The New York Times has just published an opinion piece, *"One Nation, Tracked – An investigation in the smartphone tracking industry"* that is likely to raise questions.

I'd like to provide some context and provide Babbage's thoughts on what it means overall, to our industry and to Alexander Babbage's products; TruTrade and PinPoint, powered by Alexander Babbage. In addition to the overview below, if you'd like to discuss further please contact me directly.

Article Background:
The article is titled *"Twelve Million Phones, One Dataset, Zero Privacy"* by Stuart Thompson and Charlie Warzel of The Times Privacy Project. They obtained a data set of pings from 12 million mobile devices over several months in 2016 and 2017 covering 50 billion location pings.

The article has some beautiful data visualizations, for example an image of where phones were seen inside and around The Pentagon. The source of the data is described as apps running on smartphones that are transmitting their location with a unique device ID. This data is described as being sold and re-sold in a largely unregulated industry. The article ends by calling for Congress to *"step in to protect Americans' needs as consumers and rights as citizens."*

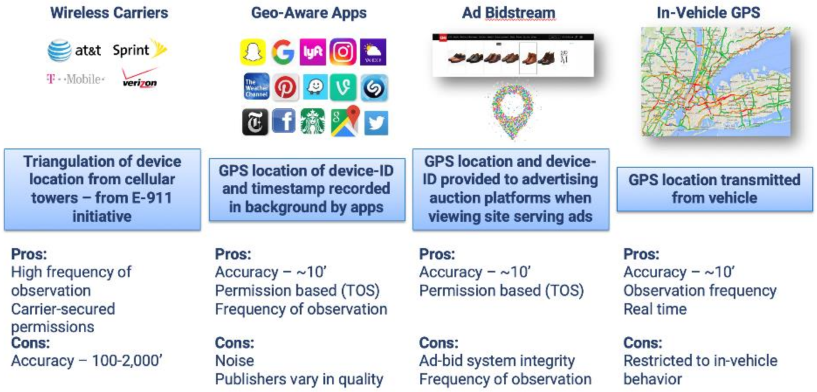
My thoughts:
Overall, the article is an accurate reporting of how data is collected, protected and analyzed. It glosses over where the consumer receives a benefit from sharing their data, and hence why we expect to continue to see data being shared. In addition to more targeted ads – a debatable benefit – consumers get a better user experience from having the weather, or the restaurant reservation app, or their Uber driver know where they are at that moment in time. Imagine opening a weather app and having to put in your ZIP or street address to get the weather when you're traveling. Consumers also get free services, such as weather, that have to be monetized somehow. Consumers accept advertising rather than pay for an app. Many consumers – especially younger consumers – also accept that their data is being monetized to provide the services they use regularly – for example, Facebook, Instagram, Google Maps etc.

The mere existence of the data doesn't make it as easy to track an individual as the article implies. Yes, the data can be purchased from different vendors, but there are several barriers to visualizing and using it in the ways described. None of these are overwhelming, but it is very unlikely that an individual is going to be able to source the data and, for example, stalk their ex with this type of data because:

1. The data is licensed under contract, typically between companies and the contracts have language restricting access, identification of an individual, resale, etc.
2. The data sets are expensive – 6 and 7-figure license fees are the norm for a full data set that could achieve what the article describes.
3. The data volume is massive and unwieldy – for TruTrade we receive over 40Gb of compressed data per day. Finding an individual device requires processing petabytes of data (a petabyte is approximately a million gigabytes). This requires significant technical infrastructure (e.g. AWS), technical expertise (e.g. programmers and software stacks)

and processing power (e.g. configuring and running clusters of multiple machines in the cloud) to store and analyze the data. It's not like searching an Excel spreadsheet for your ex's name and there's no publicly available simple Google-like search of device locations.

4. The data from apps is typically historic, not real-time. There are different sources of location data – ad bidstream, mobile carriers, in-car navigation – that are real-time, but each has other issues.



Wireless Carriers	Geo-Aware Apps	Ad Bidstream	In-Vehicle GPS
Triangulation of device location from cellular towers – from E-911 initiative	GPS location of device-ID and timestamp recorded in background by apps	GPS location and device-ID provided to advertising auction platforms when viewing site serving ads	GPS location transmitted from vehicle
Pros: High frequency of observation Carrier-secured permissions	**Pros:** Accuracy – ~10' Permission based (TOS) Frequency of observation	**Pros:** Accuracy – ~10' Permission based (TOS)	**Pros:** Accuracy – ~10' Observation frequency Real time
Cons: Accuracy – 100-2,000'	**Cons:** Noise Publishers vary in quality	**Cons:** Ad-bid system integrity Frequency of observation	**Cons:** Restricted to in-vehicle behavior

Source: Alexander Babbage

Surveillance technology is all around us – your mobile phone is just one way in which your behaviors are being tracked and sold. From your credit score, your home energy usage, your response rate to catalog mailings, your click behavior and your requests to Alexa, the advent of cheap storage and processing power means that almost everything you do is tracked, stored, analyzed and resold. Of the list above, only credit score is regulated – and even in this highly regulated area, there are synthetic proxies for credit score that provide a similar piece of information that gets around the regulations.

It seems very difficult to put the genie back in the bottle. The simple call for *"Congress should do something"* shows, in my opinion, a lack of understanding of the complexity of our society and how interwoven technology is into our lives. The authors acknowledge that fact – *"Until then, one thing is certain: We are living in the world's most advanced surveillance system."*

What are the implications for TruTrade and PinPoint powered by Alexander Babbage?

There will be regulation, but it will have limited impact on the collection and use of the data. The California Consumer Privacy Act (CCPA) will take effect on January 1, 2020. The California Attorney General will issue regulations on or before July 1, 2020 and will not bring any enforcement actions July 1, 2020 or shortly before. On personal information and geolocation data, CCPA is similar to the European privacy directive known as GDPR that went into effect in May 2018, so we can look to the implementation of GDPR to guide how CCPA might impact.

State regulators are more likely to lead the way than the Federal government.
If California continues to lead the way, then the needs of their largest tech companies will be integrated into the legislation. The entire digital advertising industry relies on geo-location and Personally Identifiable Information (PII). Many other industries and technology companies are built on this data.

Lack of understanding of technology and fear of unintended consequences will impact any legislative discussion. Pair this with the fact that Alphabet, Facebook, Microsoft and Amazon are some of the largest spenders on lobbying in Washington and we should expect any proposals to be modified to ensure the continued ability to collect and monetize personal information. Our lawyers, Trusted Counsel, have an excellent white paper on the impact of CCPA if you want to learn more.

Companies are not monoliths – for example grocery stores that recognize you when you approach and pull your order are reliant on a myriad of technologies, contractors and third parties for the service to work. These companies are collecting and passing information that previously would have been siloed and more easily regulated.

Informed Consent will guide implementation
The US focus is on consumer rights and informed consent. If a consumer chooses to share their data with a provider, and gives their permission for it to be sold, then it can be. In practice this manifests itself in nag screens in the user interface asking consumers to give permission to share their location data and linking out to terms and conditions if they do so. These have become more friendly and written in plain English, but still most consumers click "Agree" quickly to get to the app. In Europe, websites have implemented "Agree" buttons to comply with GDPR, but little else has changed.

Users must have the right to find out what data is collected on them, and the right to opt-out. Babbage has already taken action with our data partners to ensure compliance with CCPA. We are watching closely for any trend shifts in the data we see, but with a panel of 120M devices and data going back to January 2017, we have a very robust sample to analyze and trend from.

It's scary, but we've yet to find the harm
The Times article is interesting, and in some ways alarming – but it has failed to identify a single case where a consumer has been harmed or discriminated against because their data was available. Even the security threats suggested such as who is in the Pentagon and finding their families is just using location data to replicate other means, e.g. identifying, following and spying on Pentagon employees using a human.

The genie is already out of the bottle
With an estimated 230M smartphones in use in the US, an average of nine apps being used daily and 80 different apps on the phone it is unlikely that even a major uptick in people turning off location services will impact every app or reduce the volume of data materially.

At Babbage, we are very focused on the productive use of data to improve our client's businesses. We won't allow you to use the data to identify an individual (a few have asked), we will only report aggregated and anonymized data. We are working closely with our legal counsel and our data partners to ensure we continue to have the largest, most accurate and compliant dataset in the industry.

This is a complex topic and I encourage you to explore it in detail. I welcome any questions or thoughts you have.

Alan McKeon – President & CEO, Alexander Babbage