American Phone-Tracking Firm Demo’d Surveillance Powers by Spying on CIA and NSA

Sam Biddle, Jack Poulson ⋮ 20-26 minutes ⋮ 4/22/2022

In the months leading up to Russia’s invasion of Ukraine, two obscure American startups met to discuss a potential surveillance partnership that would merge the ability to track the movements of billions of people via their phones with a constant stream of data purchased directly from Twitter. According to Brendon Clark of Anomaly Six — or “A6” — the combination of its cellphone location-tracking technology with the social media surveillance provided by Zignal Labs would permit the U.S. government to effortlessly spy on Russian forces as they amassed along the Ukrainian border, or similarly track Chinese nuclear submarines. To prove that the technology worked, Clark pointed A6’s powers inward, spying on the National Security Agency and CIA, using their own cellphones against them.

Virginia-based Anomaly Six was founded in 2018 by two ex-military intelligence officers and maintains a public presence that is scant to the point of mysterious, its website disclosing nothing about what the firm actually does. But there’s a good chance that A6 knows an immense amount about you. The company is one of many that purchases vast reams of location data, tracking hundreds of millions of people around the world by exploiting a poorly understood fact: Countless common smartphone apps are constantly harvesting your location and relaying it to advertisers, typically without your knowledge or informed consent, relying on disclosures buried in the legalese of the sprawling terms of service that the companies involved count on you never reading. Once your location is beamed to an advertiser, there is currently no law in the United States prohibiting the further sale and resale of that information to firms like Anomaly Six, which are free to sell it to their private sector and governmental clientele. For anyone interested in tracking the daily lives of others, the digital advertising industry is taking care of the grunt work day in and day out — all a third party need do is buy access.

Company materials obtained by The Intercept and Tech Inquiry provide new details of just how powerful Anomaly Six’s globe-spanning surveillance powers are, capable of providing any paying customer with abilities previously reserved for spy bureaus and militaries.

According to audiovisual recordings of an A6 presentation reviewed by The Intercept and Tech Inquiry, the firm claims that it can track roughly 3 billion devices in real time, equivalent to a fifth of the world’s population. The staggering surveillance capacity was cited during a pitch to provide A6’s phone-tracking capabilities to Zignal Labs, a social media monitoring firm that leverages its access to Twitter’s rarely granted “firehose” data stream to sift through hundreds of millions of tweets per day without restriction. With their powers combined, A6 proposed, Zignal’s corporate and governmental clients could not only surveil global social media activity, but also determine who exactly sent certain tweets, where they sent them from, who they were with, where they’d been previously, and where they went next. This enormously augmented capability would be an obvious boon to both regimes keeping tabs on their global adversaries and companies keeping tabs on their employees.

The source of the materials, who spoke on the condition of anonymity to protect their livelihood, expressed grave concern about the legality of government contractors such as Anomaly Six and Zignal Labs “revealing social posts, usernames, and locations of Americans” to “Defense Department” users. The source also asserted that Zignal Labs had willfully deceived Twitter by withholding the broader military and corporate surveillance use cases of its firehose access. Twitter’s terms of service technically prohibit a third party from “conducting or providing surveillance or gathering intelligence” using its access to the platform, though the practice is common and enforcement of this ban is rare. Asked about these concerns, spokesperson Tom Korolsyshun told The Intercept “Zignal abides by privacy laws and guidelines set forth by our data partners.”

A6 claims that its GPS dragnet yields between 30 to 60 location pings per device per day and 2.5 trillion locational data points annually worldwide, adding up to 280 terabytes of location data per year and many petabytes in total, suggesting that the company surveils roughly 230 million devices on an average day. A6’s salesperson added that while many rival firms gather personal location data via a phone’s Bluetooth and Wi-Fi connections that provide general whereabouts, Anomaly 6 harvests only GPS pinpoints, potentially accurate to within several feet. In addition to location, A6 claimed that it has built a library of over 2 billion email addresses and other personal details that people share when signing up for smartphone apps that can be used to identify who the GPS ping belongs to. All of this is powered, A6’s Clark noted during the pitch, by general ignorance of the ubiquity and invasiveness of smartphone software development kits, known as SDKs: "Everything is agreed to and sent by the user even though they probably don't read the 60 pages in the [end user license agreement]."

The Intercept was not able to corroborate Anomaly Six's claims about its data or capabilities, which were made in the context of a sales pitch. Privacy researcher Zach Edwards told The Intercept that he believed the claims were plausible but cautioned that firms can be prone to exaggerating the quality of their data. Mobile security researcher Will Strafach agreed, noting that A6's data sourcing boasts "sound alarming but aren't terribly far off from ambitious claims by others." According to Wolfie Christl, a researcher specializing in the surveillance and privacy implications of the app data industry, even if Anomaly Six's capabilities are exaggerated or based partly on inaccurate data, a company possessing even a fraction of these spy powers would be deeply concerning from a personal privacy standpoint.

Reached for comment, Zignal's spokesperson provided the following statement: "While Anomaly 6 has in the past demonstrated its capabilities to Zignal Labs, Zignal Labs does not have a relationship with Anomaly 6. We have never integrated Anomaly 6's capabilities into our platform, nor have we ever delivered Anomaly 6 to any of our customers."

When asked about the company's presentation and its surveillance capabilities, Anomaly Six co-founder Brendan Huff responded in an email that "Anomaly Six is a veteran-owned small business that cares about American interests, natural security, and understands the law."

Companies like A6 are fueled by the ubiquity of SDKs, which are turnkey packages of code that software-makers can slip in their apps to easily add functionality and quickly monetize their offerings with ads. According to Clark, A6 can siphon exact GPS measurements gathered through covert partnerships with "thousands" of smartphone apps, an approach he described in his presentation as a "farm-to-table approach to data acquisition." This data isn't just useful for people hoping to sell you things: The largely unregulated global trade in personal data is increasingly finding customers not only at marketing agencies, but also federal agencies tracking immigrants and drone targets as well as sanctions and tax evasion. According to public records first reported by Motherboard, U.S. Special Operations Command paid Anomaly Six $590,000 in September 2020 for a year of access to the firm's "commercial telemetry feed."

Anomaly Six software lets its customers browse all of this data in a convenient and intuitive Google Maps-style satellite view of Earth. Users need only find a location of interest and draw a box around it, and A6 fills that boundary with dots denoting smartphones that passed through that area. Clicking a dot will provide you with lines representing the device's — and its owner's — movements around a neighborhood, city, or indeed the entire world.

As the Russian military continued its buildup along the country's border with Ukraine, the A6 sales rep detailed how GPS surveillance could help turn Zignal into a sort of private spy agency capable of assisting state clientele in monitoring troop movements. Imagine, Clark explained, if the crisis zone tweets Zignal rapidly surfaces through the firehose were only a starting point. Using satellite imagery tweeted by accounts conducting increasingly popular "open-source intelligence," or OSINT, investigations, Clark showed how A6's GPS tracking would let Zignal clients determine not simply that the military buildup was taking place, but track the phones of Russian soldiers as they mobilized to determine exactly where they'd trained, where they were stationed, and which units they belonged to. In one case, Clark showed A6 software tracing Russian troop phones backward through time, away from the border and back to a military installation outside Yurga, and suggested that they could be traced further, all the way back to their individual homes. Previous reporting by the Wall Street Journal indicates that this phone-tracking method is already used to monitor Russian military maneuvers and that American troops are just as vulnerable.

In another A6 map demonstration, Clark zoomed in closely on the town of Molkino, in southern Russia, where the Wagner Group, an infamous Russian mercenary outfit, is reportedly headquartered. The map showed dozens of dots indicating devices at the Wagner base, along with scattered lines showing their recent movements. "So you can just start watching these devices," Clark explained. "Any time they start leaving the area, I'm looking at potential Russian predeployment activity for their nonstandard actors, their nonuniform people. So if you see them go into Libya or Democratic Republic of the Congo or things like that, that can help you better understand potential soft power actions the Russians are doing."

> To fully impress upon its audience the immense power of this software, Anomaly Six did what few in the world can claim to do: spied on American spies.

The pitch noted that this kind of mass phone surveillance could be used by Zignal to aid unspecified clients with “counter-messaging,” debunking Russian claims that such military buildups were mere training exercises and not the runup to an invasion. “When you’re looking at counter-messaging, where you guys have a huge part of the value you provide your client in the counter-messaging piece is — [Russia is] saying, ‘Oh, it’s just local, regional, um, exercises.’ Like, no. We can see from the data that they’re coming from all over Russia.”

To fully impress upon its audience the immense power of this software, Anomaly Six did what few in the world can claim to do: spied on American spies. “I like making fun of our own people,” Clark began. Pulling up a Google Maps-like satellite view, the sales rep showed the NSA’s headquarters in Fort Meade, Maryland, and the CIA’s headquarters in Langley, Virginia. With virtual boundary boxes drawn around both, a technique known as geofencing, A6’s software revealed an incredible intelligence bounty: 183 dots representing phones that had visited both agencies potentially belonging to American intelligence personnel, with hundreds of lines streaking outward revealing their movements, ready to track throughout the world. “So, if I’m a foreign intel officer, that’s 183 start points for me now,” Clark noted.

The NSA and CIA both declined to comment.

Anomaly Six tracked a device that had visited the NSA and CIA headquarters to an air base outside of Zarqa, Jordan.

Screenshot: The Intercept / Google Maps

Clicking on one of dots from the NSA allowed Clark to follow that individual’s exact movements, virtually every moment of their life, from that previous year until the present. “I mean, just think of fun things like sourcing,” Clark said. “If I’m a foreign intel officer, I don’t have access to things like the agency or the fort, I can find where those people live, I can find where they travel, I can see when they leave the country.” The demonstration then tracked the individual around the United States and abroad to a training center and airfield roughly an hour’s drive northwest of Muwaffaq Salti Air Base in Zarqa, Jordan, where the U.S. reportedly maintains a fleet of drones.

> “It doesn’t take a lot of creativity to see how foreign spies can use this information for espionage, blackmail, all kinds of, as they used to say, dastardly deeds.”

“There is sure as hell a serious national security threat if a data broker can track a couple hundred intelligence officials to their homes and around the world,” Sen. Ron Wyden, D-Ore., a vocal critic of the personal data industry, told The Intercept in an interview. “It doesn’t take a lot of creativity to see how foreign spies can use this information for espionage, blackmail, all kinds of, as they used to say, dastardly deeds.”

Back stateside, the person was tracked to their own home. A6’s software includes a function called “Regularity,” a button clients can press that automatically analyzes frequently visited locations to deduce where a target lives and works, even though the GPS pinpoints sourced by A6 omit the phone owner's name. Privacy researchers have long shown that even "anonymized" location data is trivially easy to attach to an individual based on where they frequent most, a fact borne out by A6's own demonstration. After hitting the "Regularity" button, Clark zoomed in on a Google Street View image of their home.

"Industry has repeatedly claimed that collecting and selling this cellphone location data won't violate privacy because it is tied to device ID numbers instead of people's names. This feature proves just how facile those claims are," said Nate Wessler, deputy director of the American Civil Liberties Union's Speech, Privacy, and Technology Project. "Of course, following a person's movements 24 hours a day, day after day, will tell you where they live, where they work, who they spend time with, and who they are. The privacy violation is immense."

The demo continued with a surveillance exercise tagging U.S. naval movements, using a tweeted satellite photo of the USS Dwight D. Eisenhower in the Mediterranean Sea snapped by the commercial firm Maxar Technologies. Clark broke down how a single satellite snapshot could be turned into surveillance that he claimed was even more powerful than that executed from space. Using the latitude and longitude coordinates appended to the Maxar photo along with its time stamp, A6 was able to pick up a single phone signal from the ship's position at that moment, south of Crete. "But it only takes one," Clark noted. "So when I look back where that one device goes: Oh, it goes back to Norfolk. And actually, on the carrier in the satellite picture — what else is on the carrier? When you look, here are all the other devices." His screen revealed a view of the carrier docked in Virginia, teeming with thousands of colorful dots representing phone location pings gathered by A6. "Well, now I can see every time that that ship is deploying. I don't need satellites right now. I can use this."

Though Clark conceded that the company has far less data available on Chinese phone owners, the demo concluded with a GPS ping picked up aboard an alleged Chinese nuclear submarine. Using only unclassified satellite imagery and commercial advertising data, Anomaly Six was able to track the precise movements of the world's most sophisticated military and intelligence forces. With tools like those sold by A6 and Zignal, even an OSINT hobbyist would have global surveillance powers previously held only by nations. "People put way too much on social media," Clark added with a laugh.

As location data has proliferated largely unchecked by government oversight in the United States, one hand washes another, creating a private sector capable of state-level surveillance powers that can also fuel the state's own growing appetite for surveillance without the usual judicial scrutiny. Critics say the loose trade in advertising data constitutes a loophole in the Fourth Amendment, which requires the government to make its case to a judge before obtaining location coordinates from a cellular provider. But the total commodification of phone data has made it possible for the government to skip the court order and simply buy data that's often even more accurate than what could be provided by the likes of Verizon. Civil libertarians say this leaves a dangerous gap between the protections intended by the Constitution and the law's grasp on the modern data trade.

"The Supreme Court has made clear that cellphone location information is protected under the Fourth Amendment because of the detailed picture of a person's life it can reveal," explained Wessler. "Government agencies' purchases of access to Americans' sensitive location data raise serious questions about whether they are engaged in an illegal end run around the Fourth Amendment's warrant requirement. It is time for Congress to end the legal uncertainty enabling this surveillance once and for all by moving toward passage of the Fourth Amendment Is Not For Sale Act."

Though such legislation could restrict the government's ability to piggyback off commercial surveillance, app-makers and data brokers would remain free to surveil phone owners. Still, Wyden, a co-sponsor of that bill, told The Intercept that he believes "this legislation sends a very strong message" to the "Wild West" of ad-based surveillance but that clamping down on the location data supply chain would be "certainly a question for the future." Wyden suggested that protecting a device's location trail from snooping apps and advertisers might be best handled by the Federal Trade Commission. Separate legislation previously introduced by Wyden would empower the FTC to crack down on promiscuous data sharing and broaden consumers' ability to opt out of ad tracking.

A6 is far from the only firm engaged in privatized device-tracking surveillance. Three of Anomaly Six's key employees previously worked at competing firm Babel Street, which named all three of them in a 2018 lawsuit first reported by the Wall Street Journal. According to the legal filing, Brendan Huff and Jeffrey Heinz co-founded Anomaly Six (and lesser-known Datalus 5) months after ending their employment at Babel Street in April 2018, with the intent of replicating Babel's cellphone location surveillance product, "Locate X," in a partnership with major Babel competitor Semantic AI. In July 2018, Clark followed Huff and Heinz by resigning from his position as Babel’s “primary interface to … intelligence community clients” and becoming an employee of both Anomaly Six and Semantic.

Like its rival Dataminr, Zignal touts its mundane partnerships with the likes of Levi’s and the Sacramento Kings, marketing itself publicly in vague terms that carry little indication that it uses Twitter for intelligence-gathering purposes, ostensibly in clear violation of Twitter’s anti-surveillance policy. Zignal’s ties to government run deep: Zignal’s advisory board includes a former head of the U.S. Army Special Operations Command, Charles Cleveland, as well as the CEO of the Rendon Group, John Rendon, whose bio notes that he “pioneered the use of strategic communications and real-time information management as an element of national power, serving as a consultant to the White House, U.S. National Security community, including the U.S. Department of Defense.” Further, public records state that Zignal was paid roughly $4 million to subcontract under defense staffing firm ECS Federal on Project Maven for “Publicly Available Information … Data Aggregation” and a related “Publicly Available Information enclave” in the U.S. Army’s Secure Unclassified Network.

The remarkable world-spanning capabilities of Anomaly Six are representative of the quantum leap occurring in the field of OSINT. While the term is often used to describe the internet-enabled detective work that draws on public records to, say, pinpoint the location of a war crime from a grainy video clip, “automated OSINT” systems now use software to combine enormous datasets that far outpace what a human could do on their own. Automated OSINT has also become something of a misnomer, using information that is by no means “open source” or in the public domain, like commercial GPS data that must be bought from a private broker.

While OSINT techniques are powerful, they are generally shielded from accusations of privacy violation because the “open source” nature of the underlying information means that it was already to some extent public. This is a defense that Anomaly Six, with its trove of billions of purchased data points, can’t muster. In February, the Dutch Review Committee on the Intelligence and Security Services issued a report on automated OSINT techniques and the threat to personal privacy they may represent: “The volume, nature and range of personal data in these automated OSINT tools may lead to a more serious violation of fundamental rights, in particular the right to privacy, than consulting data from publicly accessible online information sources, such as publicly accessible social media data or data retrieved using a generic search engine.” This fusion of publicly available data, privately procured personal records, and computerized analysis isn’t the future of governmental surveillance, but the present. Last year, the New York Times reported that the Defense Intelligence Agency “buys commercially available databases containing location data from smartphone apps and searches it for Americans’ past movements without a warrant,” a surveillance method now regularly practiced throughout the Pentagon, the Department of Homeland Security, the IRS, and beyond.