PERPTRAC

The Next Generation of Physical Security Surveillance

Take Control of Your Personal Safety

A Surveillance Method and System Developed and Patented
by Greenline Analytics

US Patent No.: US 10,045,156 B2

Demo App, Summary and Prospectus Accessible at

http://perptracdemo.com

1. EXECUTIVE SUMMARY

A Public Surveillance Utility Supported By A Subscription-Based Service That Allows Users To Identify And Track Anyone Anywhere

The technological innovation known as PerpTrac (Patent No.: US 10,045,156) constitutes a method and a system of indiscriminately collecting everyone's mobile phone beacon data in order to compile in a cloud-based archive a comprehensive portrait of each person's public movements, including identities, geographical trails, speeds and motions. This surveillance service records only the unique unencrypted plaintext networking identifiers from the beacons regularly broadcasted by mobile phones; **PerpTrac does not detect or record encrypted communications like phone calls, text messages, contacts, phone numbers or user-entered internet traffic.** Utilizing dedicated RF detectors and phones containing the crowd-sourcing app as the sensor grid, PerpTrac harvests exclusively the unconcealed networking beacon data from phones (a default background process already performed by Android and iOS devices.) PerpTrac employs advanced data analytics, interfaces with online sources of personal data, and synthesis with both maps and a variety of short-range and long-range video surveillance services to generate a wealth of comprehensible tabular data, visualizations and personal profiles.

Anyone can download the free app to their mobile device to create such a "Guardian Angel" record of everyone nearby. Paid subscribers access the database to investigate specific GPS trails, view detailed personal profiles, and enable watchlists. Features include the capabilities to **track the detailed movements of anyone (known or unknown)** manually, view detailed personal profiles of anyone, or **enable text-message alerts** from proximity-based automated surveillance **of personally watchlisted individuals**, **groups or places** -- such as yourself, loved ones, registered drunk drivers, subjects of restraining orders, registered sex offenders, terrorist suspects, persons at risk of committing gun violence, other potential criminals, or high-crime areas. Users can also enable PerpTrac's built-in "hardware-free" **security alarm system for homes, schools, businesses and government offices combining digital and video monitoring**.

By utilizing the watchlist, governments and law enforcement officers can multiply their manpower and warrantless capability for monitoring suspects and enforcing street traffic laws. By conducting a search, they can view **detailed crime-scene reconstructions** to investigate cases and acquire evidence acceptable for presentation in a court of law. Business owners can monitor employee behavior and augment inventory control. Advertisers like Amazon can assemble valuable individualistic marketing data on the verifiable habits and preferences of most people in order to refine targeted advertising capabilities. **Without violating any privacy laws or requiring substantial overhead costs to the service provider, the software-driven PerpTrac system can provide subscribers comprehensive physical security surveillance at a price that the average citizen can afford**. There exists no similar technology in the market of physical security surveillance; ownership of the patent equates to control of the new multibillion-dollar industry of mobile-phone-beacon-based physical-security mass surveillance (MOPS.)

2. WHAT DATA DOES PERPTRAC COLLECT?

Often transmitted every second that a phone is powered on, mobile-phone plaintext beacons serve as a virtual bread-crumb trail tagged with a digital license plate. Data recorded by PerpTrac includes beacon-embedded serial numbers unique to an individual mobile phone, such as the Wi-Fi Media Access Control (MAC) address, the Bluetooth MAC address, the Temporary Mobile Subscriber Identity (TMSI), the International Mobile Subscriber Identity (IMSI), the International Mobile Equipment Identity (IMEI), along with other serial numbers identifying the device on a cellular network. This surveillance method also collects semi-individualistic information elements contained in these beacons that advertise certain attributes of the phone. Such data includes the specific Wi-Fi networks to which the owners have configured the originating phones to connect, the Bluetooth class of device, as well as advanced Wi-Fi networking capabilities, which collectively create a fairly unique digital signature.

PerpTrac indirectly determines the precise locational origin of each detected beacon's transmission to within less than a meter through three-dimensional geographical triangulation employing four or more GPS-enabled local sensors that utilize locational methods such as wireless fingerprinting of areas and received signal-strength indication for the cellular, Wi-Fi and Bluetooth signals detected from mobile devices. **PerpTrac does not read or record the GPS data of a mobile device that does not already function as a PerpTrac sensor**. The local detectors ascertain geographical coordinates and elevation of detected mobile devices. Emulating the internal locational methods employed by smart phones currently, the beacon detectors precisely acquire their own geographical location from

- Internal GPS capability
- Cellular ID location services from local cell towers accessed through a cellular service provider

- Scanning for the distances to identifiable local cell towers, Wi-Fi access points and Bluetooth beacons whose geographical coordinates are available in publicly accessible databases

- Terrestrial "GPS-simulating" transmitter services provided by NextNav and Locata

- Inertial sensors that include a compass (for direction), accelerometer (for speed) and gyroscope (for turning motions) that allow the sensor to extrapolate its own location based on recently acquired location data

- Barometers and thermometers that, in combination with local weather data, allow determination of altitude along with GPS, Wi-Fi and cellular

PerpTrac's tracking capability precisely determines the location of its sensors and, by association with this data, acquires through dozens or hundreds of these sensors the location data on the same individual phone beacons from detected devices. Collectively the Wi-Fi, Bluetooth and cellular beacons from mobile devices can transmit multiple times every second to several PerpTrac sensors in close proximity, allowing PerpTrac to ascertain through triangulation numerous highly precise geographical "bread-crumb" coordinates that help to produce an exceptionally accurate record of a geographical trail. In order to prevent surfeit data, PerpTrac does impose limits on the number of serial numbers that the system records for each signal type from individual phones.

Modern communications networks' rigid requirement for connected devices to transmit unencrypted unique serial numbers to manage data routing confirms that PerpTrac's method of surveillance will continue to operate effectively in the foreseeable future. The advent of 5G cellular networks augments PerpTrac's surveillance capabilities by increasing the frequency of cellular beacons and diminishing certain aspects of network security in order to manage the addition of so many more devices and so much more data traffic. Nor will 5G replace Wi-Fi in the near future considering the continuous expansion of Wi-Fi's

- Market
- Bandwidth capabilities
- Reductions in hardware costs
- Reductions in access fees (Wi-Fi is free in many areas)
- Entrenchment in communications infrastructure
- Customer control of network management (nonexistent on 5G networks)

A great improvement in PerpTrac's already comprehensive surveillance powers has arisen from the complementing of Wi-Fi with a new high-speed networking option that improves PerpTrac's capability to track precisely identifiable geographical trails.

A PerpTrac sensor only relays to the central archive the unencrypted networking beacon data from detected nearby mobile devices and the sensor's own location data internally generated from within the PerpTrac app. **PerpTrac neither detects nor collects any encrypted communications from any device, such as phone calls, text messages, phone numbers, contacts, email messages, email addresses, data transmitted by other apps, or website traffic including browsing or submissions.** Instead, PerpTrac collects the plaintext networking utility data from all mobile phones that, only when aggregated by numerous sensors and stored in a central archive, can illuminate the public movements of identifiable persons. PerpTrac amplifies this data collected by its sensors with various personal information from public databases and third-party data vendors.

3. HOW IS THE DATA COLLECTED?

PerpTrac employs millions of local sensors in the form of both dedicated RF scanning devices (cost = $500 per unit, range = 1.5 square miles) and smart phones with the free crowd-sourcing PerpTrac app installed. These two forms of detectors sense the regularly repeating unencrypted RF beacons transmitted from mobile phones, including unique serial numbers, recorded Wi-Fi networks and class of Bluetooth device. The app serves both as a portal to the database AND a crowd-sourcing sensor that works in the background on any smart phone with the free app installed. Subscription-based access open to anyone allows app users to utilize the portal to identify, track and monitor virtually any person carrying a mobile phone virtually anywhere. Aside from subscribers, nonsubscribers can also use the free app as a physical security surveillance sensor that will constantly monitor their surroundings 24/7 in order to provide law enforcement officers and civilian subscribers detailed data on the identities and GPS trails of everyone who passes in the proximity of the phone. Anyone with the app installed can enjoy a high degree of confidence that investigators will solve virtually every crime that occurs within the phone's proximity. Moreover, nonsubscribers will have a record of people's movements in their proximity that, when merged with records from other sensors, they can access in the future if they later decide to subscribe to the service. Although some dedicated sensors will also be utilized to gather the data too, the millions of smart phones that will have this free crowd-sourcing app installed will function as the primary sensors for this system. In other words, the vast majority of the hardware costs for the sensors has already been paid for in the initial cost of the smart phone by people who will download the app in the future. Customers who want the enhanced quality and reliability of surveillance provided by dedicated high powered sensors can purchase and deploy these specialty detectors themselves, in a simple process similar to installing an Internet router. PerpTrac amplifies the data collected by its sensors with various personal information gleaned from public databases and purchased from third-party data vendors.

4. WHAT DOES THE PROCESSED DATA INCLUDE?

Naturally, an enormous list of serial numbers tagged with time stamps and geographical coordinates would not constitute a digestible presentation of information for the average consumer, nor even for a professional investigator. Once the sensors first receive beacon transmissions from nearby mobile phones, the sensors relay this raw data to the central database that compiles it. Advanced data analytics then discern dozens of details about the historical movements of individual phones and the interactions of their owners. In this manner, PerpTrac extracts from the raw beacon data all information potentially relevant for a criminal investigation.

PerpTrac then amplifies this processed data with related information on people's identities and movements acquired from other data collection services, free online personal-data archives, video surveillance collection companies, and a PerpTrac-based outsourcing private-investigator utility. These third-party sources include resellers of data mined from SS7 cellular carrier location databases that contain records of the locations of all cellular phone users. PerpTrac also allows subscribers to aggregate further information on the subjects of their searches with options to purchase private information about individuals from third-party personal-data brokers like Axiom and Epsilon, along with other sources of personal data mined from users of websites and apps. Publicly available information includes data from social media sites like Facebook and public databases like the White Pages.

In response to a subscriber's specific query, PerpTrac generates a simplified presentation of the relevant information from its database in a user-friendly chart complemented by visualizations on Google Maps, Google Street View and local video surveillance. PerpTrac permits subscribers to simplify the vast archive of data and precisely refine searches to maximize the ease with which users can find and comprehend the data relevant for their search. The search parameters control panel (that is always accessible from any search results page) allows users the choice to display or not display most of the

search parameters and filters, and that choice can be saved for future searches until the user decides to change it. Additionally, the user can refine the search by designating specific ranges or values to filter the search parameters. Users can save multiple configurations of selected search parameters and filters, and then choose to apply these settings only to the displayed search results, the entirety of the current search results, or to all search results. These results for identifiable historical geographical trails include visualizations illustrating much of the data, a detailed chart displaying the data collected from mobile phone beacon events, and links to detailed personal profiles of individuals.

Identification Method

PerpTrac associates recorded geographical trails with identities by employing overlapping methods for extrapolating the home address of the owner of the tracked phone. The central database's record of an individual's entire historical geographical trail synthesized from a digital breadcrumb trail of unique serial numbers allows the system's data analytics to detect routinely visited locations that form the basis for this identity discovery. The primary method for such discovery involves ascertaining a phone's regular location during time windows of eight hours or more and then cross-referencing this location with public databases of street addresses in order to confirm that the site is a residential address. White Pages listings and other supplemental online personal-data archives can help to determine the names of tracked subjects based on a home address. Similarly, PerpTrac surmises the place of work or school for the individual, when applicable, and displays this information along with the home address in the expanded name field.

Aside from a phone's locational trail, PerpTrac utilizes other raw beacon data from mobile devices owned by that individual to validate this extrapolation of the home and work addresses. PerpTrac cross-references the presumed home and work locations with the country and home network code embedded in the IMSI (International Mobile Subscriber Identity) serial number, when detected from that geographical trail by any one

of the millions of PerpTrac sensors. The surveillance service further verifies the home and work addresses by analyzing the IMEI (International Mobile Equipment Identity) beacon records of more stationary cellular-enabled mobile devices, like tablets and laptops, associated with that contiguous geographical trail. If these devices do not frequently depart the presumed home address and only signal during limited time frames when that person's phone beacons indicate they are present at the presumed residence, PerpTrac analytics may infer that the person is home and using the device. Similarly, an analysis of Bluetooth devices based on the broadcasted Class of Device designation can validate the presumed home and work address.

A cross-comparison of the presumed home and work addresses with the configured Wi-Fi network list broadcasted by devices owned by that person can also aid in this identity discovery. PerpTrac first ascertains the GPS coordinates of these hotspots by accessing public databases of Wi-Fi locations like Wireless Geographic Logging Engine or paid services like Skyhook. Password-protected Wi-Fi networks in the configured network list that correspond to the locations of the presumed home or work site can corroborate the discovery. PerpTrac facilitates this analysis of the Wi-Fi networks to which an individual routinely connects by aggregating a comprehensive list of mobile devices owned by that person, including the type, manufacturer and model of device denoted by the IMEI and suggested by the MAC addresses. In addition to aiding the identification process, this secondary analysis also helps the surveillance system disregard for tracking purposes mobile devices, like laptops and tablets used by some people, that do not help ascertain useful locational trails.

Third-party investigators can contribute to the identification process by interfacing with the PerpTrac database in order to generate leads that result in certifying an individual's identity. Aside from simply questioning an individual at the presumed home or work, analysis of other frequented locations along that person's historical geographical trail and saved Wi-Fi network lists from a mobile device used by that person can allow police investigators to determine a person's identity from CCTV footage and records of credit card transactions. PerpTrac also offers the option to overlay on the map of an entire GPS trail the sites of known CCTV cameras along this route that can assist identification

through the same method. Similarly, questioning associates linked by PerpTrac data to a tracked subject can facilitate this identification process. PerpTrac's private investigator outsourcing service can also aid the identification process in this manner. Police and PerpTrac's PI's can then submit findings from such investigations to a PerpTrac review board for possible inclusion in the service's publicly accessible subscription-based database.

Although PerpTrac does primarily identify a person based on a home address that likely serves as a residence for multiple individuals, the service's secondary utilizations of other personal information extracted from mobile-phone networking beacons enables the surveillance system to distinguish between everyone residing in a single domicile. The unique serial numbers of each person's phone directly aids in this differentiation. Moreover, these unique digital tags indirectly help PerpTrac to discern between different people living at the same home by manifesting unique geographical trails with temporal movement routines and frequented locations that constitute an individual's GPS fingerprint. As with general identification, video surveillance can also assist with discriminating individuals who share the same home address. A fusion of unique mobile-device serial numbers, digitally and geographically fingerprinted GPS trails, online databases, video surveillance and third-party investigators endow PerpTrac's data analytics with the knowledge required to extrapolate personal identities from the torrents of alphanumeric raw beacon data broadcasted by mobile-devices incessantly pulsing through public airwaves.

Visualized Data

Google Maps, Google Street View photographs and third-party video surveillance form the basis for PerpTrac's visualized search results. PerpTrac provides data-enhanced video surveillance to both subscribers who have independent access to local video surveillance and those who do not have such access. For subscribers with independent access to video surveillance feeds available online, (like street cams or security cameras on homes, business and government buildings), PerpTrac offers an interface with these services augmented by seamless integration with the PerpTrac database. PerpTrac permits manual inputs of video-surveillance feeds from short-range GPS-mapped fixed cameras (initially mapped through the PerpTrac interface by the user, if necessary) and GPS-guided drones independently accessible by individual subscribers. For all users, partnership with companies that conduct and resell long-range aerial video-surveillance, like the San Francisco-based startup Planet and Dayton-based Persistent Surveillance Systems, represents an optional capability that the PerpTrac company may choose to deploy. Such a video service can provide subscribers with reliable 24/7 video feeds covering populated areas generated by miniaturized satellites, low-flying drone swarms, standard commercial drones and camera-mounted Cessna aircraft. Subscribers can pool funds to expand the aerial surveillance zone or otherwise place on private property (including cars) license-plate cameras and other high-definition zoom cameras, along with fixed high-definition wide-area cameras located atop high-altitude structures, in targeted locations to provide all subscribers with supplemental ground-based video footage. Along with these additional funds provided by individual subscribers, the federal subsidies to finance these forms of video surveillance may assist the PerpTrac company in covering the remaining costs of this augmentation to the service. The reliability of a combination of 24/7 short-range and wide-range aerial video surveillance of population zones provides a bedrock for correlating the phone beacon data recorded by PerpTrac with a visual record of the physical movements of people in public.

Subscribers can view PerpTrac data superimposed onto any of these visualizations so that moving markers, locational trails and stops appear overlaid on the chosen visual

background of a subject's public movements. 3D imaging of locations from Google Maps and Google Earth allow PerpTrac to visually display on three-dimensional maps the collected altitude data of mobile devices. Additional information like speed or associates appear when the subscriber clicks on a segment of a displayed geographical trail. Subscribers can also choose to display a number of types of sites of potential interest. One optional feature overlays on maps or GPS-mapped video feeds color-coded markers signifying the locations of sites where selected individuals frequently visit. PerpTrac derives this information from a simple analysis of that person's historical geographical trail recorded by PerpTrac, corroborated by a cross-comparison of the Wi-Fi configured network list broadcasted by devices owned by that person indicating locations frequented by that mobile device. Another optional overlay utilizes data from the Tritech crime-mapping system to superimpose on the visualizations any reported high crime areas in the search area. Also, users can choose to display known CCTV video surveillance sites in the search area (which they can limit to only cameras along displayed locational trails) that can allow investigators to better track or identify persons of interest (by facial recognition or locating the site of credit card transactions.) The synthesis of refined phone beacon data with the corresponding maps and video provides a lucid illustration of locational trails and macroscopic physical behaviors that can serve to enhance investigations and provide persuasive evidence in a court of law.

Chart Data

The user can organize a chart in a view based on any of the selected search parameters.

Name Field

The name field constitutes the foundation for the surveillance service on which the entire data is based. PerpTrac anchors the name field to all recorded mobile phone serial numbers that are linked to an individual owner. This field displays these numbers grouped by device and can also include the owner's name, home address and work or school address. When known by the PerpTrac database, only the name and home address display initially. Otherwise, only the serial number detected for that beacon event displays initially. Clicking on the expandable name field allows users to view the work address (if available) and all of the serial numbers of mobile devices associated to that person, grouped by device, with the device and serial number detected in that particular beacon highlighted in bold font. For example:

John Smith
Home: 11 Farmington Ave., West Hartford, CT 06119
Work: Day Hill Dental, 1060 Dayhill Rd., Windsor, CT 06095

iPhone 5s

TMSI:	####, . . .
IMSI:	####
IMEI:	####
Wi-Fi MAC Address:	**####**
Bluetooth MAC Address:	####
Configured Network List:	Smith Home, Starbucks, …
Bluetooth Class of Device:	Mobile phone

Kindle Fire HD Tablet

Wi-Fi MAC Address:	####
Bluetooth MAC Address:	####
Configured Network List:	Smith Home, xfinity, …
Bluetooth Class of Device:	Tablet

Unless the user adjusts the default setting for duplicate events (see below), only one event displays per person in the search results chart.

Options in the name field allow users quick access to an individual chart for this person exclusively, or alternatively to remove this person from the current display of search results. In the search parameters control panel the user can limit the displayed search results to entire groups, such as watchlist, watchlist plus selected people, whitelist, whitelist plus selected people, infrequent visitors, infrequent visitors plus selected people, and other custom groups created in the watchlist. One option present in every name field, both in search results (visualizations and charts) and the watchlist, is a shortcut to that person's personal profile page where users can view all information collected about that individual. Conversely, the name field in the search results and the profile pages allows the user to add that person to the watchlist, and the name field in the watchlist and profile pages allows the user to conduct a new search or view previous searches conducted on that account for that individual. In this manner the name field serves as the focal point for PerpTrac's three key features: search results, watchlist and personal profiles.

Other Fields

- Time: The time that one or more local sensors records a beacon event from an individual phone
- Visit Duration: The time interval that the phone is recorded continuously in the specified proximity of the center of the surveillance zone (the designated search area)
- Blink Rate: The time interval between this recorded beacon event and the previously recorded beacon event generated by the same phone
- Duplicate Interval: The minimum time interval between displays of the same form of beacon events generated by the same device. By default, PerpTrac sets the duplicate interval to the value of the searched time frame in order to simplify the chart display to one entry per person. The user can adjust this field as needed in order to display a more detailed analysis of a person's movements either from the search parameters control panel or from the search results chart column title using a zoom tool available there. Of course, if the user sets the duplicate interval to a value below that of the blink rate for an individual, entries for that person's beacons will only display as frequently as the blink rate.
- Device Location: The geographical coordinates of the phone at that time
- Center Location: The center coordinate of the surveillance zone
- Radius: The radius of the surveillance zone
- Proximity: The phone's proximity to the center of the surveillance zone at that time
- Velocity: The velocity (speed and direction) of the phone at that time
- Average-Speed: The average speed of the person in the current search zone

- Lingering: Whether the phone is lingering in the vicinity of the device location during that time frame

- Stop and Go: Whether the phone is moving in a "stop-and-go" motion at that time

- Rapid Acceleration: Whether the phone accelerates rapidly at that time

- Overlapping: Whether the phone moves in a manner that retraces its path at that time

- Frequent Trajectory Deviator: Whether the phone frequently deviates from its trajectory during the designated time frame

- Infrequent Visitor: Whether the phone's owner is characterized as an infrequent visitor to the search area

- Frequent Visitor: Whether the phone's owner is characterized as an frequent visitor to the search area – further corroborated by a cross-comparison of the presumed home address with the configured Wi-Fi network list broadcasted by devices owned by that person

- Associates: Whether the phone's owner appears to be an associate of another person identified in the current search zone, based on characteristics such as regularly lingering in close proximity to another phone, regularly traveling continuously in close proximity to another phone, or sharing in common one or more of the same encrypted Wi-Fi network in the configured network list. An NSA program designated "Co-Traveler" has utilized similar association techniques for several years. Arranging the chart by Associates will group names by shared associates.

- Signal Loss: Whether the signal from the phone ceases (on cellular, Wi-Fi and Bluetooth frequencies, as measured by all deployed sensors) for a significant period of time while the device appears to remain in range of sensors

- Average Signal Loss: A measure of the percentage of time during the selected time frame that PerpTrac ceases to detect any networking beacons from the phone.

Search criterion that involve a measure of a spectrum of values display the recorded value as a color coded number. Such criterion include speed (ex. 85 (mph)), average speed (ex. 81 (mph)), average signal loss (ex. 6%), frequent visitor (ex. 2 (visits per day)), infrequent visitor (ex. .001 (visits per day)), proximity (ex. 8 (meters)), blink rate (ex. .2 (seconds)), duration (ex. .5 (minutes)), etc. Equipped with options to choose which search parameters PerpTrac displays on the chart and to enter values and ranges for most of the search parameters that filter the search results, users can precisely control the display of this content to suit their needs.

Combating Evasion Techniques

In addition to a comprehensive portrait of the average citizen's public movements, PerpTrac provides a sweeping dragnet that can collect data useful for tracking criminals who endeavor to evade this method of surveillance. Several included monitoring features can identify and track people attempting to evade this form of tracking who use burner phones or multiple retained phones, employ falsified serial numbers, only emit certain beacons infrequently, enable airplane mode, disable cellular data, Wi-Fi and/or Bluetooth networking, utilizes encrypted messaging apps, power-off their phones or simply do not carry phones during crimes. The variety of data contained in mobile phone beacons enables PerpTrac to identify and track individuals by following certain signals (like Bluetooth MAC addresses) when those for other networks (like Wi-Fi MAC addresses and IMEIs) are not as easy to follow. Other identifying data that is not randomized, such as the configured network list or the Bluetooth class of device, can further aid in this determination by plotting points along the same geographical trail. Moreover, the amount of recorded beacon events in the PerpTrac database allows the system's analytics to plot moment-to-moment locations and velocities (speeds and trajectories) in order to discern a contiguous geographical trail, which then allows for identification of the user in

conjunction with records of other beacons from that phone and behaviors (like sleeping locations) extrapolated from tracked geographical trails. Additional criteria governing this function include the matches with the Frequently Visited Locations and probable residence signatures of known individuals. This capability receives support from the service's discernment of trackable associates who are traveling with a targeted individual. The fact that PerpTrac's locally situated sensors receive beacon signals before they pass through network nodes allows the system to capture serial numbers like the Wi-Fi MAC address before one of these nodes anonymizes the number. PerpTrac can thereby monitor the movements of identifiable encrypted phones by employing local sensors in this manner to track serial numbers that ignore embedded messaging encryption, virtual private networks and anonymous browsing.

If the PerpTrac sensor grid has a geographical gap (perhaps early in its deployment) that allows a detected criminal suspect to evade continuous tracking and identification, law enforcement can still use recorded serial numbers associated to a phone owned by that individual to identity, apprehend and substantiate evidence suitable for a court of law. A serial number like the IMSI and TMSI can allow wireless service providers responding to a search warrant to identify directly the phone's owner. Numbers like the MAC addresses and IMEI contain coded entries that identify the network card manufacturer or phone manufacturer who can, in turn, identify the WSP and the home address of the registered phone. In the case of a phone not registered to a home address, police can still remotely access through the WSP the phone, including its location and microphone.

A randomizer-detection monitoring feature built into the PerpTrac analytics identifies periodically randomizing serial numbers, such as a TMSI or a MAC address, associated to an individual mobile device. In addition to utilizing the above features, PerpTrac cross references detected changing serial numbers along a contiguous geographical trail with other serial numbers simultaneously detected by PerpTrac as well as the industry-standard encoding format for specific serial number types in order to determine if a number is spoofed, as well as deducing its replacement by another serial number when randomization occurs. In this manner PerpTrac's analytics can group together multiple randomized serial numbers belonging to the same phone for purposes of unified

identification and the creation of composite geographical trails of the phone's owner. When PerpTrac does detect such spoofed serial numbers (with the exception of the TMSI, which periodically randomizes by design), the designation "(spoofed)" appears instead of the several faked serial numbers in search results (though the user does have the option to view the actual spoofed numbers), though tracking of the individual continues unfettered.

Employing these in-house digital detection methods, PerpTrac can identify and continuously monitor the locations of most individuals who attempt to evade the surveillance. Options in the name field of the search parameters control panel allows users to single out such individuals in the search results. Users can choose to display only search results for people that are spoofing serial numbers, using multiple phones, using burner phones or beginning to use a new phone. A separate field displays a signal loss indicator that users can also use to filter search results to only display people whose digital presence disappears from PerpTrac surveillance from time to time. Subscribers can also amplify the results with other people from this foundation without limiting the search results exclusively to such evasion suspects.

Aside from the indiscriminate digital collection of data, PerpTrac's partnerships with third-party personal-data collection companies allows the system to monitor people who elude the above methods of combating evasion. Partnered third-party personal-data brokers that collect information on users mined from apps and websites can improve the scope and depth of PerpTrac's similar database. The purchase and input of vast feeds of long-range video surveillance into the PerpTrac archives allows live monitors and investigators to track criminal suspects who do not carry phones forward or backward in time (at times with the help of short-range CCTV video surveillance locations pinpointed by the PerpTrac map of known CCTV sites superimposed on maps or GPS-mapped video surveillance) to either their residences or associates where mobile phone beacons can then identify them, or else to the locations of credit card purchases or facial close-ups recorded on CCTV that can lead to their identification

One optional capability that the PerpTrac company may deploy involves outsourcing personal information collection to private investigator provides a physical source for streams of targeted surveillance data. Although PerpTrac may in the future utilize existing technology to remotely power on phones that are powered off to facilitate tracking, PerpTrac can currently allow subscribers to hire partnered private investigators to conduct physical surveillance of individuals who sometimes or always emit no phone beacons. This optional service allows subscribers (who could not otherwise afford a PI or integrate that information with the PerpTrac data) to pool funds to pay private investigators to monitor persons of interest physically in order to close gaps in PerpTrac's digital field of surveillance coverage. Taking advantage of the services Uberization of the PI business, contributors to PI funds can select the best PI for the price the fund can pay, as well as finance investigative tools for preferred PI's like drones, cameras and GPS trackers. Employing broad data-collection, advanced data analytics and partnerships with online sources for amplifying the personal information archive, PerpTrac provides a hyper-accurate illustration of virtually everyone's travels. Compiling a series of overlapping data streams, this surveillance method effectively closes the loop on criminals who are undeterred by the daunting challenge posed by PerpTrac to continued criminal behavior and seek to elude this revolutionary investigative tool.

Personal Profiles

By harnessing all of the refined data collected by PerpTrac sensors along with personal information acquired from third parties, PerpTrac assembles an intricate personal profile of everyone in its database accessible by clicking on a person's identity designation on any page. Along with one-click access to the individual's historical GPS trail, the profile page includes a wealth of other information such as

- A photograph of the person
- Physical descriptions like height, weight, visualizations of skin color, eye color, and hair color, along with unique identifying characteristics like visible tattoos
- Links to publicly accessible online videos of the person that may include voice recordings
- Associates (as determined by an analysis of other people who regularly loiter or travel with their proximity)
- Regularly Used Vehicles
- Frequented Locations
- Criminal Record
- Saved search results of this person on the user's account
- Watchlist alerts generated by this person on the user's account
- Additional information acquired from third parties

- A search results map displaying the person's live location

The personal profile page serves as the central hub for comprehensive information on individuals that can serve as a useful adjunct to search results and watchlist entries.

5. HOW DOES A SUBSCRIBER USE THE SERVICE?

Demo App Accessible at

http://perptracdemo.com

PerpTrac serves exclusively to record, analyze and organize this beacon information in a central database that can clearly identify, precisely track and carefully monitor anyone carrying a smart phone virtually anywhere. This archive of people's movements and physical interactions presents the data in a format designed to facilitate criminal investigations by illuminating for subscribers details about these identifiable and precise locational trails, such as an individual's name, associates, home address, or identity as a frequent or infrequent visitor to a geographical zone based on the PerpTrac record of his previous travels, along with the other details cited above in the chart description. Subscribers can utilize three principle features of this surveillance service.

1. Investigate Specific GPS Trails

    a. Previously Identified People: Having entered into the search field a person's name, home address or a phone serial number previously identified by PerpTrac, users can track their historical locations.

    b. Unknown People: Having entered into the search field a specific location and time frame, users can identify previously unknown individuals present at those locations during those time frames as well as track their historical locations both inside and outside of the search zone.

2. View Detailed Personal Profiles: Users can peruse vast amounts of aggregated personal information on individuals. In addition to historical GPS trails, this data includes photographs, physical descriptions, associates, frequented locations, frequently used vehicles, criminal records, etc.

3. Enable Auto-Monitored Watchlists: Users can configure watchlists to send automated alerts to their phones when designated individuals or groups of people trespass in defined surveillance zones.

PerpTrac empowers users with a powerful new personal security tool that can track known people, both identify and track unknown people, illuminate intricate personal profiles of anyone, and send alerts about suspicious movements.

Subscribers can access the archive designed for purposes of physical security surveillance by searching for information on known individuals through a people search or for information on individuals whom they have yet to identify through a location search. In either case, users have the option to select a time frame (by default the current time displays in this field) using a drop-down calendar menu, or the user can change the time frame later from the search results page. As with other features such as the watchlist and Call 911, the capability for voice activation and response within the app can facilitate this process. Search results include a chart composed of several configurable search parameters and multiple forms of visualizations for this refined data. Subscribers can place into surveillance watchlists persons identified in search results, and users can view detailed profile information on specific individuals by clicking on their names on any page.

Users can adjust filters available for most of the search criteria to refine and simplify the search results, limiting the chart and visual displays to only certain people, speeds, etc. Through the basic configurations control panel users can change the default settings that fundamentally define search parameters and filters. Users can add, open separately or merge multiple windows while navigating the app in order to control the on-screen display of information, simultaneously displaying any combination of maps overlaid with locational trails showing stationary or moving locational markers, correlating stationary or rotating images form Google Street View, correlating local video surveillance, and correlating data displayed in one or more charts. The advanced search parameters and filters described above allow users to ascertain quickly information most relevant for an investigation. A Call 911 always appears as a toolbar shortcut while the app is open,

along with unobtrusive promotional targeted advertisement links to Amazon (generated in part by Amazon's data mining of the PerpTrac database and inserted by Amazon into the PerpTrac interface) that include the personalized Amazon menus "Recommended for You" and "Special Deals for You" as well as "Earn Money for Referrals" that offers reductions in the subscription price when subscribers successfully refer new customers to PerpTrac or Amazon Prime.

Visualizations

Google Maps, Google Street View photographs and third-party video surveillance form the basis for PerpTrac's visualized search results. The default search results page includes an interactive map showing the general location of the subjects of the search during the designated time frame, overlaid with color-coded circular markers indicating their precise positions and thinner lines representing their traveling locational trails. Users can click a variable-speed play button to begin movement of the selected circular markers along the path of the locational trail, corresponding to the timings and locations of those people's recorded movements. Black circles along the trails indicate stops. Users can remove the display of the markers or trails at any time from any visualization. Additional options include the ability to change

> The visualization from the default street map to satellite view, Google Street View, PerpTrac's database of long-range video surveillance, or manually accessed short-range CCTV video surveillance.
>
> The search filters from the default settings to another the time frame (which, for a people search auto-adjusts the location to encompass the new locational trail) the radius of the location, the people represented on the visualization (include/exclude watchlist, include/exclude whitelist, include/exclude frequent visitors, include/exclude infrequent visitors, choose people (all color-coded locational trails are faded and the user manually selects which ones to display)

Any of several search parameters from a control panel that includes a more comprehensive set of options

The stationary markers or locational trails of people on the maps always include a user-activated pop-up that permits the subscriber to view that person's identity (name, address or serial number), velocity and time frame at that location. Users can add or remove data fields from this pop-up in the basic configurations control panel.

An informational panel to the side of the visualizations lists all of the people included in the search results. Users can show all names or selected names (a feature also available in the search parameters control panel.) Below these two options PerpTrac lists all of the designated names with color-coded indicators matching the colors of the markers and trails displayed on the visualizations. When a user chooses to only display selected names, the other names disappear from the names list and PerpTrac fades out the corresponding markers and trails from the visualizations so that only the selected people are displayed prominently. From this informational panel users can add selected individuals to the personal watchlist or whitelist. Also on this panel (as well as in the watchlist), users can assign a nickname to any person therein that will populate into all references to that individual across their entire personal PerpTrac account.

PerpTrac provides data-enhanced video surveillance to both subscribers who have independent access to local video surveillance and those who do not have such access. For subscribers with independent access to video surveillance feeds available online, (like street cams or security cameras on homes, business and government buildings), PerpTrac offers an interface with these services augmented by seamless integration with the PerpTrac database. Subscribers initially setup the interface by saving the web address of the connection portal for the third-party video feed along with any login credentials, if required. The user then views displays of all cameras operating for that third-party service's account with each display positioned side-by-side with a Google Map. The user then enters the physical address of the cameras in the Google Maps search field and uses the zoom tool to mirror the geographical zone of coverage for each camera. The user next defines the location of the camera on that map and its approximate height of the

camera from the ground visible in the footage. A visual representation of the camera appears on the map and the subscriber clicks and that camera icon first horizontally (after which the icon flips into a vertical representation) and then vertically to replicate the estimated angle that the camera faces the zone of coverage both horizontally and vertically. Once configured in this fashion, a toolbar shortcut allows subscribers to access quickly their own video surveillance service (or those of independent third parties) equipped with all of the same features (such as zoom and smart-search event-identification) along with the option to overlay the camera displays with PerpTrac data. The combination of independent short-range video-surveillance feeds and long-range aerial video surveillance provides a range of PerpTrac data-overlaid video records for every subscriber.

Charts

Another option allows users to view information on the displayed locational trails in chart form. Users can view all of the people on a single chart, or individual people on separate charts. A color-coded spectrum of tabs appears below this latter option identifying each person by the color associated to their trail on the visualization of the search results, and users can view these individualized charts one at a time or simultaneously by merging windows. If users decide to open multiple windows inside the app and merge windows for the same search results, one option permits the user to synchronize the highlighted chart display with the activity in the visualization. For example, if the user chose to display an individual's chart and the corresponding map and then played the locational trail to engage the marker to proceed along the historical path, with the chart sync enabled the single-row highlighting on the chart moves from event to event following the progress of the marker on the map. Zooming in on the map would zoom in the results of the duplicate interval on the chart, unless the user unlocked this column's sync feature from the search parameters control panel.

PerpTrac does impose some limits on account usage. Subscribers can save or share with other subscribers their configured search results. There does exist a limit to the number

of shares permitted, particularly when it includes data that the subscriber personally purchased from third-party personal-data vendors) saved in a list of contacts linked to their PerpTrac account. Similarly, PerpTrac does impose limits on the number of people for whom a subscriber can search or add to a watchlist. The $9.99 subscription fee may include unlimited searches for ten designated family and friends, as well as five free searches for other people every month. Subscribers are then charged for each additional search after reaching this quota. There is also an upper limit to the number of people allowed on a watchlist or whitelist, but this depends on server load and will vary. However, subscribers can watchlist or whitelist entire groups of people, such as registered sex offenders, and designate entire groups of locales or people as no-trespass zones. Subscribers can share their account with a limited number of family members living at the same residence.

Subscribers can view more in-depth information by accessing PerpTrac's compiled personal profiles of tracked individuals linked from the search results page. Options to enhance the data within search results and these profiles include interfaces with third-party personal-data brokers for purchasing additional data on identified individuals, as well as a PerpTrac private investigator outsourcing service that subscribers can crowd-fund to track designated individuals. Users can access these interfaces through a crowd-funding link available on search results and profile pages, from which users can create or join crowd-funding groups for this purpose and then contribute part or all of the funds necessary to initiate the supplemental data acquisitions. Data acquired from these sources that does not fit into any of the fields for search results will automatically populate in personal profile pages for that individual, along with all of the other data on that individual. Subscribers can share these profile pages, but with the same limits on sharing any data purchased from third-party data vendors. The profile pages include shortcuts to all saved search results for the person, their frequented locations (also viewable on the search results visualizations), their associates, all watchlist alerts generated by this person's movements, along with other detailed information.

Watchlist

In addition to the search results and personal profiles functions, the watchlist feature represents another primary utility provided by the PerpTrac service. An optional automated alert system linked to personally generated watchlists and whitelists permit subscribers to receive an audio-visual alert about persons or places of concern when either the tracked person (which can include the subscriber or another person from the whitelist) enters or departs designated geographical zones or personal proximity areas during designated time frames, or an unknown person trespasses or makes designated suspicious movements in a designated zone at a designated time. A whitelist designation denotes an exception to the watchlist when the person on the whitelist is not the actual subject of a configured watchlist alert. By default the whitelist includes the subscriber and all family members with access to this account, but may also include other people such as the subscriber's children, spouse, parents, extended family, friends, co-workers or employees.

The alert originates on the phone through the app (which will open fully out of its background scanning state if not already open), at maximum volume (overriding the phone's current volume settings) or if the app cannot open properly because the user has temporarily disabled Wi-Fi and cellular data on their phone then the PerpTrac service sends a text-message alert to that phone. Subscribers can also add a limited number of other phones as recipients of such text-message alerts, though the recipients will have the option in the text message to opt out of receiving alerts from this PerpTrac account or any PerpTrac account at any time. Subscribers can share all or selected entries of their watchlists with other subscribers by clicking a share option on that page.

By default PerpTrac configures but does not enable a personal security alert and a home security alert for the subscriber that issues an alert between 12 AM – 6 AM if anyone not on the whitelist trespasses within these zones. As with all watchlist entrees, the subscriber can better calibrate these entries at any time. These two watchlist subjects (termed "everyone barred from me" and "everyone barred from my home") appear as

thumbnail-icon shortcuts in the top toolbar visible on every page next to the Call 911 option, an optional shortcutting feature using designated avatar thumbnails that the user can configure for any subject on the watchlist.

Criteria for the watchlist include the person, persons or group being tracked, the “barred from” location, person, persons or group, the radius of the no-trespass zone, as well as any relevant specific time frame or suspicious movements, including speed limitations. In order to populate the watchlist, in the subject field subscribers can

Add an individual to the watchlist (or whitelist) from the map or chart in the search results page

Search for a specific person from the name field in the watchlist page

Select one of several predefined people groups

Create and select a custom people group through a link on the watchlist page

Some predefined people groups include everyone, watchlist, selected people on the watchlist, associates of anyone on the watchlist, associates of selected people on the watchlist, selected associates of selected people on the watchlist, whitelist, associates of selected people on the whitelist, selected associates of selected people on the whitelist, infrequent visitors to a defined location, frequent visitors to a defined location, registered sex offenders, registered drunk driving offenders, designees of a terrorist watch list, registered felons, and associates of other blacklisted subjects.

The user then chooses an approximate location or a specific person in the location search field on this page. The user defines one or more locations in the “barred from” location/people field on this page in the same manner that they choose a location in the main PerpTrac search page. Users can alternatively choose one or more predefined location groups, such as the subscriber’s home, bars and liquor stores, gun stores and gun shows, childcare centers, schools, high crime areas identified by the third-party Tritech crime mapping system, and custom groups created by other PerpTrac subscribers.

Alternatively, users can create and select custom location groups through a link on the watchlist page. Users can define the specific location with a combination of the map zoom tool and a zone-activating rectangular highlighting tool (with options to add or subtract pixels, create multiple selection areas and inverse the selection area(s)) on a map displaying that search result. In cases when the subscriber wants to receive an alert when the subject of a watchlist entry departs a designated zone, like a child leaving home or school unauthorized, the user simply designates the location and clicks the inverse option to bar the subject of the watchlist entry from entering any place other than the originally designated location.

When choosing a person from whom to bar the subject of the watchlist entry, options include the subscriber, a person from the white list, another subject of the watchlist, felons, designees of a terrorist watch list, another identified person or a user-defined address. Users can then manually adjust the default radius of the alert zone for the selected "barred from" person. Alternatively, subscribers can select a group of people, such as whitelist or a series of individually entered persons, and then define a universal radius or configure the radius for each individual person or location.

Beyond watchlisting people based on their identities or locations, subscribers can enable watchlist surveillance of people based on their behaviors, including the timing of their appearance at a location, and other suspicious behaviors at a location such as speeding, loitering, backtracking or circling. The user can define the time frame as always, designating a particular time of day, time of week, time of month, time of year, or a custom time frame with a special start and end time. The user can define the speed criterion as N/A (the default setting) or a greater than / less than of a particular value in miles per hour. The user can simply enable static options such as loitering, backtracking or circling. For example, a traffic cop can watchlist anyone from a stretch of road around closing time for bars on Friday and Saturday nights based on speeds in excess of 20 mph over the posted speed limit. Alternatively, a home owner can watchlist infrequent visitors from their property, sidewalk and the surrounding street during 12 AM – 6 AM based on suspicious behaviors like loitering, backtracking or circling. In addition to the configurable options visible on this page, an edit button permits users to adjust other

criteria for the watchlist. Aside from these features, users can utilize most of the other search criteria, such as the burner-phone-user indicator, to create and modify watchlist groups. Combining charts, visualizations, profile pages and watchlists in a surveillance service founded on a massive umbrella archive of data cataloguing people's movements, PerpTrac provides comprehensive solutions to the challenges faced by most law-abiding citizens and criminal investigators.

6. HOW CAN PERPTRAC HELP ME?

By precipitating the advent of the new industry of mobile-phone-beacon-based physical-security mass surveillance (MOPS), PerpTrac has the potential to illuminate crime scenes, monitor suspects, deter crime and empower citizens with a powerful new tool enhancing personal and public safety. The broad range potential applications of this technology can address a host of perennial societal problems that have plagued modern civilization.

1. Home Alarm and Personal-Proximity Alarm: Popular watchlist features created and shortcut by default allow subscribers to easily enable a home alarm system or proximity alarm system to receive alerts when designated “trespass” events occurs. Included with the $9.99 monthly subscription at no additional cost, this alarm system offers an economical alternative to traditional home alarm systems and bodyguards.

2. Locating and Monitoring Loved Ones: Watchlist designations permit subscribers great ease when keeping track of loved ones. Enabled watchlist entries can alert the subscriber whenever a loved one leaves a designated area, or whenever an unwanted person enters close proximity to the loved one. Even if a watchlist entry is not enabled, shortcut icons in the toolbar allow quick access to a comprehensive description of a loved ones travels and current whereabouts. For example, using Google Assistant voice activation a subscriber could simply say, "Find my daughter," to see her location on Google Maps, and "Show me where she has been tonight," to see her locational trail on a map or long-range video surveillance including dots and time frames at locations where she visited, and "Who has she been with tonight," to see a list of the names or home addresses of her associates, and "Where did each of these people go when my daughter's phone was off tonight," to see the relevant locational trails for that time period.

3. Guardian Angel: Anyone with the free app installed on their phone, whether a subscriber or not, enjoys the security provided by 24-7 recording of everyone within their proximity regardless of any watchlist settings. From car accidents to robberies and almost every physical crime in between, PerpTrac monitoring can report to police and courts critical information through its public database that originated from the victim's phone's proximity surveillance.

4. Monitoring Criminals -- The Watchlist's Scope: Text message alerts inform subscribers when designated known or unknown individuals trespass or move suspiciously within designated geographical or personal-proximity zones. By using machines to efficiently digitize the previously labor-intensive surveillance process, PerpTrac's watchlist serves both police and civilians as a manpower multiplier.

    a. Terrorism: Instead of 100 law enforcement personnel tracking a single terrorist suspect 24-7, a single law enforcement officer can track 100 terrorist suspects 24-7 by utilizing PerpTrac's watchlist feature to send the officer text-message alerts whenever a suspect lingers in close proximity to another suspect or potential target, or whenever a suspect enters a gun store or gun show, and in so doing potentially stop terrorist attacks. Embedded encryption messaging or virtual private networking utilized in part by individuals trying to evade surveillance of criminal activities, such as the previously known ISIS associates responsible for the 2016 Paris attacks, cannot conceal the phone's owners from PerpTrac surveillance. (See ante, **4. WHAT DOES THE PROCESSED DATA INCLUDE**, *Combating Evasion Techniques*.) This multiplied monitoring manpower will allow governments to expand greatly terrorist watchlists in order to include all known suspects, as opposed to the longstanding practice of limiting these watchlists to only the most obvious terrorist suspects while removing less conspicuous suspects from active surveillance, as occurred in the case of the Boston Marathon bombing ringleader. In particular, investigators can incorporate these expanded terrorist watchlists into the

PerpTrac watchlist service to provide automated 24-7 protection of all public transportation choke points and gathering sites from anyone exhibiting affiliation with terrorist groups like Al Qaeda and ISIS.

b. School Shootings: As an early warning indicator of school shootings, PerpTrac allows school security and administrators to receive alerts when infrequent visitors encroach upon school grounds while classes are in session.

c. Other Crimes: Similarly, police or victims can use the same technology to monitor any individuals who are at known risk of committing gun violence, domestic violence, sexual violence, violation of restraining orders, geographical parole violations, or other repeat offenses such as drunk driving. Subscribers can also track victims of crimes or their perpetrators at-large, such as in the cases of amber or silver alerts.

5. Crime Scene Reconstruction: PerpTrac's location-based search function also serves as a manpower multiplier for the previously labor-intensive task of crime-scene investigations. Police investigators can immediately learn the identities, precise movements, associates and locational histories of all persons of interest at any crime scene accessible without warrants in a user-friendly database that helps to minimize an investigation's manpower requirements. Mobile phone beacon data collected by PerpTrac, personal data acquired from public databases and partnered third parties, and long-range video surveillance that PerpTrac purchases from other companies provides a detailed, comprehensive portrait of crimes. Investigators can even track people through areas of limited visibility with PerpTrac's map of beacon data and purchased infrared video surveillance of corresponding locations. In addition to facilitating the investigator's understanding of the crime scene and generating leads, evidence acquired through PerpTrac can be acceptable for presentation as evidence in a court of law. Whether the crime is premeditated or, as in the case of most crimes, not premeditated, PerpTrac preserves this detailed record of the crime.

6. Immigration Control: Immigration control officials can digitally monitor groups of illegal immigrants crossing national borders at unauthorized points of entry by enabling a watchlist addition for the border region that issues alerts whenever any phone not whitelisted trespasses in this zone at any time. The tendency for such illegal immigrants to travel in groups that have at least one phone makes them particularly susceptible to this form of monitoring. Beyond pinpointing precise locations, PerpTrac's ability to conduct surveillance across national boundaries also enables the service to identify immigrants, both legal and illegal, as well as smugglers of illegal immigrants. This identification technology could facilitate monitoring, management and recording of border crossings at official points of entry.

7. Rescue Operations: PerpTrac can help to guide rescue operations for people lost, incapacitated or trapped inside hidden locations in disaster zones or the wilderness with the capability to locate precisely these people through the use of sensors that subscribers have already deployed or new sensors that rescuers use in transit to track down those in need of urgent help.

8. Identification Despite Poor Visibility: One of the primary drawbacks of video surveillance represents no challenge to PerpTrac's digital surveillance of mobile phone beacons. Nighttime, bad weather, coverings (like hats, sunglasses and masks) or objects (like vehicles and buildings) obstructing facial recognition or license plate identification, areas without video surveillance, the visible anonymity of crowds (such as riots) and other visibility obstacles have no impact on diminishing PerpTrac's surveillance of RF beacons conducted by millions of sensors located in every populated area. PerpTrac renders ineffective the easily donned cloak of invisibility that criminals have enjoyed throughout history continuing into the age of video surveillance. PerpTrac then supplements this tracking methodology with video surveillance feeds from satellites, aircraft, mobile and fixed ground cameras that display infrared video recordings during times of limited visibility. A toolbar shortcut allows subscribers one-click access to a visualization of PerpTrac data for their personal proximity zone displayed on

a map, Google Street View 360-degree photographs or video surveillance (where available.)

9. Dissuading Criminals: The daunting prospect of eluding PerpTrac's surveillance dragnet may dissuade many premeditating criminals from committing criminal offenses, as well as increase the average individual's self-awareness of law-abiding behavior to ensure greater compliance with the established legal codes. By catching some criminals and dissuading many more people from committing crimes, PerpTrac can reduce crime in order to produce a host of benefits such as diminishing the threat of criminal behavior to the average citizen, raising property values, improving schools, increasing development of commercial and residential areas, lowering incarceration rates, and reducing the number of car accidents.

10. Street Traffic Surveillance: One feature of the watchlist allows an automated service to monitor street traffic violations in any area for enhanced traffic law enforcement. Police officers can enable the automated surveillance of speeders, traffic-light violators and other reckless drivers in order to receive alerts about their violations and have access to digital evidence suitable for a court of law. A simple location search can quickly solve virtually all violent cases involving motor vehicles, including hit-and-runs and drive-by shootings.

11. Marketing Research: Marketers can harvest valuable personal data for enhanced targeted advertisement opportunities by surveying the geographical routines and physical behaviors of a majority of a nation's population. The potential for an exclusive partnership with Amazon may produce the greatest utility for this purpose. Allowing Amazon exclusive access to the entirety of the database (without any of the restrictions on the number of searches and amount of simultaneously viewable data placed on subscribers) would allow Amazon to merge this personal data about personal habits and routines with its existing profiles of buying habits to create much more refined predictors of customer preferences that can greatly augment Amazon's targeted advertising capabilities. Small, unobtrusive links to Amazon in the toolbar may include replications of Amazon menus for individualized recommended products and services for users

of that account, special deals for these recommendations, and a promotional offer that deducts some percentage of the next month's subscription fee (maybe a free month) for subscribers who refer new customers to either PerpTrac or Amazon. Similarly, a link on the sign-up page can offer a reduction in the subscription cost when a new subscriber uses the Amazon Prime link to also sign-up for Prime, a reduction that will continue as long as that PerpTrac subscriber remains subscribed to Prime. By powerfully enhancing Amazon's targeted advertising precision while also augmenting Amazon's customer base, PerpTrac can generate a large revenue stream from expanding the use of the database to include marketing purposes.

12. Employee Monitoring and Inventory Control: Employers can closely monitor employees to ensure job compliance and, in combination with local video surveillance, monitor both employees and customers to prevent inventory loss from theft.

13. Lie Detector: Subscribers can immediately corroborate people's claims about their locations and travels, including optional voice assistant responses to interrogations.

14. Military Surveillance: The wide-ranging surveillance capabilities of the PerpTrac service can augment existing capabilities for militaries worldwide, from tracking down targets, identifying belligerents and otherwise monitoring people's movements on urban battlefields.

These benefits represent a mere snapshot of the boon to society offered by this surveillance technology.

7. HOW COSTLY, UNIQUE AND PROFITABLE IS THIS ENTERPRISE?

For the relatively small expenditure of $50 million in the first year and $30 million per year in subsequent years to develop and maintain the physical surveillance service, the unique proprietary PerpTrac method and system offers **the potential for billions of dollars in profits per year to the company licensed to sell the service. The costs amount to a relatively minimal investment due to PerpTrac's identity as a service that (1) chiefly functions on software-driven mechanisms** devoid of physical infrastructure owned or maintained by the company, (2) partly outsources to services directly paid for by subscribers (in addition to the subscription fee), and (3) represents a high-publicity technology that may not require substantial additional advertisement. Moreover, federal grants for homeland security and law enforcement innovations may assist with the modest development and maintenance expenditures. Revenue generated from subscription fees to subscribers as well as sales of dedicated sensors can also help to offset remaining costs. With the potential to create and dominate the new industry of mobile-phone-beacon-based physical-security mass surveillance (MOPS) through exclusive U.S. proprietary rights to the foundational method and system for that industry as well as an absence of proprietary barriers to business in other countries, the company licensed to sell the PerpTrac service may encounter only minimal market competition. The subscription-based service's general utility to society and individual utility to average citizens could, as indicated by the model of the Amazon Prime service, easily generate billions of dollars in revenue on a yearly basis.

Cost Analysis

Required developmental and operational expenditures for PerpTrac include financing hardware rental fees, separate hardware development and production as well as maintenance, software development and maintenance, acquisition of additional data from third parties, advertising and other manpower requirements.

- The Cloud-Based Database

  Estimated Maximum Cost: $10 million / year

  The primary overhead cost arises from the development, storage space and software maintenance of the cloud-based central archive. By renting space on the cloud, PerpTrac avoids the costs of owning and maintaining the hardware for the database. As with other hardware and software costs, the initial development expenditures will constitute the bulk of the financial investment for this asset.

- The App and Website

  Estimated Maximum Cost: $1 million / year

  Building from the foundation created by the demonstration app accessible at http://perptracdemo.com/, construction of the PerpTrac app and website will represent a significantly less technically challenging endeavor than the backend of the service. With the front-end already engineered in such detail, the contracted software developers may complete this interface with the central database well before development of this backend reaches a fully operational stage. Due to this divergent time window, a limited version of the app and website may deploy alongside a rudimentary database initially and engineers will later add features to

the front-end as they become available on the backend.

- The Sensor Grid

Estimated Maximum Cost: $500 thousand / year ($250 / unit)

Smart phones constitute the vast majority of the sensor grid so that subscribers and non-subscribers have already paid for most of the sensors in the initial cost of the phones on which the sensor runs as a background service of the free app. The PerpTrac company must finance the cost of developing, producing and repairing the warranteed high-powered sensor units, though this expenditure will naturally reflect in the retail price of these beacon detectors. Derived from similar wireless sensors and presumably subsidized by federal grants, such development of these particular sensors can rapidly achieve economies of scale to lower this cost of production. Subscribers directly pay for these optional dedicated high-powered sensors that they self-install (like an Internet router), which cost no more than $500 per unit (extended warranty extra) and cover a surveillance zone of up to 1.5 square miles. In order to increase the coverage of the entire surveillance grid, PerpTrac may incentivize purchase of these sensors with increased subscription benefits, reduced subscription fees or rebates for the sensors themselves.

- Third-Party Video Surveillance

Estimated Maximum Cost: $10 million / year

The integration of video surveillance footage with PerpTrac's aggregated archive of refined phone-beacon data represents a critical facet of the PerpTrac service that warrants prioritized investments in the acquisition of these video feeds recorded by third parties. Relying solely on subscribers and free online sources to provide such footage may not generate a sufficiently reliable and comprehensive video service for most customers; the purchase en masse of footage from resellers may constitute the bulk of PerpTrac's annual investments (and could, optionally, well exceed the $10 million per year cost estimate.) If the company licensed to provide PerpTrac decides to incorporate this optional capability into the surveillance service, PerpTrac will seek to acquire both short-range ground footage and long-range aerial footage purchased for a maximum number of population centers, ideally expanding the service's available video surveillance to most inhabited regions. Subscribers can pool funds to expand aerial surveillance zones or otherwise place on private property (including cars) license-plate cameras and other high-definition zoom cameras, along with fixed high-definition wide-area cameras located atop high-altitude structures, in targeted locations to provide all subscribers with supplemental ground-based video footage. Commercially operated miniature satellites like those deployed by San Francisco-based Planet, micro-drones utilized (not exclusively) by the U.S. Navy, commercial drones, and video-mounted Cessna airplanes like those utilized by Dayton-based Persistent Surveillance Systems currently operate as a feasible source for wide-area aerial video surveillance. Along with these additional funds provided by individual subscribers, federal subsidies to finance these forms of video surveillance may assist the PerpTrac company in covering the remaining costs of this optional augmentation to the service. Improvements in these already effective video recording services may arise from the potential of the PerpTrac company to purchase one or more of these footage resellers buoyed by federal

grants to develop these sources of video surveillance for complete integration with the PerpTrac service.

- Third-Party Personal-Data Brokers

Estimated Maximum Cost: $500 thousand / year

In order to compensate for potential gaps in PerpTrac's surveillance of people's movements and to amplify the database with other personal information potentially relevant for criminal investigations, PerpTrac complements its internally acquired data stream with information from third parties. Free online sources such as the White Pages and Facebook can serve this purpose alongside personal-data brokers like Epsilon and Axiom. International resellers of SS7 cellular carrier location databases can specifically help to corroborate and augment the accuracy of individual location data derived from PerpTrac sensors. While subscribers would finance most of the costs of acquiring such limited-access third-party data through additional fees paid directly to these data brokers, the PerpTrac company may, at its own discretion, purchase some of the data (such as SS7 location information) for unrestricted access to all subscribers.

- The Optional Private Investigator Service

Estimated Maximum Cost: $0 / year

A private investigator service represents one optional capability that the company licensed to provide PerpTrac may choose to deploy. Serving a function similar to that of third-party personal-data brokers, this mass deployment of targeted surveillance based on physically collected personal data from targets can improve PerpTrac's databases, particularly when tracking off-the-grid individuals who do not carry phones. Operating like a paparazzi outsourcing service applied to criminal suspects (as opposed to celebrities), PerpTrac's PI utility allows subscribers to pool funds in order to finance a private investigator to track a person of interest with physical tracking methods and to stream relevant data like GPS positions and video to the PerpTrac database. Although PerpTrac would provide access for all subscribers to information acquired from this surveillance method (following an appropriate waiting period that safeguards the PI from the target's own scrutiny,) individual subscribers would finance the PI utility entirely through additional fees paid through PerpTrac to the investigators.

- Marketing

Estimated Maximum Cost: $0 / year

The revolutionary societal benefits and utility to the average citizen offered by PerpTrac along with its controversial enterprise to help initiate a new age of mass surveillance signify a product that will figure as a centerpiece of public dialogue in the news media and social media. Such discussions reverberating across the airwaves may reach such magnitude that the PerpTrac company need not make significant additional expenditures for advertising. This marketing financial strategy may roughly resemble the revolutionary model of low-expenditure marketing through free advertisement airtime via news media publicity demonstrated by Donald trump's 2016 presidential campaign. Software driven solutions such as the PerpTrac website itself, advertisements through partnered third-party companies and an official social media presence may suffice to supplement the free advertising provided by the public dialogue about this technology.

- Legal

Estimated Maximum Cost: $5 million / year

Although the PerpTrac service does not violate any criminal laws, the possibility of defending against lawsuits by people adversely impacted by this technology represents one potential cost. PerpTrac's U.S. patent and a thorough international patent search conducted during that patent application indicate that there will emerge no significant proprietary challenge to providing the PerpTrac service in any country. While any company should consider some likelihood of civil litigation when formulating annual cost estimates, PerpTrac could face an increased measure of such legal pressure due to the perception that PerpTrac's mass surveillance may infringe on privacy rights and may allow malicious parties to misuse the service for criminal purposes. PerpTrac's civil indemnity from law suits exists on a presumably stable foundation of established legal codes, mass surveillance practices and technologies that includes

  - The well established legality of PerpTrac's data collection methodology, which exclusively harvests unencrypted networking beacon data such as MAC addresses
  - In the event of changes in domestic privacy laws, the option to operate the PerpTrac service from an overseas location immune from criminal prosecutions due to the absence of international legal codes and law enforcement for personal privacy violations
  - The immense free benefits of this technology to both individuals and society
  - The greatly augmented benefits available to subscribers
  - The prevalence of other mass surveillance services worldwide from wide-area video monitoring, license-plate-capture video monitoring, data

mining companies like Google and Facebook that harvest personal information through apps and websites, and the mass recording of telecommunications metadata and content by federal governments

- The unchallenged existence of publicly accessible records of home addresses, telephone numbers and other personal information from the White Pages and social media services like Facebook
- The existence of unchallenged services like the Internet provided by Internet service providers that regularly do facilitate massive criminal activity (black markets, money laundering, stalking, terrorism, attacks on national infrastructure, breaches of protected federal and corporate databases, etc.) while simultaneously providing a valuable utility to individuals and society
- PerpTrac's rigid safeguards against misuse of this service that include an official misuse-complaints review board and PerpTrac's user policy that allows the company to cancel accounts of users who violate this policy and provide extraordinary assistance to criminal prosecutions of such violators

Arguing from this solid legal basis, lawyers on retainer for the PerpTrac company could effectively defend any foreseeable legal challenges to this surveillance service.

- Other Manpower Requirements

  Estimated Maximum Cost: $3 million / year

  Aside from the above costs of developing and operating the PerpTrac service, additional expenditures include customer service for technical support and account management, the misuse-complaints review board, and internal administrative services.

In the unlikely scenario that federal grants for PerpTrac do not materialize, a subscription fee of $9.99 per month charged to as few as three million customers would immediately cover the projected costs of the development and operation of the entire service.

The Market Niche for This Unique Invention

PerpTrac represents a unique technological innovation that faces a scarcity of market competition from commercially available competing technologies because this service marks the advent of the entirely new industry known by the acronym MOPS (mobile-phone-beacon-based physical-security mass surveillance), a subset of the general industry of physical security surveillance. The MOPS method and system encompassed by the PerpTrac U.S. patent has the potential to dominate an industry through exclusive U.S. proprietary rights to the foundational method and system for that industry as well as an absence of proprietary barriers to business in other countries. For the foreseeable future, the single company licensed to sell the PerpTrac service should not encounter market competition in the United States that does not infringe on this patent. The act of filing the PerpTrac U.S. patent has now established its proprietary method and system as prior art barring all parties from acquiring patent protection for this innovation in other countries, ensuring PerpTrac's market access to all countries. A thorough international patent search conducted during that patent application corroborates that there will emerge no significant proprietary challenge to providing the PerpTrac service in any country. Moreover, the likelihood that this company will aggregate a vast database of virtually everyone's historical movements everywhere indicates that no other future startup company, including any that infringe on the patent, will have the capability to offer a comparable service that can rival the historical length and geographical depth of the data available through PerpTrac.

Currently there exists no other commercially available service for mass surveillance of mobile phone identities and movements. Nor does there exist any other service that interweaves this data with visualizations overlaid on maps and video engineered into a user interface designed to facilitate criminal investigations. The absence of such a service, so conspicuous to overworked criminal investigators, explains why some experts contend that approximately 70% of crimes against persons and 90% of violations of street traffic laws go unsolved. Similarly, police are woefully understaffed to conduct preventative surveillance on criminal suspects, such as the subjects of restraining orders

or criminal watchlists. The ongoing expansion of the 9/11 War into its 18th year, the longest war in U.S. history that pits the lone superpower against a ragtag band of outlaws that persistently eludes identification and tracking, perhaps most blatantly demonstrates the inadequacy of current physical surveillance systems.

Presuming a scenario in which a company develops the PerpTrac service to its full potential and the police (who would then require far less manpower to conduct investigations and surveillance) enjoyed sufficient manpower to enforce the law against criminal suspects identified by PerpTrac, this technology has the capability to solve half of these crimes that currently go unsolved. Beyond the impact of catching many more criminals, PerpTrac can further reduce crime rates by helping police intercede suspects before they commit crimes and by dissuading people from committing crimes faced with the daunting microscope of this revolutionary form of omnipresent mass surveillance. PerpTrac has the potential to reduce crime, multiply police manpower and stop terrorist attacks worldwide while simultaneously providing the average citizen with augmented personal security that they can control personally.

Current technologies in the general industry of physical security surveillance collectively represent an antiquated solution for the epidemic of global crime and terrorism plaguing the 21st century.

- Stingrays (IMSI-Catchers): Ranging from $1500 - $150,000, these mobile units constitute fake cell towers that deceive nearby phones into connecting to them, thereby enabling the Stingray operator to have some measure of ability to record encrypted data from a connected phone and manipulate the phone's functions. Fully featured Stingrays pose an extremely high cost per unit. Individual units only cover a limited range and therefore collect a miniscule amount of data on people's movements compared to PerpTrac; Stingrays do not represent a cost-feasible solution for mass surveillance of an area larger than a cell tower's coverage zone. Stingrays do not pool data into a central database, essentially limiting users to a one-sensor system. The raw data collected by Stingrays does not get refined into the detailed portrait of

individuals' movements provided by PerpTrac, nor does the Stingray present the data in a highly organized and user-friendly fashion that greatly facilitates criminal investigations. Since Stingrays function by hacking phones and accessing encrypted data (phone numbers, contacts, messages, voice conversations, internet activity), the conspicuous privacy violations inherent in this technology greatly restrict its potential for mass surveillance. Laws in most countries exclusively limit sales of Stingrays to law enforcement agencies, and their officers can only legally deploy one of these units if first authorized by a warrant. The cost, limited range, failure to pool and refine raw data sufficiently, inadequate data presentation, and severe legal restrictions to owning and operating a Stingray indicate that this technology represents an infeasible option for effective mass surveillance of a large area and entirely negate its potential for use by civilians.

- SS7 Cellular Location Tracking: Resellers of access to SS7 cellular carrier location databases permit customers to locate the approximate live location and limited historical locational trails of other people based on a phone number or serial number linked to an individual cellular phone user. The geographical data cannot precisely pinpoint live locations, let alone detailed geographical trails, since the locational method depends entirely on gauging a phone's proximity to cell towers. Wi-Fi and Bluetooth-based locational tracking, on the other hand, allow for much greater precision in determining individual beacon origins because the sensors operate in much greater numbers and in much closer proximity to the phones, and those systems can extrapolate GPS trails from a much greater number of geographical plot points because those types of beacons transmit so much more frequently than cellular beacons. Aside from the severe limitations in geographical tracking, SS7 access produces very little raw data and virtually no refined data on individuals, restricting its ability to inform an investigation. Users cannot conduct searches for unknown individuals by location, and the system is not designed for mass surveillance so that the ability to track several people is quite limited. Not easily accessible to the average consumer, the system lacks

a user-friendly interface and does not organize and present data in a manner purposefully designed to facilitate most criminal investigations. Although SS7 access can assist an investigation as an adjunct to other surveillance services, the technology does not represent a feasible option for mass surveillance due to its geographical imprecision, limitations on the types of data collected, inability of most people to utilize the service and crude presentation of data.

- Cell-Tower Dumps: Available only to law enforcement officers with a warrant, this service provided by cell tower operators grants access to limited databases to aid investigations into serious crimes (usually violent) that seek to identify persons of interest at a location. A cell-tower dump represents the location-based alternative to an investigator subpoenaing phone records from a wireless service provider for a known person of interest. Regarded with disdain by some officers, cell-tower dumps produce vast amounts of a limited variety of raw data on everyone within a cell tower's zone of coverage, which can measure up to one-half a square mile. The geographical imprecision of the data and its poorly organized presentation often require that investigators devote massive amounts of manpower to identify persons of interest and then acquire more persuasive evidence sufficient to meet the standards for a court of law. Civilians cannot access cell-tower dump services. The fact that police have to rely on this laborious method to conduct digital location-based searches for persons of interest at a crime scene illustrates the current failure of society to deploy an effective mass-surveillance tool in the age of the smart phone.

- Personal-Data Brokers: Currently available only to corporate clients, personal-data brokers provide a broad range of private information on individuals mined from websites and apps utilized by those people. This information can include locational data on identifiable people. The wide variety of personal data distinguishes this service from other physical surveillance options, but the inability of average citizens to access this service

and gaps in the data archives of people or GPS trails negates this alternative as a viable option for comprehensive mass surveillance. Nevertheless, the range and depth of data collected by this service suggests the promise of its incorporation into more comprehensive mass surveillance solutions.

- Digital Tags: The tagging of persons or property with digital tags like TrackR and Tile tracking devices that utilize a network connection to enable tracking of individuals does not represent a feasible option for mass surveillance. This technology includes hardware that operates via GPS or Bluetooth (via crowd-sourced GPS dependant on nearby phone users running the corresponding app) requiring users to physically adhere the unit to each individual tracked subject. Similarly, commercially available tracking apps requires the user to physically access the phone of a tracked subject (or otherwise hack their phones) and install a geographical monitoring app. Since an investigator cannot use these tagging methods to track everyone, such technology can only provide marginal assistance to efforts at monitoring a limited number of subjects at best. Digital tags represent a largely impractical solution for mass surveillance due to the virtual absence of any benefit to crime scene reconstruction, the conspicuous violation of privacy laws inherent in most practical methods of installing this surveillance system, the infeasibility of either physically placing tracking devices on people unnoticed or accessing most subjects' phones, the related ease with which subjects can evade the monitoring, the absence of a comprehensive historical locational database, the manpower required to monitor subjects closely, and the cost of the hardware. Despite the inability of digital tags to provide a comprehensive solution to the challenge posed by digital mass surveillance, this technology can serve as a useful adjunct to a more comprehensive solution such as PerpTrac.

- Video Surveillance: Amidst a series of inadequate options for physical security mass surveillance of digital markers, video surveillance systems do provide a visual alternative that has greatly improved physical security since their mass deployment over the past forty years. Providing a reliable source

for information on people's physical behaviors and a valuable tool for identifying individuals, video footage does represent a surveillance option available to many civilians. Moreover, there exists no privacy violation for recording people in public areas, though recording audio (often times a critical adjunct to video's visual presentation of behaviors and identities) does legally require consent from property owners or the recorded party, and sometimes both, depending on local laws. Despite this capability to monitor and record physical behaviors without intruding on privacy rights in public, video surveillance does not provide a comprehensive solution for mass surveillance; there exists no such commercially available service and the interwoven locations of public and private properties presents a significant obstacle to seamless video surveillance across an wide area. Restrictions on a user's ability to access footage from several cameras outside of one's own property presents a severe obstacle to tracking individuals by camera. The expense of blanketing areas with sufficient cameras to eliminate significant blind spots in zone coverage and the highly limited range of coverage for most cameras in use today indicate that mass surveillance by video represents an expensive enterprise.

Compounding these shortcomings, subjects of surveillance can easily evade visual identification on camera by obscuring faces or license plates, only appearing during times of poor visibility such as nighttime or simply avoiding the limited number of camera surveillance zones by navigating through blind spots in the coverage. Even clear pictures of faces are useless unless someone involved in the investigation happens to know the person of interest (the rising potential of facial-recognition notwithstanding), and records of license plates only facilitate an investigation that can access the department of motor vehicles restricted archives. Aside from the limitations imposed by certain privacy considerations, the absence of a mass surveillance service, the price tag of video surveillance, and the ease with which subjects can evade tracking

and identification, video technology can serve as a useful adjunct to a more comprehensive solution for physical security surveillance.

- Private Investigators: Of all these alternatives in the industry of physical security surveillance, the PI business represents by far the most longstanding and reliable option. Capable of acquiring a broad range of detailed information on subjects through an array of methods, private investigators can monitor subjects who emit no digital signature virtually anywhere. However, the considerable expense of hiring a professional investigator to follow physically a subject in order to harvest information about their personal identity and behaviors represents an insurmountable cost to many. Moreover, the limits of the manpower of an individual PI and the PI industry as a whole prohibit this option as a viable solution for mass surveillance. Nevertheless, the PI business in its current form and in the model for crowd-sourcing the business proposed by PerpTrac offers the potential for PI's to serve as a highly useful adjunct to a more comprehensive solution to the challenge of physical security mass surveillance.

Unlike Stingrays, SS7 tracking services, cell-tower dumps, personal-data brokers, digital tags, video surveillance and private investigators, PerpTrac represents a comprehensive solution for physical-security mass surveillance immediately accessible to anyone at a minimal cost. Unlike these alternatives, PerpTrac does not represent a violation of privacy laws because there exists no reasonable expectation of privacy for UNencrypted radio transmissions of network beacon data and PerpTrac exclusively records these types of UNencrypted radio transmissions. Not requiring a warrant for access or geographical restrictions on the coverage zones of sensors, anyone can utilize the service to access comprehensive data for identifying individuals and tracking their precise movements anywhere. As an umbrella technology, PerpTrac does not exclude adjunct services but rather includes such services as SS7 access, digital tags used by private investigators, video surveillance and personal data broker archives. In addition to universal access, identification, tracking and incorporation of other useful technologies, PerpTrac features low costs to both operate and utilize, virtually unlimited range of coverage, unrivaled

locational precision, acquisition of several forms of raw data, a plethora of refined data, user-friendly presentations of this data, the capability to search by person or location, in-depth personal profiles, watchlist monitoring and advanced capabilities for crime scene reconstruction, ease of use, unrivaled manpower multiplication, the provision of evidence sufficient for the standards of a court of law, along with effective measures to combat evasion techniques that largely preclude elusion of this form of surveillance. The broad range of benefits of PerpTrac compared to other surveillance technologies suggests the revolutionary potential of this service.

Security experts have compared PerpTrac to the advent of the surveillance camera in terms of its potential wide-ranging impact on criminal investigations and deterrence of crime. Instead of dozens of $500 cameras to cover comprehensively a city block, a single $500 dedicated PerpTrac sensor can cover 1.5 square miles in a surveillance zone augmented by all of the activated smart phones in the area that have the app installed. Moreover, PerpTrac can positively identify and track subjects beyond the range of that single sensor, whereas surveillance cameras often cannot identify subjects of surveillance and users can rarely access video surveillance footage of the subject outside of that local video surveillance system's range. Even when compared to the leading technology in the general industry of physical security surveillance, PerpTrac represents a superior alternative. PerpTrac's market niche based on

- The scarcity of current competition
- The unlikelihood that the proposed database will encounter serious market competition
- The fact that the PerpTrac U.S. patent entitles the owner to intellectual property ownership of both the method and the specific system inside the United States and guarantees the owner market access to all countries

indicates that this patent bestows the owner with a legal proprietary claim that can enable that owner to dominate the entire multi-billion-dollar MOPS industry.

Profit Potential

The low cost, secure market niche and versatile uses of PerpTrac's patented surveillance method and system suggest a great potential for profitability for the licensed company that deploys this service. Including initial development and overhead costs, operational costs for this service will not exceed (or even be close to) $50 million per year. In a conservative estimate that excludes every country except the United States and posits that only about 1/30 of the population subscribes to the service for $9.99 per month, profits from these 10 million customers exceed $1 billion per year. An analogy to the Amazon Prime subscription model can provide a useful estimate of the potential for profits from subscription fees, particularly considering that PerpTrac offers far greater utility to the average citizen and society at large than the shipping benefits and auxiliary services provided by Amazon Prime.

The profits estimate soars from $1 billion to $10 billion or more per year when considering

- The market for this technology in every other country
- The realistic potential for far more than 10 million customers in the United States alone
- Sales of hardware like sensors and auxiliary services like the private-investigator outsourcing
- Advertisement revenue from allowing Amazon or a similar company access to the entire database for targeted advertising and link placement in the toolbar
- Contracts with federal governments, state governments and large corporations

The inception of profits from a relatively small customer base can help precipitate a snowballing of sales from these other sources. The central archive constitutes the focal point of a profitability positive feedback loop: the more data collected, the more useful and attractive the database becomes to consumers, advertisers and governments, inspiring

more subscribers which, in turn, proliferates more sensors that further expand the central archive. Once that database grows sufficiently comprehensive to provide a reliable record of past behaviors and prediction of future behaviors for virtually everyone in a nation's population, the prospect of large-scale contracts with governments and marketing agencies represents potentially the most profitable undertaking for this mass surveillance initiative.

8. IS THIS A PROVEN TECHNOLOGY?

The PerpTrac prototype successfully identified the home addresses of car thieves caught on camera in West Hartford, Connecticut in 2015 and 2017. While this technology represents an innovation in the field of physical security mass surveillance, the foundational technology for PerpTrac has existed as a bedrock of several industries for many years. Examples include GPS navigation and tracking, internet traffic routing, cyber-security, department-store marketing research, inventory management, mobile phones, cloud-based data storage, personal data brokers, and street traffic analysis. Google in particular has engineered many of its services on this cornerstone.

1. GPS Navigation: GPS-oriented visualizations of people's locations like Google Maps, Google Street View and Google Earth have become a technological cornerstone for modern transportation. Aside from accessing the U.S. Department of Defense's global positioning satellites, Google employs other forms of network beacons to enhance its geographical mapping services. Google's program for mapping Wi-Fi networks to improve locational accuracy for Google Maps currently functions by utilizing background services on Android phones to detect and record regularly all SSID's and MAC addresses within sensing proximity and then transmit this data to Google. In addition to the close similarity with PerpTrac's background scanning for all nearby mobile phones, this Google Wi-Fi mapping program produces an archive of hotspots that is similar to public databases of Wi-Fi sites that PerpTrac uses to cross-reference with a device's configured network list in order to deduce the owner's frequented locations. In addition to navigation, locational tracking of mobile devices as employed by Google Maps, Google's Find My Device service and digital tagging services like Tile and TrackR have empowered citizens, companies and governments alike with a powerful new tool to locate and follow people and objects.

2. Internet Routing and Cyber-Security: Radio-frequency beacon sensing and MAC-address recording exists to enable network traffic routing systems like Google's Wi-Fi mesh-router access points. Similar beacon monitoring assists cyber security services that record MAC addresses for MAC-address filtering to restrict network access to authorized users, as well as for the identification of hackers and their locational trails.

3. Marketing Research and Inventory Management: For years department stores have monitored mobile-phone beacons for marketing research on customer traffic flow and personal buying practices. This application has included services that involve video surveillance overlays. Similarly, warehouses have employed Bluetooth beacons for inventory management.

4. Mobile Phones: The hardware and software of smart-phone technology exists today as a ubiquitous presence facilitates the daily operations of modern society. In particular, smart phone apps and network interfaces figure centrally in this activity.

5. Cloud-Based Data Storage: Data storage like Google Drive has allowed an entirely new set of industries to flourish by utilizing the servers of other companies for management of data on a scale previously infeasible to most companies.

6. Personal-Data Brokers: Personal-data collection and analytics in vast databases have become a fixture of modern society. Most websites and apps now harvest a wide variety of forms of personal data on users for resale to personal-data brokers that, in turn, sell this valuable private information to marketing companies.

7. Street-Traffic Analysis: The recording and analysis of street traffic patterns through the detection of Bluetooth and Wi-Fi beacons has allowed local governments to gather valuable data on traffic flow patterns that can inform highway construction and other activities.

In the context of Google's prominent involvement in many of these technologies, Google has accumulated one of the largest and well known databases of GPS trails. Moreover, Google has world famous expertise in collecting, analyzing, organizing and visualizing vast amounts of just the sort of data that PerpTrac collects. Either Google or a similar technology company would profit greatly from repurposing existing technologies in order to harness a record of everyone's precise identifiable locational trail both for targeted advertising enhancement and the untapped purpose of a commercially available physical security surveillance service. By repurposing and expanding existing mobile internet technologies, PerpTrac utilizes proven technologies to create the new industry of mobile-phone-based physical-security mass surveillance.

9. WHAT ARE THE PRIVACY CONCERNS?

The PerpTrac surveillance sensors record only the unencrypted plaintext networking identifiers contained within the beacons regularly broadcasted by mobile phones. The recording includes a time-stamped geographical approximation of the site for each beacon's origin based on the quantifiable electromagnetic characteristics of the radio beacon detected by multiple sensors. **PerpTrac does not detect or record encrypted communications of any kind, nor does it detect or record unencrypted personal communications that may include phone calls, text messages, contacts, phone numbers or user-entered internet traffic.** In order to record the unencrypted networking beacon data, PerpTrac utilizes as the sensor grid dedicated radio-frequency detectors and smart phones containing the crowd-sourcing app. Located in public areas or in private areas with the consent of the property owners, these sensors do not engage in unauthorized physical intrusion on private property. In terms of this particular utilization of smart phones, PerpTrac emulates a standard default background process already performed by Android and iOS devices that constantly harvests exclusively the unconcealed networking beacon data and geographical approximations from nearby wireless devices.

Rather than collecting this valuable marketing data allegedly for the exclusive purpose of improving the geographical accuracy of locational services, as Google and Apple contend they do, PerpTrac harvests this data in order to amplify the long-established public service provided by the White Pages. In addition to a public listing of the home addresses of identified individuals, PerpTrac provides a public archive of their historical geographical trails along with the capability to identify and similarly discover the trails of unknown individuals who traverse a particular location during a designated time frame. This data accumulated about an individual reflects that which a private citizen or private investigator could collect by physically following the individual. As with so many other human endeavors, computers can accomplish on a massive scale tasks that manpower

alone can only achieve on a miniscule scale. PerpTrac's sensors simulate digital private investigators that take note of every mobile phone user's regularly broadcasted digital license plate along with its moment-to-moment location. The public mandate for augmented physical security mass surveillance today manifests in polls, such as a Washington Post poll in November 2013, that revealed only 14% of Americans want fewer surveillance cameras in public spaces.

Legal Basis

The PerpTrac surveillance service operates based on a solid legal foundation that abides by existing privacy laws and continues well-established societal precedents. PerpTrac does not detect or record any encrypted data, such as communications content or personal metadata. There exists no reasonable expectation of privacy for the unencrypted radio transmissions of network beacon data that PerpTrac does record, the only raw data collected by PerpTrac. Moreover, there exists no constitutional protection for information divulged to a third party under the Supreme Court's expectation of privacy test. Nor does the service violate stalking laws because, as is the case with a private investigator, there exists no intention to harm the subject of the surveillance. Personal-data acquisition conducted using legitimate methods constitutes a perfectly legal practice if it has a purpose or benefit to the person or group, such as the numerous benefits of PerpTrac described above. In order to help ensure proper usage of the surveillance service, PerpTrac's Abuse Complaints Department reviews subscriber-issued reports on potential misuse of the people-monitoring utility. Any subscriber or non-subscriber found to be utilizing the PerpTrac service for malicious purposes, especially in pursuit of a criminal enterprise, will face both permanent prohibition from access to the service and prosecution to the fullest extent of the law.

The practice of detecting and recording the unique identifying networking serial numbers of wireless devices constitutes an industry-standard requirement for internet technologies. These serial numbers ignore encryption (including device-embedded encryption, virtual private networks, app-generated end-to-end encryption and anonymous browsing) so they

appear in plaintext. The collection of unencrypted serial numbers, such as the media access control (MAC) address for Wi-Fi and Bluetooth network interfacing chips as well as the temporary mobile subscriber identity (TMSI) and international mobile equipment identity (IMEI) for cellular interfacing, represents an indispensable tool that allows a network to address data packets to individual devices. Cellular networks regularly record TMSI's as they monitor the locations and route data to devices. Several contemporary services collect MAC addresses, from public Wi-Fi routing systems to wireless intrusion detection systems to tracking devices. Phones constantly broadcast these identifying numbers and networks dutifully record them, even when a phone connects to a public or known Wi-Fi network without the knowledge of the user. Similarly, smart phones regularly intercept such packets of data from nearby wireless devices and relay that information to Google and Apple. No laws prevent the collection of these unencrypted serial numbers, and neither Google nor Apple have faced any significant legal challenges to this behavior.

There exists no likely scenario in which future privacy laws would change in order to prohibit the recording of these unencrypted broadcasts of networking serial numbers, considering the indispensability of this procedure to the proper operation of today's communications infrastructure. Regarding exclusively the utilizations of these recordings, courts and legislatures would likely address more intrusive and less socially beneficial collections of personal data before modifying laws to allow simultaneously these recordings but disallow their application to personal-data harvesting for PerpTrac's proposed public and private service of physical security surveillance. The prospect of such alterations in privacy laws appears remote in an age when Google and Apple collect much of the same type of valuable marketing data for uncertain purposes while most websites and apps harvest a wide variety of in-depth encrypted personal information on users for resale to predatory marketing agencies. Nevertheless, if any of these unlikely reevaluations of privacy laws does occur in the future, an international option can resolve this legal dilemma for the company licensed to sell the PerpTrac service. There exists no clear international legal standard and absolutely no law enforcement governing the tracking of people in other countries. Simply relocating the central database to another

country may provide a viable option if changing privacy laws interfere with PerpTrac operations in any given nation.

Unlike the placement of video cameras in private residences without the consent of the residents, the collection of the locational trails of identifiable phones within private residences represents an unreliable recording of personal information that inherently does not violate privacy laws applicable to these dwellings. With personal effects scattered across the domicile without concern about theft, the plethora of distractions inherent to home-life and multiple communications devices easily accessible, people do not reliably tether themselves to their mobile phones inside their homes to the extent that they do so outside of their homes. In light of these standard home-life habits, PerpTrac does not allow users to monitor reliably people's movements within private domiciles. Its inefficacy for this purpose precludes any serious potential for such a privacy breach. Moreover, the ability of phone users to turn off their own phones at home and recede from publicly accessible video surveillance further indicates that PerpTrac does not violate privacy rights by allowing subscribers to track subjects inside their domiciles. The capability to ascertain if a particular individual or anyone at all is present at a home represents an existing faculty that people can employ simply with a passing glance by looking for cars in a driveway or parking spot, or physically monitoring a residence. The general determination that a person is present at a private residence amounts to public information that people can currently obtain, so PerpTrac's ability to so inform users does not represent an unauthorized disclosure of personal information.

Some of the optional capabilities featured by the PerpTrac service constitute tools that the company licensed to sell the service may choose to incorporate or excise based on privacy considerations. These nonessential utilities include

- The assimilation of vast records of aerial video surveillance

- Personal-data profiles populated with a combination of PerpTrac data and publicly accessible personal information

- Interfaces with SS7 cellular location databases and third-party personal-data brokers

- The outsourced private investigator service that may additionally utilize digital-tag technologies and commercial drones

None of these utilities represent mandatory features of the PerpTrac service. Despite the remarkable potential for augmenting the mass surveillance service with these utilities, the unlikely potential for criminal legal challenges and the likelihood of a measure of civil legal challenges may dissuade the PerpTrac company from employing these well-established commercially available services after a careful assessment of the privacy implications of such potentially intrusive forms of mass surveillance.

Precedents

A host of common technologies, services and practices pervading modern society today constitute precedents justifying the deployment of the PerpTrac mass surveillance service.

The Privacy Practices of Google and Apple: The two companies that dominate the mobile phone market already collect much of the same beacon data surreptitiously and without accountability using a background service embedded in their operating systems. While they ostensibly perform this data harvesting for the purpose of improving geographical accuracy of locational services, this personal data adds to their already immense vaults of private information on owners and non-owners of their products alike. These vaults include personal information that Google and Apple aggressively collect through the recording of most encrypted data from phones and services by deceiving users into signing lengthy, complex privacy agreements composed of legal jargon and abstruse statements that even many professional contract lawyers have failed to comprehend. For example, Google reserves the right to access and record every email message of every Gmail user. This mass replication of encrypted personal data continues in the public spotlight despite any rational justification for the activity, and millions of users continue to sign up for Gmail accounts, and otherwise utilize Google and Apple products and services, either oblivious to or complacent in the widespread public knowledge of these "authorized" privacy intrusions.

Data Mining by Websites and Apps: Similar to the personal-data practices of Google and Apple but lacking the shroud of secrecy about their full range of motives, software design companies routinely harvest private data about the users of most websites and apps for resale to targeted advertisement companies without users knowledge, in most cases.

Video Surveillance: The history of video surveillance suggests a model for the public acceptance of mass surveillance: initial skepticism and backlash from privacy advocates disintegrates as the societal benefits for crime prevention, law enforcement and personal security become manifest and the technology spreads worldwide to government offices, streets, public gathering sites, businesses and homes. Modern populations calmly accept the fact that the government, a business or private citizen can and likely will make a permanent video record of anyone's physical appearance, behaviors, interactions and travels in any public area, as well as some private areas.

Private Investigators: Any citizen may legally hire a private detective to track and videotape the detailed public movements, behaviors and interactions of any other citizen, as long as they bear no malicious intent. Unfortunately, before PerpTrac the cost of such a service made this surveillance option prohibitively expensive for the average citizen, such that only the wealthy could monitor convicted or suspected criminals and loved ones in this manner. Similarly, paparazzi celebrity news reporters have always engaged in such activity without legal repercussions.

The Internet: The advent of the Internet signaled the dawn of a new age of crime as black markets for drugs, guns, bombs, poisons, the sex trade, and money laundering became accessible to everyone everywhere, while other criminal activities flourished such as

- Stalking
- Conspiracies to cripple a nation with national infrastructure sabotage
- The potential to derail entire businesses or governmental bodies by taking down a website

- Industrial and corporate sabotage

- Election rigging through the manipulation of voting machines and voter opinion

- The polarization of the electorate and government in response to a deluge of unvetted knowledge

- The proliferation of inaccurate fact claims left unchecked that create the basis for disinformation campaigns by corporate and political entities against proven scientific theories and laws

- The ability of corporate propaganda to mislead the general public in covert service of large-scale mass murder

- Malicious propaganda operations including the spread of ideologies inciting violence

- The proliferation of criminal tradecraft based on previously restricted engineering knowledge including bomb making, creating plastic guns from 3D printers and nuclear weapons designs

- The spread of international terrorist movements

- Confidence scams such as phishing, spearphishing, and other solicitations based on personal information acquired online

- Fraudulent claims submissions, like tax and medical claims

- Theft of encrypted personal information

- Ransomware

- The theft of corporate secrets, intellectual property and state secrets

The 2009 release and consequent global proliferation of the Stuxnet Mod malware by the Netanyahu Israeli government as part of its efforts to intensify cyberwarfare on the Iranian nuclear program has triggered the dawn of a far more dangerous internet era posing an increasingly existential threat to entire nation states. Nevertheless, the countless benefits of the internet have persuaded the general public of this invention's utility such that there exists no significant public support for dismantling the internet.

The Edward Snowden Revelations: Since 9/11 many federal governments have partnered with the telecomm industry to engage in mass surveillance of encrypted mobile phone data and other internet traffic in an unsubstantiated effort to prevent terrorist attacks. The national security wings of many federal governments already have the capability to monitor most encrypted communications. The utilization of stolen phones, burner phones, impenetrable messaging apps, traditional face-to-face communications and phone-less traveling has nevertheless allowed criminals to conceal their identities, physical movements, behaviors and interactions from federal investigators. Nevertheless, this warrantless electronic mass surveillance continues unabated, even years after Edward Snowden revealed some of its extent to the global community. While providing little additional data on law-abiding citizens to the federal government, PerpTrac does provide it with the capability to combat these evasion techniques employed by many criminals. Simultaneously, PerpTrac provides a wealth of useful knowledge on people's behaviors to all investigators, as well as citizens who cannot receive protection from limited local police departments, who lack access to such top-secret shadow databases and yet require this capability to monitor and investigate criminal suspects.

> The White Pages: The public listing of the home addresses and phone numbers of virtually the entire adult population exists as a long-practiced public service that faces no significant legal challenge over its potential to violate privacy rights.

Both the method and the purpose of PerpTrac's personal-data collection policy continue the traditions established by a plethora of societal precedents that include the privacy practices of Google and Apple, general data mining by websites and apps, video surveillance, private investigators, the Internet, the Edward Snowden revelations, and the White Pages. Beyond the societal precedent, a persuasive legal foundation protecting both the collection of unencrypted networking beacon data and personal-data collection services that provide critical societal benefits justifies PerpTrac's privacy policy and shields the service from significant legal challenges.

Further Reading on Privacy Concerns

https://s3.amazonaws.com/s3.documentcloud.org/documents/1100394/google-v-joffe.pdf

https://en.m.wikipedia.org/wiki/Pen_register

https://en.n.wikipedia.org/wiki/Electronic_Communications_Privacy_Act

10. REFERENCES

1. Clifford, Stephanie. "Attention, Shoppers: Store Is Tracking Your Cell." *The New York Times*, 14 July 2013.

2. Fung, Brian. "How Stores Use Your Phone's Wi-Fi To Track Your Shopping Habits." *The Washington Post*, 19 October 2013.

3. Tanner, Adam. "Here's How Others Can Easily Snoop On Your Cell Phone." *Forbes*, 18 February 2014.

4. Chevalier, Ally. "Cell Phone Tracking With The Power Off." *Brighthub.com*, 30 September 2009.

5. "Mobile Phone Tracking." *Wikipedia*.

6. "IMSI Trackers and Mobile Security" available at https://www.cis.upenn.edu/current-students/undergraduate/courses/documents/EAS499Honors-IMSICatchersandMobileSecurity-V18F-1.pdf

7. "Footpath Beta Test" available at http://repository.up.ac.za/bitstream/handle/2263/19770/Hermant_Use(2012).pdf

8. "Google Web Mapping Can Track Your Phone", CNET

9. http://eff.org/deeplinks/2015/10/6-spooky-ways-local-law-enforcement-watching-you

10. "Cell Phone Data Spying: It's Not Just the NSA", USA Today, 12/8/13

11. "Where've You Been: Your Smart Phone's Wi-Fi Is Telling Everyone" by Sean Gallagher, *ArsTechnica*, 11/5/14.

12. "Shielding MAC Addresses From Stalkers Is Hard and Android Fails Miserably At It" by Dan Goodwin, *ArsTechnica*, 3/23/17.

13. "How Often Does a Cell Phone Ping the Towers" at *quora.com*

14. "The Problem With Mobile Phones" from *Surveillance Self-Defense* available at http://ssd.eff.org/en/module/problem-mobile-phones

15. “For Sale: Systems That Can Secretly Track Where Cell-Phone Users Go Around the World” by Craig Timberg, *Washington Post.*

16. “New Surveillance Technology Can Track Everyone in an Area for Several Hours at a Time” by Craig Timberg, *Washington Post,* 2/5/14.

17. “Betrayed By Our Own Data” by Von Kai Biermann, *Zeit Online*, 3/10/11.

* GREENLINE ANALYTICS

http://greenlineanalytics.com/

Statistical Consulting, Data Analysis, and Software Development

Contact us at

cbaldwin@greenlineanalytics.com

OUR TEAM

CAREY BALDWIN

Chief Executive Officer

Statistical Analyst, Software Engineer

JOHN H. MALONE, ESQ.

Chief Legal Adviser

Board Certified Criminal Trial Attorney

2016 Connecticut Prosecutor of the Year

https://ccjeca.org/employee-awards

Career Retrospective

www.bristolpress.com/BP-General+News/305043/john-malone-lawyer-for-40-years-retires

> Malone's methodical approach to trying cases has served the state well over the years, **said Chief's State's Attorney Kevin Kane**, the only member of the division who has served longer. "John's steady, reliable, dedicated, and hardworking," Kane said. "He's a role model for other prosecutors. He's thorough in case preparation and analysis. He's always willing to take on hard cases and do as much work as it takes to do it well."