of 118 prediction studies. *Psychological Assessment*, *21*, 1-21.

John Doe vs. Bobby Jindal et al., 11-554-BAJ-SCR, U.S. Ct. Middle District of Louisiana (2012). Retrieved August 30, 2014 from http://www.plainsite.org/dockets/l6t4m4we/louisiana-middle-district-court/doe-v-jindal-et-al/

Levenson, J. S., Hern, A. L. (2007). Sex offender residence restrictions: Unintended consequences and community reentry. *Justice Research and Policy*, *9*, 59-74.

Mell, P., & Grance, T. (2011). The NIST definition of cloud computing: Recommendations of the National Institute of Standards and Technology (Special Publication 800-145). Washington, DC: National Institute of Standards and Technology, U.S. Department of Commerce.

Mercado, C. C., Alvarez, S., & Levenson, J. S. (2008). The impact of specialized sex offender legislation on community reentry. *Sexual Abuse: A Journal of Research and Treatment*, *20*, 188-205.

Nieto, M., & Jung, D. (2006). *The impact of residency restrictions on sex offenders and correctional management practices: A literature review.* Sacramento, CA: California Research Bureau.

Rice, M. E., & Harris, G. T. (2003). The Size and Sign of Treatment Effects in Sex Offender Therapy. *Annals New York Academy of Sciences*, *989*, 428-440.

Savaya, R., & Waysman, M. (2005). The logic model: A tool for incorporating theory in development and evaluation of programs. *Administration in Social Work*, *29*, 85-103.

St. Pierre, R. G. (2004). Using randomized experiments. In J. S. Wholey, H. P. Hatry and K. E. Newcomer (Eds.). *Handbook of Practical Program Evaluation* (2nd Ed.) (pp. 150-175). San Francisco: Jossey-Bass.

Stolberg, H. O., Norman, G., & Trop, I. (2004). Randomized controlled trials. *American Journal of Roetgenology*, *183*, 1539-1544.

Vess, J. (2008). Sex offender risk assessment: Consideration of human rights in community protection legislation. *Legal and Criminological Psychology*, 13, 245-256.

Ward, T., Gannon, T., Vess, J. (2009). Human Rights, Ethical Principles, and Standards in Forensic Psychology. *International Journal of Offender Therapy and Comparative Criminology*, *53*, 126-144.

Ward, T., & Stewart, C. A. (2003). The treatment of sex offenders: Risk management and good lives. *Professional Psychology: Research and Practice*, *34*, 353-360.

W.K. Kellogg Foundation (2006). *Logic Model Development Guide*. Battle Creek, MI: W.K. Kellogg Foundation.

Appendices

Appendix 1. Semi-structured interview protocol for management.

Appendix 2. Semi-structured interview protocol for agents.

Appendix 3. Feedback form for client participants.

Appendix 4. Logic model (larger size).

Appendix 1: Semi-structured interview protocol for management

Opening

- This interview is confidential / recorded.
    - Therefore need a verbal yes/no to give your consent to be recorded.
- The recording will be transcribed and anonymized, and no information that you provide today will be personally identifiable in any documentation.
- Should take no more than one hour at the most.

1. **Involvement**
    a. What was your role in the Securus pilot?

2. **Logic model**
    a. What overall need for Parole and Probation was Securus designed to address?
    b. Who were the key stakeholders in the project?
        i. Did you feel that there was adequate communication between the stakeholders?
        ii. If not, how could communication be improved?
    c. What were the specific aims of the pilot project?
        i. What did you hope to achieve?
        ii. What were the anticipated outcomes?
    d. What were the anticipated **short-term** benefits:
        i. For the agents?
        ii. For the clients?
    e. What were the anticipated **long-term** benefits:
        i. For the agents?
        ii. For the clients?

3. **Process/implementation**
    a. Libraries
        i. Which libraries were chosen to remain active for the pilot?
            1. On what basis were these libraries chosen?
        ii. Were any libraries customized?
            1. Were any 'severity' levels used?
            2. Was <u>any</u> customization requested?
    b. Training
        i. How were agents trained to install/use the software?
        ii. Did you feel this training was adequate?
    c. Agent selection
        i. On what criteria did management select agents to take part?
        ii. Were these criteria adhered to?
    d. Client selection
        i. On what basis did management expect clients to be selected?
        ii. What were the inclusion/exclusion criteria?
        iii. Were these criteria adhered to?
    e. How was the pilot funded?
        i. Did clients contribute to funding the software?
        ii. Did this funding model work/meet your expectations?
    f. Monitoring

i. What were the expectations for agents in terms of actively monitoring clients' activities?
    1. How often?
    2. How long?
ii. How were these expectations communicated to staff?
iii. Were your expectations met?

g. Violations
    i. What was the anticipated chain of command if/when violations of AUP occurred?
        1. Hypothetical?

4. Feedback (if any?)

a. User-friendliness (if used)
    i. How easy was it to use the software?
    ii. Any technological/process problems?
b. Data/information
    i. What information data did the software provide you with?
        1. Are their plans (beyond monitoring/this feasibility study) to use the available data?
    ii. How much data did it give you?
        1. Was that data useful?
    iii. Are there any specific legal implications of collecting these data from clients?
        1. Is there a trade-off between public safety and clients' privacy?
c. Do you think the software added value to the work of the Board of Parole and Probation?

5. Moving forward

a. What would you consider to be the measures of success for this project?
b. Do you anticipate a further need for this software?
c. What improvements would you like to see to the software?
    i. With hindsight, are there any ways in which you would change implementation in the future?
    ii. Are there any specific customizations that you would like to request from Securus?
d. Could you see the software being made mandatory for some clients?
e. Would you continue with the current funding model?
f. What is the potential **demand** for this approach?
    i. Are there clients not yet reached who might benefit from this software?
    ii. Any suggestions for how we could improve the numbers of clients participating (in order to better evaluate the outcomes)?
g. Would you consider this a project that would require further evaluation?

Appendix 2: Semi-structured interview protocol for agents

Opening

- This interview is confidential / recorded.
    - Therefore need a verbal yes/no to give your consent to be recorded.
- The recording will be transcribed and anonymized, and no information that you provide today will be personally identifiable in any documentation.
- Should take no more than one hour at the most.

1. **Process/implementation**
    a. What was your role in the Securus pilot?
    b. Training
        i. Did you receive training to install/use the software?
        ii. Did you feel this training was adequate?
    c. Client selection
        i. How were clients selected?
        ii. What were the inclusion/exclusion criteria?
    d. Installation
        i. Take me through the installation process?
            1. Any problems?
    e. Monitoring
        i. Take me through the process you used to monitor clients activities?
            1. Any systems you put in place?
        ii. How often did you use the software to monitor clients?
        iii. On average, how long did you spend monitoring when you did?
    f. Outcomes
        i. Did you have any clients violate your AUP?
            1. How did you follow-up on this? (Get info for case example)
            2. Who and how?
                a. Hypothetical?
        ii. Did you have any clients demonstrate risky behavior that fell short of violating your AUP?
            1. How did you follow up on this? (Get info for case example)
            2. Who and how?
                a. Hypothetical?
        iii. Did you see any evidence of your clients trying to circumvent the system? (i.e., evidence-eliminating software, use of other machines, uninstalling, etc)
            1. If so, what did you do?

2. **Program aims**
    a. Overall, in your own words, what was the goal of Securus?
        i. What *problem* does Securus solve?
        ii. What were the intended benefits to you?
        iii. What were the intended benefits to your clients?

3. **Feedback**
    a. User-friendliness
        i. How easy was it to use the software?
        ii. Any technological/process problems?

b. Data/information
    i. What information data did the software provide you with?
    ii. How much data did it give you?
        1. Was that data useful?
c. Relationships with clients
    i. What, if any, affect did the software have on the working relationship between you and your clients on Securus?
        1. In your opinion, were the clients satisfied with the software?
        2. Did you receive any complaints?
d. Do you think the software added value to the work you do?

4. Moving forward

a. Is there a further need for this software?
b. Are there clients not yet reached who might benefit from this software?
    i. Any suggestions for how we could improve the numbers of clients participating (in order to better evaluate the outcomes)?
c. What improvements would you like to see to the software/process?
d. Could you see the software being made mandatory for some clients?

Appendix 3: Feedback form for client participants

University of Massachusetts Lowell
UMASS

E-SAFETY PILOT PROJECT EVALUATION

FEEDBACK QUESTIONNAIRE

Instructions

Please read the following questions carefully and indicate your response by circling the number that best matches how you feel.
Space has been provided for you to provide brief explanations of each of your responses.

Q1: How satisfied were you with the way in which the software, the project goals, and the procedures involved in the pilot project were explained to you?

Very satisfied	Fairly satisfied	Neither satisfied nor unsatisfied	Fairly unsatisfied	Very unsatisfied
5	4	3	2	1

Please explain your answer: _____

Q2: How satisfied were you with the level of communication you received with the pilot project staff?

Very satisfied	Fairly satisfied	Neither satisfied nor unsatisfied	Fairly unsatisfied	Very unsatisfied
5	4	3	2	1

Please explain your answer: _____

Q3: How satisfied were you with the boundaries set by Parole and Probation in terms of what they considered to be <u>appropriate</u> and <u>inappropriate</u> internet use?

Very satisfied	Fairly satisfied	Neither satisfied nor unsatisfied	Fairly unsatisfied	Very unsatisfied
5	4	3	2	1

Please explain your answer: _____

Q 4: How satisfied were you with the way the software operated and your ability to use it?

Very satisfied	Fairly satisfied	Neither satisfied nor unsatisfied	Fairly unsatisfied	Very unsatisfied
5	4	3	2	1

Please explain your answer: _____

Q 5: How obtrusive (noticeable) did you feel the technology was during the pilot study?

Very obtrusive	Fairly obtrusive	Neither obtrusive nor unobtrusive	Fairly unobtrusive	Very unobtrusive
5	4	3	2	1

Please explain your answer: _____

6: Did you feel that participation in the pilot had a positive or negative effect on your feelings of privacy?

Very positive	Fairly positive	No effect	Fairly negative	Very negative
5	4	3	2	1

Please explain your answer: _____

Q 7: How satisfied were you that the data related to your computer use was being managed in a secure way?

Very satisfied	Fairly satisfied	Neither satisfied nor unsatisfied	Fairly unsatisfied	Very unsatisfied
5	4	3	2	1

Please explain your answer: _____

Q 8: How important was it to you that participation in the pilot project was voluntary?

Very important	Somewhat important	Not important
4	3	1

Please explain your answer: _____

Q 9: Did you in any way feel obliged (required) to take part in the pilot study?

Very obligated	Somewhat obligated	Not obligated
3	2	1

Please explain your answer: _____

Q 10: Did you feel that the process being tested in this pilot project had a positive or negative effect on your relationship with your Parole/Probation Agent?

Very positive	Fairly positive	No effect	Fairly negative	Very negative
5	4	3	2	1

Please explain your answer: _____

Q 11: How necessary do you feel supervision of computer use is for individuals convicted of a sexual offense?

Very necessary	Fairly necessary	Neither necessary nor unnecessary	Fairly unnecessary	Very unnecessary
5	4	3	2	1

Please explain your answer: _____

Q 12: Did you feel that participating in this pilot had a positive or negative effect on your ability to change/affect your own level of risk (as perceived by Parole/Probation)?

Very positive	Fairly positive	No effect	Fairly negative	Very negative
5	4	3	2	1

Please explain your answer: _____

Q 13: Did you feel that participation in this pilot project had a positive or negative effect your computer use?

Very positive	Fairly positive	No effect	Fairly negative	Very negative
5	4	3	2	1

Please explain your answer: _____

Q 14: How much would you agree/disagree with the following statement? "I believe that the software acted as a guard/deterrent against inappropriate computer use."

Strongly agree	Agree	Disagree	Strongly disagree
4	3	2	1

Please explain your answer: _____

Q 15: How much would you agree/disagree with the following statement? "I would be interested in continuing to have my computer use monitored."

Strongly agree	Agree	Disagree	Strongly disagree

4 3 2 1

Please explain your answer: _____

Q 16: How much would you agree/disagree with the following statement? "I have benefitted from participating in this pilot project."

Strongly agree	Agree	Disagree	Strongly disagree
4	3	2	1

Please explain your answer: _____

Q17: Did you feel that <u>remote</u> monitoring specifically had a positive or negative effect on your experience of supervision?

Very positive	Fairly positive	No effect	Fairly negative	Very negative
5	4	3	2	1

Please explain your answer: _____

Q 18: Overall, how would you rate your experience as a participant in this pilot project?

Very good	Good	Average	Bad	Very bad
5	4	3	2	1

Please explain your answer: _____

_____

_____

_____

_____

Thank you for your feedback!

The evaluation team would like to extend the opportunity for you to discuss your experiences further with the team. This will involve a short telephone interview lasting approximately 30 minutes.

If you would like to participate in a telephone interview, please provide a name (full name not necessary) and telephone number below on which the Principal Investigator can contact you to arrange a convenient time to discuss your experiences as a participant in this project.

You are not obliged to participate in a telephone interview. If you choose to participate, you are free to withdraw at any time (even during the interview) and you may request to have any data collected from you destroyed, by contacting the Principal Investigator on the contact details below. Withdrawal or non-participation will have no effect on your current or future relationships or access to services provided by the Pennsylvania Board of Probation and Parole, the University of Massachusetts Lowell, or Pennsylvania State University.

Name: _____

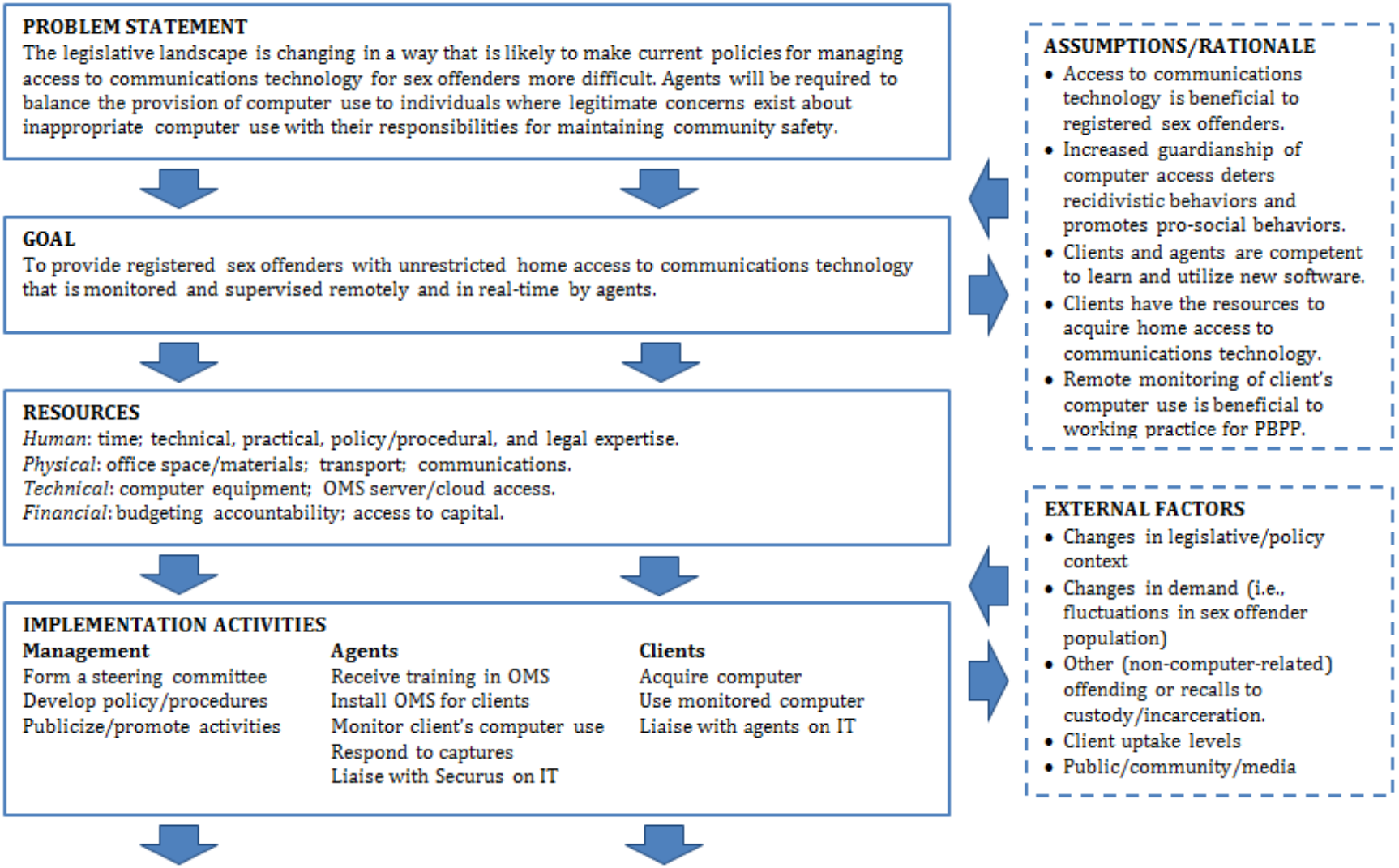
Telephone: _____ (please include area code)

By signing below, I agree to receive a telephone call from the Principal Investigator inviting me to take part in a telephone interview.

Signed: _____

Principal Investigator: Dr. Ian A. Elliott, University of Massachussetts Lowell, Room 443, 113 Wilder St., Lowell, MA 01854. Tel: (978) 934-4109.

Appendix 4: Logic model (larger size)



OUTCOMES		SHORT TERM →	MEDIUM TERM →	LONG TERM
AGENTS	KNOWLEDGE	Increased awareness/exposure to risks related to computer use.	Greater nuance in understanding of risks related to computer use.	Comprehensive understanding of risks related to computer use.
	PRACTICE	Ability to *identify* risk. Reactively respond to new offending.	Ability to identify *changes* in risk over time. Reactively respond to risky behavior.	Ability to identify *antecedents* to risk. Proactively respond to risk antecedents/changes over time.
	WORKLOAD	Remote monitoring of clients and access to data.	Ability to manage tasks (e.g., home visits) where appropriate.	Increased efficiency in use of workload and resources.
	ATTITUDES	Shared accountability/ responsibility for risk related to computer use.	Improved communication of risk decisions to/from clients.	More inclusive professional relationships with clients.
	SKILLS	Improved engagement with technology.	Customization of technology and generation of reports.	Comprehensive incorporation of technology into everyday practice.
CLIENTS	ACCESS	Access to immediately beneficial services (housing, communication, treatment).	Access to medium-term beneficial services (education, training, employment).	Increased economic/pro-social activity; reduced dependence on government services.
	KNOWLEDGE	Awareness of own risk perception.	Understanding own risk and identifies recidivistic behaviors.	Reduction in recidivistic behaviors (and reoffending).
	BEHAVIOR	Increased guardianship; reduction in anonymity in computer use.	Development and demonstration of pro-social computer use.	Increased pro-social computer use.
	ASPIRATIONS	Shared accountability/responsibility for risk related to computer use.	Increased perception of self-efficacy and agency in risk related to computer use.	Increased self-esteem and responsibility for computer use.