9. WHAT ARE THE PRIVACY CONCERNS?

The TrailTracker 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. **TrailTracker 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, TrailTracker 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, TrailTracker 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, TrailTracker 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, TrailTracker 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. TrailTracker'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 TrailTracker surveillance service operates based on a solid legal foundation that abides by existing privacy laws and continues well-established societal precedents. TrailTracker 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 TrailTracker does record, the only raw data collected by TrailTracker. 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 TrailTracker described above. In order to help ensure proper usage of the surveillance service, TrailTracker'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 TrailTracker 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 TrailTracker'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 TrailTracker 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 TrailTracker 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, TrailTracker 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 TrailTracker 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 TrailTracker's ability to so inform users does not represent an unauthorized disclosure of personal information.

Some of the optional capabilities featured by the TrailTracker 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 TrailTracker 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 TrailTracker 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 TrailTracker 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 TrailTracker 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 TrailTracker 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, TrailTracker does provide it with the capability to combat these evasion techniques employed by many criminals. Simultaneously, TrailTracker 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 TrailTracker'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 TrailTracker'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