The Harvard psychology students credited with inventing the first electronic monitoring device were testing out a concept to reward juvenile offenders for attending court approved activities such as school, job, etc. In the 1960s, the devices were created using army surplus supplies: “missile tracking equipment, portable transceivers, battery packs, and radio frequency relay stations.” The wearable devices were designed to “activate a relay station” when the offender entered an approved location/area. The radio frequency location monitoring technology was introduced into the court system twenty years later in the 1980s only after a U.S. judge saw a watch used by a villain to track the location of the hero in a Spider-Man comic. And, instead of using the technology according to its original purpose (to positively reinforce good behavior), the court employed it for an entirely different/opposing criminal control concept: house arrest. Prior to the adoption of this technology, sentencing prisoners to remain at home for part of or the entire day entailed the employment of a trained person to constantly guard the offender at his or her home, and, in effect, was mostly reserved for the wealthy and/or high-profile prisoners. Receivers were installed in the non-violent offender’s home and wearable devices were made with material that could not be easily taken off. Thirty years later, this first generation technology still remains the most common type of electronic monitoring technology.

ELECTRONIC MONITORING: IN NEED OF A COMPLETE CONCEPTUAL OVERHAUL

Although satellite tracking or second-generation electronic monitoring technology is steadily growing in popularity, the underlying goal remains the same: act as a substitute guard and deter criminal activity/enforcing boundaries through constant surveillance of an offender’s location. And, despite its long tenure and expanding popularity (electronic offender monitoring is projected to be a $6 billion industry by 2018), “the viability of EM surveillance” to serve as an effective house arrest tool to deter criminal behavior and reduce recidivism still remains unsubstantiated. Unlike having an armed guard(s) following the offender around his or her house, location tracking has no way of providing parole officers knowledge of what types of activities are going on in the home. Recently, while under house arrest via a satellite ankle monitor, a US man was able to lure an underage woman to his home via Facebook and then rape, impregnate, and hold her hostage over a period of several weeks. His crimes went undetected throughout the duration of his house arrest sentence.

Furthermore, since the technology was not designed to restrain offenders to a particular area, prisoners are easily able to escape without the deterrent of immediate punishment. For instance, radio frequency devices can be removed with hardware tools such as a bolt cutters and satellite devices can be left un-charged. (Researchers have even found that it’s possible for offenders to hack devices and to spoof/send parole officers fake GPS locations messages using a home-
The number of breaches can be quite high. For instance, in New Zealand, the number of electronic monitoring breaches increased from 22.1% in 2012-2013 to 23.2% in 2014-2015. In the US, recent security breaches have left up to 16,000 offenders un-monitored for hours at a time. And, in many cases, either police officers did not arrive in time to recapture the escapee or failed to respond due to the high volume of such incidents. One estimate given by a California parole officer stated that it takes an average of 12 days to recapture the offender. And, the news is filled with incidents where these offenders have gone on to commit brutal crimes such as rape or murder.

Many offenders might even prefer a prison sentence or an armed guard enforcing their house arrest. This technology has given false alerts that offenders violated parole or the battery has failed to charge their batteries leading to extended or felony sentences. And, in some US districts, offenders are now being held financially responsible for the cost of their electronic monitoring sentences. Daily fees range from $5.00 to $25.00 not including installation fees, and can cost over $10,000 for a single offenders house arrest sentence. When the offender cannot pay, he or she may be sent to prison and then burden is shifted back to the tax payer/government. Although the average cost of electronic monitoring in the US ($6,000/year/person) is much less than the cost of a prison sentence ($26,000/year/person), it is still a substantial financial burden to either the tax paying public or the offender.

Despite the issues outlined above, the continued use of location tracking based electronic monitoring to enforce house arrest in the US might be largely attributed to governmental lobbying by third party electronic monitoring contractors. The largest US electronic monitoring company, BI, was awarded a $372 million 5-year contract in 2009 by the government and is owned by a private prison company that has spent millions of dollars in lobbying and campaign donation over the past decade.

An improved electronic monitoring surveillance system is not light years or even financially out of reach. In fact, many parents and dog owners use more sophisticated technology to monitor their charges from a distance than parole officers using the latest electronic monitoring technology. (It is easy to see why you would not leave a child unsupervised at home and rely only GPS coordinates to decipher whether he or she is in harm’s way or misbehaving.) Options for monitoring children are endless and many of the software applications are cheap or even free. The options for parents to monitor their children via video and audio surveillance are numerous. For instance, presence is a free app in the iTunes store that can be used to transform old cell phones or tablets into a real time home motion detector. Along with live a view of the room, users receive video alerts when motion is detected. The app is also compatible with wireless sensors to monitor such things as the temperature, humidity, whether a door is open/shut, etc. within the home. TheOneSpy product claims not only to allow parents to track the GPS location of a child via their cell phone, it also allows parents to operate camera and microphones at a distant, gain access to text messages, and tap phone calls. A yearlong subscription costs less than $150. And, parents can monitor and sensor all network traffic by purchasing a special parental control router such as Skydog ($149). Even with such readily available surveillance technologies, parents still must assume the responsibility of sifting through the data and knowing when and how to respond. Does the ability to remotely monitor what your toddler is doing in the mean that you can leave her or him at home alone? Likewise, is even the most advanced surveillance technology an adequate way to enforce house arrest if there are not enough employees to remotely monitor recorded activities or if police cannot respond immediately to security breaches?

**ELECTRONIC MONITORING: A RE-CONCEPTUALIZATION BASED ON CURRENT TECHNOLOGY**

According to the “Swift and Certain” paradigm, both constant surveillance and “swift and certain” punishment is needed “to deter crime” and reduce “incarceration and recidivism”. To design an electronic monitoring system based on these principles, the potential types of technology, their cost, and their levels of human involvement will be examined in the following sections.
Complete surveillance would entail not only knowing the location of an offender, but also both what he or she is doing and what he or she is planning to do. With greater insight into the offender’s activities, the parole officer will have more information to assess an offender’s rehabilitation progress and potential for recidivism. Furthermore, such information is crucial to forestalling criminal behavior. To our knowledge, a brain decoding tool/real time mind reading tool does not exist (yet). However, it is an active area of research. Using fMRI technology, researchers are now developing techniques to decode brain waves. For instance, researchers have been able to reconstruct a video of what a person is looking at, albeit fuzzy, and also categorize a person’s dream. And, the judicially related applications of this technology are being explored such as determining if someone is lying, how reliable a particular memory is, and if a person has visited a particular location before. While such technology is being explored/ in the meantime, there are many video, audio, device, and internet surveillance tools that can be used to monitor what an offender is doing and what he or she is planning to do. It might not be possible to read on offender’s mind, but the ability to read his or her text messages or listen to his or her phone calls is possible. And, as discussed in a later section, the rate limiting/prohibiting factor might not be the cost or lack of robustness of such technology, but issues related to managing the mass amount of generated data.

Monitoring Offenders with a Virtual Eye

Had there been a surveillance system to monitor who was entering and exiting the apartment of the man that managed to abduct and impregnate a minor while under electronic monitoring house arrest, the crime might have been stopped much sooner or it might have deterred the offender from committing it altogether. Real time video surveillance technology is readily available from do-it yourself versions that can easily be assembled for under $200 to mid-range cameras such as the Full HD Day & Night Vandal-Proof Dome Network Camera that retails around $500 to high end technology such as the ELI-SN2-SP60, a solar powered, wireless 4G camera that cost around $5,000 plus $100+/month data plans. Many cameras also offer the option to record audio. In all three cases, real time monitoring is accomplished using IP cameras that require either local area network (LAN) or wide area network (WAN) access to transfer data to be stored or viewed.

Can Virtual Eyes Get Cataracts? Vulnerabilities in Standard Video Surveillance Systems

Although it is a prevalent surveillance technology, the reliance on the internet means that cameras are vulnerable to being hacked. For example, hackers found an exploit in the built in web server of a $900 D-Link IP security camera to retrieve the admin password and perform all types of malicious activities such as rebooting it and accessing data. In a $1000+ IQInvision (commonly used in schools, by police, and businesses) camera, hackers were able to perform a command injection and access the admin area and take command of it. The hackers were able to demonstrate that with root access it is possible to freeze the admins video page with a static image so any new activity would remain undetected, while the hacker could still view the live video feed. Since many security cameras use the same open source firmware, such vulnerabilities are wide spread. Additionally, since specific products are not usually listed in the bug releases, operators/admins should ensure firmware is up to date. (And, the product should never be used without changing default passwords.)

There are privacy concerns regarding monitoring activity within an offender’s home via video surveillance. Even if permission is granted to continuously monitor an offender in all rooms of his or her home, it might prove difficult to justify if he or she lives with non-offenders.

Video Surveillance Drones and Robotic Cameras

One possible alternative might be the use of a drone or robotic eye to perform random video surveillance check-ins at an offender’s home. Currently, parole officers will occasionally and unexpectedly show up at an offender’s home. (The man who abducted the minor was subject to such visits, although the officer was unable to detect any unusual activity. If such a visit could have been performed more frequently and with a greater element of surprise, perhaps the criminal activity could have been identified. Additionally, the use of a drone would keep the police officer out of harm’s way. The
ideal parole officer check in drone would be remote operated from the comfort of an officer’s desk or even pre-programmed and not require manual operation at all. Video surveillance drones can cost anywhere from less than $100 to over a $1000. However, many of the commercially available drones only have a small battery life/limited flight time of under 30 minutes or less. One of the most popular drones on Amazon, the DJI Phantom 3, has price tag of around $1,600, uses GPS for navigation, offers 20 minutes of flying time, can be charged in the car, features live video streaming, and has a 2,000 feet line-of-sight. In the US, some police departments are now using a throwable, mobile robotic camera to inspect situations that could be too dangerous for a human. The commercial technology is rather cost-prohibitive with the Recon Scout selling for $9,000 and still requires the user to be close to the site.

Wearable Devices: Seeing What the Offender Sees (Salvaging the Google Glass?)

Another alternative to the static placement of surveillance cameras around the offender’s home are wearable video cameras. Next generation wearable electronic monitoring devices could both track the GPS location of a prisoner and provide visual and/or audio insight into his or her activities. A parole officer could surreptitiously check in on his or her ward and have the ability to see what he or she is viewing. Who are they messaging on Facebook? What conversations are they having and with whom? In the US, wearable cameras are already being deployed by police departments to monitor police officer behavior while they are on patrol. The footage is used by courts to determine if a police has acted illegally/abused a criminal. Police body cameras can be attached either on clothing or glasses, and have been purchased by departments for as little as $50 each. Although the cameras themselves are inexpensive storage is costing some police departments in the millions (ex. $2.6 million for storage and the extra staff needed to manage the video data), while other departments are paying from $20 to $100 /month/polic officer for data management plans. It seems that many departments might be paying too much to the surveillance contractors. As a reference, Amazon offers its users unlimited cloud storage for only $60 a year.

Another option would be to employ analytics software to identify unusual activity. In the case of monitoring traffic going in and out of a house, a software program could be used or developed to identify when the offender left the home or when an unregistered or new person showed up at an offender’s door, and only then send an alert to the parole officer. It would be necessary to rigorously test such a system to determine if unusual activity could be detected accurately, consistently, and in a timely manner. One surveillance camera, simplicam, offers to provide facial recognition and identification of strangers and costs $199.99 for the camera and one year of recording services. Video surveillance analytic software is especially popular in the retail world. Stores are alerted when behavior associated with shoplifting is detected by the software. Footage is also used to analyze consumer behavior such as demographic analysis, foot traffic, and employee speed of service.

Police departments in the US such as the NYPD and LAPD use Palantir’s software to make connections between data...
sets. (In the US, the same software is also used by the CIA, DHS, NSA, FBI, the CDC, the Marine Corps, the Air Force, Special Operations Command, West Point, the Joint IED-defeat organization and Allies, the Recovery Accountability and Transparency Board and the National Center for Missing and Exploited Children.) “Users do not have to use SQL queries or employ engineers to write strings in order to search petabytes of data. Instead, natural language is used to query data and results are returned in real-time.”31 For the LAPD, it seems that the system cost over $400,000. According to Palantir’s website, the company offers a video analytics feature that allows “user to tag individuals and events within video data and associate those tags with information from other data sources.” 32

Hitachi Data Systems offers both a pre-built “end-to-end” video management solution designed to “to give law enforcement, emergency management and other security organizations greater situational awareness and the capacity to more effectively and efficiently extract insights from a broader range of data sources to ensure faster response times when a situation developed” and a predictive crime feature. Hitachi Visualization Predictive Crime Analytics (PCA) add-on module uses “real-time event data captured from public safety systems and sensors with historical and contextual crime data from record management systems, social media and other sources” to assign threat levels for individual neighborhoods. 33 Price is upon request.

An analytics system tailored for probation management could be built using commercial open source software such as Talend. With Talend, a real time data solution can be developed without the need for “complicated code” or “big data programming skills”. 34

For data analysis, software systems such as Planatir’s do not rely on single source of data such as real time video surveillance, but make use of various types of data such as criminal records, public records, etc. To effectively use or design such a system to monitor parolees in real-time, other sources of data aside from video or audio footage such as online activity, phone calls, SMS messages, etc could prove beneficial.

**Monitoring Offender’s Virtual Location**

When the first offenders were placed on electronic monitoring house arrest, the internet as we know it did not yet exist. In effect, the potential threat posed by a non-violent offender on house arrest was much less. And, with only the option of land line phone, it was much easier to monitor an offender’s communication with the outside world. Due to the development of these technologies/popularity of cybercrimes, both the offender’s physical and virtual/online location should be monitored. If the online activity of the man who used Facebook to rape/imprison/impregnate a minor while under house arrest had been monitored7, police might have been able to intervene and/or prevent the crime. Or, had the man known he was being monitored, he might have been deterred from committing the crime.Without implementing this type of surveillance or prohibiting the offender from online access, it’s easy to justify eliminating electric offender monitoring altogether as an outdated/inadequate criminal control/rehabilitation tool.

**Computer Monitoring Software, Network Monitoring, Commercial Spyware: a Trust Issue**

Many software programs exist that can be installed on an offender’s computer or phone to either monitor or restrict access. Securus Software’s OMS takes screenshots of an offender’s computer if he or she types certain keywords or phrases and then the image is uploaded to a server. 35 In the case of Securus, it is not compatible with Linux or Mac OS’s.36 It does not seem to be compatible with phone OS’s either. There are many flaws with such an approach. First, to be truly effective, the software must be installed on all devices an offender has access to. This would mean not only personal computer’s, but cell phones, tablets, etc. (Investigators recently discovered that PlayStation 4 gaming consoles were used to help plan the November 2015 Paris terrorist attack.37) To be manageable/cost effective, the software should be compatible with the offender’s operating system. Additionally, since the offender is not in solitary confinement, it would need to be installed on all of the devices he or she comes in contact with. And, even if you assume that the user will only use that one device, a computer can contain multiple permanent operating systems/or a different operating system can be booted using a liveUSB. The program would have to be installed on all of the computer’s OS’s and the assumption
would have to be made that he or she would not install a new OS or use a liveUSB. Even if an offender runs operating
system with the software, an offender could still avoid monitoring. For instance, a firewall could be used to block conne-
tions to or from the monitoring server.

Instead of using computer monitoring software, parole officers could conduct random checks either by accessing the
offender’s device remotely or during a home visit. There are a variety of low-cost and free digital forensics tools available
to gain inspect digital devices.38

Another approach is monitoring/sniffing all internet traffic on the offender’s home network. Again, the assumption
would be made that the offender is exclusively using that network. Commercial mobile spyware is subject to the same
limitations as the approaches described above, but has the possibility of monitoring both phone and internet activity.
Mobile spyware suffers from compatibility issues, and iPhones typically have to be jail broken. Additionally, a phone in-
ternet connection is required. The type of data that can be retrieved includes SMS activity, GPS coordinates (sometimes
the nearest cell phone towers as opposed to the actual location), pictures, videos, call logs, browser activity, email, and
SIM card changes. With some spyware packages, it is possible for the monitoring party to remotely control certain phone
functionality and take a picture, record video, record audio, view the screen, or wipe the phone.39 Commercial mobile
spyware such as SpyBubble, FlexiSpy, MobiStealth, Mobile-Spy, and SpyEra are not cost prohibitive and requires a sub-
scription. For instance, the premium package for FlexiSpy costs $149 for 12 months and the extreme package costs $349
for 12 months and offers features such as a password cracker and control of the audio and video recorders. 40

On the Outside Listening in: Intercepting Mobile Phone Calls and Data
An alternative way of monitoring an offender’s mobile activities without installing an application could be the use of
an IMSI catcher, commercially known as a Stingray. This spoofs a GMS tower and only works with GSM phones. (Turkcell,
Vodafone and Avea are all GSM phone operators.) A do-it-yourself tower can be assembled for less than $2000, while
the commercial products tend to cost over $100,000.41 Via this device, a man in the middle attack can be carried out to
“identify an individual’s location, eavesdrop on conversations, and intercept and manipulate SMS messages from the vic-
tim’s phone.” When a mobile device connects to the spoofed tower, data can not only be captured but also passed on to
the “the phone’s calls, SMS messages, and data on to a real tower”, so the person monitored is unaware of the attack.42

The Importance of Diversifying Surveillance Strategies
As internet surveillance tools increase in number and sophistication, so do the tools to counteract such efforts/
maintain internet anonymity and data privacy. As an example, IMSI catchers can de-crypt GSM data. However, this does
not mean that the collected data will not be further encrypted by another cryptographic protocol such as SSL. For insta-
tance, Telegram, a messaging app, encrypts messages using keys only held by the participants and is purportedly being
used as the go-to communication tool for terrorists.37 And, rather than communicate via voice calls, a device user can
use encrypted voice over IP (VoIP) apps. It is also possible to encrypt voice calls, and companies are starting to offer
phones designed for privacy.43 For instance, Silent Circle’s Blackphone advertises anonymous web browsing and private
communication.44 However, combined with the use of in-home video and audio surveillance to determine what devices
the offender has access to, offender internet/communication monitoring approaches might be not be so difficult to
implement and enforce. And, if it is possible for the surveillance cameras to detect and zoom in on device screens, these
software tools might not be needed at all. Otherwise, if you trust that an offender will access the internet only through
one device, then why not trust that he or she will no longer transgress the law?

RE-THINKING THE HOME PRISON: TECHNOLOGY TO REHABILITATE AS OPPOSED TO INCARCERATE?
Unfortunately, even if a parole officer is immediately alerted that criminal behavior is being displayed, the response
time will be delayed by the time it takes for the police to arrive at the offender’s home. In the meantime, a victim could
be raped or murdered or an identity stolen and sold on the dark net. The technology to turn a home into a prison would
require more than just surveillance. And, there seems to be little discussion regarding surrounding residential homes
with armed robotic guards. Therefore, his or her behavior should be carefully and constantly scrutinized for warning signs regarding relapses. Perhaps, surveillance activity could also be used to positively reinforce good behavior and help eradicate (as the original inventors of electronic monitoring intended). For instance, if the parole officer observes that the offender is no longer associating with former gang members and instead focusing on researching job opportunities, then he or she could reduce the offender’s electronic monitoring sentence. Or, if the parole officer observes an offender looking at gang-related material online, he or she could request that the offender attend counseling sessions or a support group. Or, even request that the offender be placed back in jail. Additionally, applications could be developed to occupy the offender’s time with educational/positive activities such as taking e-learning courses or reading/watching self-motivational or spiritual e-material. Electronic monitoring should be used as a trial period to assess an offender’s ability/motivation to re-enter society as a law abiding citizen. Otherwise, if the offender’s motivation for not committing a crime is constant surveillance and the threat of a swift and certain punishment, what will deter an offender from recidivism once his or her electronic monitoring/surveillance sentence ends?

REFERENCES

11 http://www.washingtonpost.com/posteverything/wp/2015/04/28/how-for-profit-prisons-have-become-the-biggest-lobby-no-one-is-talking-about/ (How for-profit prisons have become the biggest lobby no one is talking about, Michael Cohen; 22.11.2015)
16 http://www.pcmag.com/article2/0,2817,2427345,00.asp (22.11.2015)
Mind-Reading Tech Projects That Might Freak You Out, Chandra Steele; 22.11.2015


19 https://www.bccn-berlin.de/People/home/?contentId=661 (Bernstein Center for Computational Neuroscience Berlin, John Dylan-Haynes; 22.11.2015)


23 https://www.youtube.com/watch?v=B8DjTcANBx0 (Black Hat 2013 - Exploiting Network Surveillance Cameras Like a Hollywood Hacker; 22.11.2015)


30 http://streetfightmag.com/2014/05/13/5-platforms-that-gather-in-store-analytics-from-surveillance-footage/ (5 Platforms That Gather In-Store Analytics from Surveillance Footage, Stephanie Miles; 22.11.2015)


34 https://www.talend.com (22.11.2015)


36 Ian A. Elliot, Donald Findlater. “A Review of a ‘Managed Service’ for the home computer use of Registered Sex Offenders.” Hampshire Constabulary & The Lucy Faithfull Foundation (2010).

37 http://resources.infosecinstitute.com/isil-terrorism-and-technology-a-dangerous-mix/ (ISIL, Terrorism and Technology: A Dangerous Mix; 22.10.2015)


40 http://www.flexispy.com/
41 https://www.youtube.com/watch?v=xKihq1fC1Qg (Defcon 18 - Practical Cellphone Spying; 22.10.2015)
42 http://www.charontech.com/man_in_the_middle_article.html (22.10.2015)
44 https://silentcircle.com/ (22.10.2015)