BYRON TAU BACKCHANNEL FEB 27, 2024 6:00 AM

How the Pentagon Learned to Use Targeted Ads to Find Its Targets—and Vladimir Putin

Meet the guy who taught US intelligence agencies how to make the most of the ad tech ecosystem, "the largest information-gathering enterprise ever conceived by man."

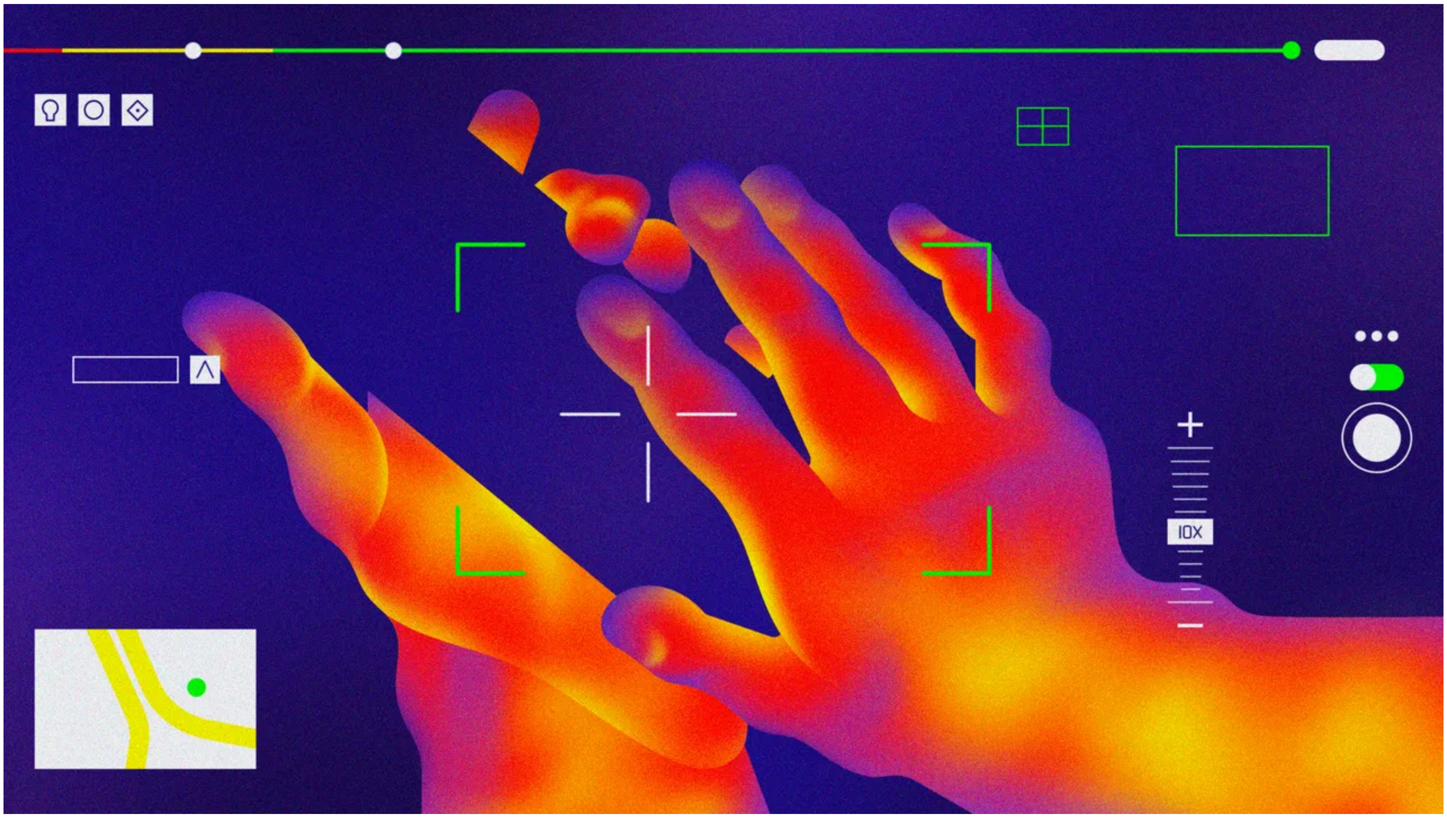
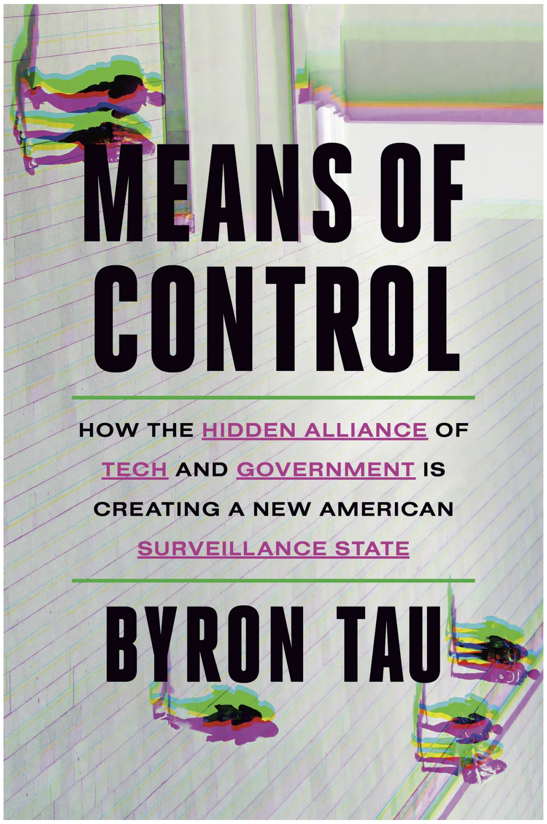


ILLUSTRATION: ZHENYA OLIINYK

SAVE

IN 2019, A government contractor and technologist named Mike Yeagley began making the rounds in Washington, DC. He had a blunt warning for anyone in the country's national security establishment who would listen: The US government had a Grindr problem.

A popular dating and hookup app, Grindr relied on the GPS capabilities of modern smartphones to connect potential partners in the same city, neighborhood, or even building. The app can show how far away a potential partner is in real time, down to the foot.


MEANS OF CONTROL
HOW THE HIDDEN ALLIANCE OF TECH AND GOVERNMENT IS CREATING A NEW AMERICAN SURVEILLANCE STATE
BYRON TAU

COURTESY OF PENGUIN RANDOM HOUSE

In its 10 years of operation, Grindr had amassed millions of users and become a central cog in gay culture around the globe.

But to Yeagley, Grindr was something else: one of the tens of thousands of carelessly designed mobile phone apps that leaked massive amounts of data into the opaque world of online advertisers. That data, Yeagley knew, was easily accessible by anyone with a little technical know-how. So Yeagley—a technology consultant then in his late forties who had worked in and around government projects nearly his entire career—made a PowerPoint presentation and went out to demonstrate precisely how that data was a serious national security risk.

As he would explain in a succession of bland government conference rooms, Yeagley was able to access the geolocation data on Grindr users through a hidden but ubiquitous entry point: the digital advertising exchanges that serve up the little digital banner ads along the top of Grindr and nearly every other ad-supported mobile app and website. This was possible because of the way online ad space is sold, through near-instantaneous auctions in a process called real-time bidding. Those auctions were rife with surveillance potential. You know that ad that seems to follow you around the internet? It's tracking you in more ways than one. In some cases, it's making your precise location available in near-real time to both advertisers and people like Mike Yeagley, who specialized in obtaining unique data sets for government agencies.

Working with Grindr data, Yeagley began drawing geofences—creating virtual boundaries in geographical data sets—around buildings belonging to government agencies that do national security work. That allowed Yeagley to see what phones were in certain buildings at certain times, and where they went afterwards. He was looking for phones belonging to Grindr users who spent their daytime hours at government office buildings. If the device spent most workdays at the Pentagon, the FBI headquarters, or the National Geospatial-Intelligence Agency building at Fort Belvoir, for example, there was a good chance its owner worked for one of those agencies. Then he started looking at the movement of those phones through the Grindr data. When they weren't at their offices, where did they go? A small number of them had lingered at highway rest stops in the DC area at the same time and in proximity to other Grindr users—sometimes during the workday and sometimes while in transit between government facilities. For other Grindr users, he could infer where they lived, see where they traveled, even guess at whom they were dating.

Intelligence agencies have a long and unfortunate history of trying to root out LGBTQ Americans from their workforce, but this wasn't Yeagley's intent. He didn't want anyone to get in trouble. No disciplinary actions were taken against any employee of the federal government based on Yeagley's presentation. His aim was to show that buried in the seemingly innocuous technical data that comes off every cell phone in the world is a rich story—one that people might prefer to keep quiet. Or at the very least, not broadcast to the whole world. And that each of these intelligence and national security agencies had employees who were recklessly, if obliviously, broadcasting intimate details of their lives to anyone who knew where to look.

As Yeagley showed, all that information was available for sale, for cheap. And it wasn't just Grindr, but rather any app that had access to a user's precise location—other dating apps, weather apps, games. Yeagley chose Grindr because it happened to generate a particularly rich set of data and its user base might be uniquely vulnerable. A Chinese company had obtained a majority stake in Grindr beginning in 2016—amping up fears among Yeagley and others in Washington that the data could be misused by a geopolitical foe. (Until 1995, gay men and women were banned from having security clearances owing in part to a belief among government counterintelligence agents that their identities might make them vulnerable to being leveraged by an adversary—a belief that persists today.)

But Yeagley's point in these sessions wasn't just to argue that advertising data presented a threat to the security of the United States and the privacy of its citizens. It was to demonstrate that these sources also presented an enormous opportunity in the right hands, used for the right purpose. When speaking to a bunch of intelligence agencies, there's no way to get their attention quite like showing them a tool capable of revealing when their agents are visiting highway rest stops.

MIKE YEAGLEY SAW both the promise and the pitfalls of advertising data because he'd played a key role in bringing advertising data into government in the first place. His 2019 road show was an attempt to spread awareness across the diverse and often siloed workforces in US intelligence. But by then, a few select corners of the intel world were already very familiar with his work, and were actively making use of it.

Yeagley had spent years working as a technology "scout"—looking for capabilities or data sets that existed in the private sector and helping to bring them into government. He'd helped pioneer a technique that some of its practitioners would jokingly come to call "ADINT"—a play on the intelligence community's jargon for different sources of intelligence, like the SIGINT (signals intelligence) that became synonymous with the rise of codebreaking and tapped phone lines in the 20th century, and the OSINT (open source intelligence) of the internet era, of which ADINT was a form. More often, though, ADINT was known in government circles as adtech data.

Adtech uses the basic lifeblood of digital commerce—the trail of data that comes off nearly all mobile phones—to deliver valuable intelligence information. Edward

Snowden's 2013 leaks showed that, for a time, spy agencies could get data from digital advertisers by tapping fiber-optic cables or internet choke points. But in the post-Snowden world, more and more traffic like that was being encrypted; no longer could the National Security Agency pull data from advertisers by eavesdropping. So it was a revelation—especially given the public outcry over Snowden's leaks—that agencies could just *buy* some of the data they needed straight from commercial entities. One technology consultant who works on projects for the US government explained it this way to me: "The advertising technology ecosystem is the largest information-gathering enterprise ever conceived by man. And it wasn't built by the government."

Everyone who possesses an iPhone or Android phone has been given an "anonymized" advertising ID by Apple or Google. That number is used to track our real-world movement, our internet browsing behavior, the apps we put on our phone, and much more. Billions of dollars have been poured into this system by America's largest corporations. Faced with a commercially available repository of data this rich and detailed, the world's governments have increasingly opened up their wallets to buy up this information on everyone, rather than hacking it or getting it through secret court orders.

Here's how it works. Imagine a woman named Marcela. She has a Google Pixel phone with the Weather Channel app installed. As she heads out the door to go on a jog, she sees overcast skies. So Marcela opens the app to check if the forecast calls for rain.

By clicking on the Weather Channel's blue icon, Marcela triggers a frenzy of digital activity aimed at serving her a personalized ad. It begins with an entity called an advertising exchange, basically a massive marketplace where billions of mobile devices and computers notify a centralized server whenever they have an open ad space.

In less than the blink of an eye, the Weather Channel app shares a ream of data with this ad exchange, including the IP address of Marcela's phone, the version of Android it's running, her carrier, plus an array of technical data about how the phone is configured, down to what resolution the screen resolution is set to. Most valuable of all, the app shares the precise GPS coordinates of Marcela's phone and the pseudonymized advertising ID number that Google has assigned to her, called an AAID. (On Apple devices, it's called an IDFA.)

To the layperson, an advertising ID is a string of gibberish, something like bdca712j-fb3c-33ad-2324-0794d394m912. To advertisers, it's a gold mine. They know that bdca712j-fb3c-33ad-2324-0794d394m912 owns a Google Pixel device with the Nike Run Club app. They know that bdca712j-fb3c-33ad-2324-0794d394m912 often frequents Runnersworld.com. And they know that bdca712j-fb3c-33ad-2324-0794d394m912 has been lusting after a pair of new Vaporfly racing shoes. They know this because Nike, Runnersworld.com, and Google are all plugged into the same advertising ecosystem, all aimed at understanding what consumers are interested in.

Advertisers use that information as they shape and deploy their ads. Say both Nike and Brooks, another running shoe brand, are trying to reach female running aficionados in a certain income bracket or in certain zip codes. Based on the huge amounts of data they can pull from the ether, they might build an "audience"—essentially a huge list of ad IDs of customers known or suspected to be in the market for running shoes. Then in an instantaneous, automated, real-time auction, advertisers tell a digital ad exchange how much they're willing to pay to reach those consumers every time they load an app or a web page.

There are some limits and safeguards on all this data. Technically, a user can reset their assigned advertising ID number (though few people do so—or even know they have one). And users do have some control over what they share, via their app settings. If consumers don't allow the app they're using to access GPS, the ad exchange can't pull the phone's GPS location, for example. (Or at least they aren't supposed to. Not all apps follow the rules, and they are sometimes not properly vetted once they are in app stores.)

Moreover, ad exchange bidding platforms do minimal due diligence on the hundreds or even thousands of entities that have a presence on their servers. So even the losing bidders still have access to all the consumer data that came off the phone during the bid request. An entire business model has been built on this: siphoning data off the real-time bidding networks, packaging it up, and reselling it to help businesses understand consumer behavior.

Geolocation is the single most valuable piece of commercial data to come off those devices. Understanding the movement of phones is now a multibillion-dollar industry. It can be used to deliver targeted advertising based on location for, say, a restaurant chain that wants to deliver targeted ads to people nearby. It can be used to measure consumer behavior and the effectiveness of advertising. How many people saw an ad and later visited a store? And the analytics can be used for planning and investment decisions. Where is the best location to put a new store? Will there be enough foot traffic to sustain such a business? Is the number of people visiting a certain retailer going up or down this month, and what does that mean for the retailer's stock price?

But this kind of data is good for something else. It has remarkable surveillance potential. Why? Because what we do in the world with our devices cannot truly be anonymized. The fact that advertisers know Marcela as bdca712j-fb3c-33ad-2324-0794d394m912 as they're watching her move around the online and offline worlds offers her almost no privacy protection. Taken together, her habits and routines are unique to her. Our real-world movement is highly specific and personal to all of us. For many years, I lived in a small 13-unit walk-up in Washington, DC. I was the only person waking up every morning at that address and going to *The Wall Street Journal*'s offices. Even if I was just an anonymized number, my behavior was as unique as a fingerprint even in a sea of hundreds of millions of others. There was no way to anonymize my identity in a data set like geolocation. Where a phone spends most of its evenings is a good proxy for where its owner lives. Advertisers know this.

Governments know this too. And Yeagley was part of a team that would try to find out how they could exploit it.

IN 2015, A company called PlaceIQ hired Yeagley. PlaceIQ was an early mover in the location data market. Back in the mid-2000s, its founder, Duncan McCall, had participated in an overland driving race from London to Gambia across the land-mine-strewn Western Sahara. He had eschewed the usual practice of hiring an expensive Bedouin guide to help ensure safe passage through the area. Instead, he found online a GPS route that someone else had posted from a few days earlier on a message board. McCall was able to download the route, load it into his own GPS device, and follow the same safe path. On that drive through the Western Sahara, McCall recalled dreaming up the idea for what would become PlaceIQ to capture all of the geospatial data that consumers were emitting and generate insights. At first the company used data from the photo-sharing website Flickr, but eventually PlaceIQ started tapping mobile ad exchanges. It would be the start of a new business model—one that would prove highly successful.

Yeagley was hired after PlaceIQ got an investment from the CIA's venture capital arm, In-Q-Tel. Just as it had poured money into numerous social media monitoring services, geospatial data had also attracted In-Q-Tel's interest. The CIA was interested in software that could analyze and understand the geographic movement of people and things. It wanted to be able to decipher when, say, two people were trying to conceal that they were traveling together. The CIA had planned to use the software with its own proprietary data, but government agencies of all kinds eventually became interested in the kind of raw data that commercial entities like PlaceIQ had—it was available through a straightforward commercial transaction and came with fewer restrictions on use inside government than secret intercepts.

> After acquiring a data set on Russia, the team realized they could track phones in the Russian president Vladimir Putin's entourage. The phones moved everywhere that Putin did.

While working there, Yeagley realized that the data itself might be valuable to the government, too. PlaceIQ was fine selling software to the government but was not prepared to sell its data to the feds. So Yeagley approached a different company called PlanetRisk—one of the hundreds and hundreds of tiny startups with ties to the US government dotted around office parks in Northern Virginia. In theory, a government defense contractor offered a more secure environment than a civilian company like PlaceIQ to do the kind of work he had in mind.

PlanetRisk straddled the corporate world and the government contracting space—building products that were aimed at helping customers understand the relative dangers of various spots around the world. For example, a company that wanted to establish a store or an office somewhere in the world might turn to PlanetRisk to analyze data on crime, civil unrest, and extreme weather as they vary geographically.

PlanetRisk hired Yeagley in 2016 as vice president of global defense—essentially a sales and business development job. The aim was for him to develop his adtech technology inside the contractor, which might try to sell it to various government agencies. Yeagley brought with him some government funding from his relationships around town in the defense and intelligence research communities.

PlanetRisk's earliest sales demo was about Syria: quantifying the crush of refugees flowing out of Syria after years of civil war and the advancing ISIS forces. From a commercial data broker called UberMedia, PlanetRisk had obtained location data on Aleppo—the besieged Syrian city that had been at the center of some of the fiercest fighting between government forces and US-backed rebels. It was an experiment in understanding what was possible. Could you even obtain location information on mobile phones in Syria? Surely a war zone was no hot spot for mobile advertising.

But to the company's surprise, the answer was yes. There were 168,786 mobile devices present in the city of Aleppo in UberMedia's data set, which measured mobile phone movements during the month of December 2015. And from that data, they could see the movement of refugees around the world.

The discovery that there was extensive data in Syria was a watershed. No longer was advertising merely a way to sell products; it was a way to peer into the habits and routines of billions. "Mobile devices are the lifeline for everyone, even refugees," Yeagley said.

PlanetRisk had sampled data from a range of location brokers—Cuebiq, X-Mode, SafeGraph, PlaceIQ, and Gravy Analytics—before settling on UberMedia. (The company has no relation to the rideshare app Uber.) UberMedia was started by the veteran advertising and technology executive Bill Gross, who had helped invent keyword-targeted ads—the kinds of ads that appear on Google when you search a specific term. UberMedia had started out as an advertising company that helped brands reach customers on Twitter. But over time, like many other companies in this space, UberMedia realized that it could do more than just target consumers with advertising. With access to several ad exchanges, it could save bid requests that contained geolocation information, and then it could sell that data. Now, this was technically against the rules of most ad exchanges, but there was little way to police the practice. At its peak, UberMedia was collecting about 200,000 bid requests per second on mobile devices around the world.

Just as UberMedia was operating in a bit of a gray zone, PlanetRisk had likewise not been entirely forthright with UberMedia. To get the Aleppo data, Yeagley told UberMedia that he needed the data as part of PlanetRisk's work with a humanitarian organization—when in fact the client was a defense contractor doing research work funded by the Pentagon. (UberMedia's CEO would later learn the truth about what Mike Yeagley wanted the data for. And others in the company had their own suspicions. "Humanitarian purposes" was a line met with a wink and nod around the company among employees who knew or suspected what was going on with Yeagley's data contracts.) Either way, UberMedia wasn't vetting its customers closely. It appeared to be more eager to make a sale than it was concerned about the privacy implications of selling the movement patterns of millions of people.

When it came time to produce a demo of PlanetRisk's commercial phone-tracking product, Yeagley's 10-year-old daughter helped him come up with a name. They called the program Locomotive—a portmanteau of *location* and *motive*. The total cost to build out a small demo was about $600,000, put up entirely by a couple of Pentagon research funding arms. As the PlanetRisk team put Locomotive through the paces and dug into the data, they found one interesting story after another.

In one instance they could see a device moving back and forth between Syria and the West—a potential concern given ISIS's interest in recruiting Westerners, training them, and sending them back to carry out terrorist attacks. But as the PlanetRisk team took a closer look, the pattern of the device's behavior indicated that it likely belonged to a humanitarian aid worker. They could track that person's device to UN facilities and a refugee camp, unlikely locales for Islamic State fighters to hang out.

They realized they could track world leaders through Locomotive, too. After acquiring a data set on Russia, the team realized they could track phones in the Russian president Vladimir Putin's entourage. The phones moved everywhere that

Putin did. They concluded the devices in question did not actually belong to Putin himself; Russian state security and counterintelligence were better than that. Instead, they believed the devices belonged to the drivers, the security personnel, the political aides, and other support staff around the Russian president; those people's phones were trackable in the advertising data. As a result, PlanetRisk knew where Putin was going and who was in his entourage.

There were other oddities. In one data set, they found one phone kept transiting between the United States and North Korea. The device would attend a Korean church in the United States on Sundays. Its owner appeared to work at a GE factory, a prominent American corporation with significant intellectual property and technology that a regime like Pyongyang would be interested in. Why was it traveling back and forth between the United States and North Korea, not exactly known as a tourist destination? PlanetRisk considered raising the issue with either the US intelligence agencies or the company but ultimately decided there wasn't much they could do. And they didn't necessarily want their phone-tracking tool to be widely known. They never got to the bottom of it.

Most alarmingly, PlanetRisk began seeing evidence of the US military's own missions in the Locomotive data. Phones would appear at American military installations such as Fort Bragg in North Carolina and MacDill Air Force Base in Tampa, Florida—home of some of the most skilled US special operators with the Joint Special Operations Command and other US Special Operations Command units. They would then transit through third-party countries like Turkey and Canada before eventually arriving in northern Syria, where they were clustering at the abandoned Lafarge cement factory outside the town of Kobane.

It dawned on the PlanetRisk team that these were US special operators converging at an unannounced military facility. Months later, their suspicions would be publicly confirmed; eventually the US government would acknowledge the facility was a forward operating base for personnel deployed in the anti-ISIS campaign.

Even worse, through Locomotive, they were getting data in pretty close to real time. UberMedia's data was usually updated every 24 hours or so. But sometimes, they saw movement that had occurred as recently as 15 or 30 minutes earlier. Here were some of the best-trained special operations units in the world, operating at an unannounced base. Yet their precise, shifting coordinates were showing up in UberMedia's advertising data. While Locomotive was a closely held project meant for government use, UberMedia's data was available for purchase by anyone who could come up with a plausible excuse. It wouldn't be difficult for the Chinese or Russian government to get this kind of data by setting up a shell company with a cover story, just as Mike Yeagley had done.

> If you ever granted a weather app permission to know where you are, there is a good chance a log of your precise movements has been saved in some data bank that tens of thousands of total strangers have access to. That includes intelligence agencies.

Initially, PlanetRisk was sampling data country by country, but it didn't take long for the team to wonder what it would cost to buy the entire world. The sales rep at UberMedia provided the answer: For a few hundred thousand dollars a month, the company would provide a global feed of every phone on earth that the company could collect on. The economics were impressive. For the military and intelligence community, a few hundred thousand a month was essentially a rounding error—in 2020, the intelligence budget was $62.7 billion. Here was a powerful intelligence tool for peanuts.

Locomotive, the first version of which was coded in 2016, blew away Pentagon brass. One government official demanded midway through the demo that the rest of it be conducted inside a SCIF, a secure government facility where classified information could be discussed. The official didn't understand how or what PlanetRisk was doing but assumed it must be a secret. A PlanetRisk employee at the briefing was mystified. "We were like, well, this is just stuff we've seen commercially," they recall. "We just licensed the data." After all, how could marketing data be classified?

Government officials were so enthralled by the capability that PlanetRisk was asked to keep Locomotive quiet. It wouldn't be classified, but the company would be asked to tightly control word of the capability to give the military time to take advantage of public ignorance of this kind of data and turn it into an operational surveillance program.

And the same executive remembered leaving another meeting with a different government official. They were on the elevator together when one official asked, could you figure out who is cheating on their spouse?

Yeah, I guess you could, the PlanetRisk executive answered.

BUT MIKE YEAGLEY wouldn't last at PlanetRisk.

As the company looked to turn Locomotive from a demo into a live product, Yeagley started to believe that his employer was taking the wrong approach. It was looking to build a data visualization platform for the government. Yet again, Yeagley thought it would be better to provide the raw data to the government and let them visualize it in any way they choose. Rather than make money off of the number of users inside government that buy a software license, Mike Yeagley wanted to just sell the government the data for a flat fee.

So Yeagley and PlanetRisk parted ways. He took his business relationship with UberMedia with him. PlanetRisk moved on to other lines of work and was eventually sold off in pieces to other defense contractors. Yeagley would land at a company called Aelius Exploitation Technologies, where he would go about trying to turn Locomotive into an actual government program for the Joint Special Operations Command—the terrorist-hunting elite special operations force that killed Osama bin Laden and Ayman Al Zarqawi and spent the past few years dismantling ISIS.

Locomotive was renamed VISR, which stood for Virtual Intelligence, Surveillance, and Reconnaissance. It would be used as part of an interagency program and would be shared widely inside the US intelligence community as a tool to generate leads.

By the time Yeagley went out to warn various security agencies about Grindr in 2019, VISR had been used domestically, too—at least for a short period of time when the FBI wanted to test its usefulness in domestic criminal cases. (In 2018, the FBI backed out of the program.) The Defense Intelligence Agency, another agency that had access to the VISR data, has also acknowledged that it used the tool on five separate occasions to look inside the United States as part of intelligence-related investigations.

But VISR, by now, is only one product among others that sell adtech data to intelligence agencies. The Department of Homeland Security has been a particularly enthusiastic adopter of this kind of data. Three of its components—US Customs and Border Protection, US Immigration and Customs Enforcement, and the US Secret Service —have bought more than 200 licenses from commercial ad tech vendors since 2019. They would use this data for finding border tunnels, tracking down unauthorized immigrants, and trying to solve domestic crimes. In 2023, a government inspector general chastised DHS over the use of adtech, saying that the department did not have adequate privacy safeguards in place and recommending that the data stop being used until policies were drawn. The DHS told the inspector general that they would continue to use the data. Adtech "is an important mission contributor to the ICE investigative process as, in combination with other information and investigative methods, it can fill knowledge gaps and produce investigative leads that might otherwise remain hidden," the agency wrote in response.

Other governments' intelligence agencies have access to this data as well. Several Israeli companies—Insanet, Patternz, and Rayzone—have built similar tools to VISR and sell it to national security and public safety entities around the world, according to reports. Rayzone has even developed the capability to deliver malware through targeted ads, according to *Haaretz*.

Which is to say, none of this is an abstract concern—even if you're just a private citizen. I'm here to tell you if you've ever been on a dating app that wanted your location or if you ever granted a weather app permission to know where you are 24/7, there is a good chance a detailed log of your precise movement patterns has been vacuumed up and saved in some data bank somewhere that tens of thousands of total strangers have access to. That includes intelligence agencies. It includes foreign governments. It includes private investigators. It even includes nosy journalists. (In 2021, a small conservative Catholic blog named *The Pillar* reported that Jeffrey Burrill, the secretary general of the US Conference of Catholic Bishops, was a regular user of Grindr. The publication reported that Burrill "visited gay bars and private residences while using a location-based hookup app" and described its source as "commercially available records of app signal data obtained by *The Pillar*.")

If you cheated on your spouse in the past few years and you were careless about your location data settings, there is a good chance there is evidence of that in data that is available for purchase. If you checked yourself into an inpatient drug rehab, that data is probably sitting in a data bank somewhere. If you told your boss you took a sick day and interviewed at a rival company, that could be in there. If you threw a brick through a storefront window during the George Floyd protests, well, your cell phone might link you to that bit of vandalism. And if you once had a few pints before causing a car crash and drove off without calling the police, data telling that story likely still exists somewhere.

We all have a vague sense that our cell phone carriers have this data about us. But law enforcement generally needs to go get a court order to get that. And it takes evidence of a crime to get such an order. This is a different kind of privacy nightmare.

I once met a disgruntled former employee of a company that competed against UberMedia and PlaceIQ. He had absconded with several gigabytes of data from his former company. It was only a small sampling of data, but it represented the comprehensive movements of tens of thousands of people for a few weeks. Lots of those people could be traced back to a residential address with a great deal of confidence. He offered me the data so I could see how invasive and powerful it was.

What can I do with this—hypothetically? I asked. In theory, could you help me draw geofences around mental hospitals? Abortion clinics? Could you look at phones that checked into a motel midday and stayed for less than two hours?

Easily, he answered.

I never went down that road.

Adapted from Means of Control: How the Hidden Alliance of Tech and Government Is Creating a New American Surveillance State, *by Byron Tau, to be published February 27, 2024, by Crown, an imprint of the Crown Publishing Group, a division of Penguin Random House LLC; Copyright © 2024 by Panopticon Project LLC.*

If you buy something using links in our stories, we may earn a commission. This helps support our journalism. Learn more.

You Might Also Like …

- 📩 Get the long view on tech with Steven Levy's Plaintext newsletter
- "Over time the trust will come": an exclusive interview with TikTok's CEO
- I stopped using passwords. It's great—and a total mess
- Inside the beef industry's campaign to influence kids
- Meet the pranksters behind Goody-2, the world's "most responsible" AI chatbot
- Is there lead in your reusable water bottle?
- 🌲 Our Gear team has branched out with a new guide to the best sleeping pads and fresh picks for the best coolers and binoculars

Byron Tau is a Washington, D.C.-based reporter and the author of the book *Means of Control: How the Hidden Alliance of Tech and Government Is Creating a New American Surveillance State*

TOPICS BOOK EXCERPT LONGREADS

SPIES, SECRECY AND SURVEILLANCE DEPARTMENT OF DEFENSE

MORE FROM WIRED

The One Internet Hack That Could Save Everything

It’s so simple: Axe 26 words from the Communications Decency Act. Welcome to a world without Section 230.

JARON LANIER

‘Over Time the Trust Will Come’: An Exclusive Interview With TikTok’s CEO

A few weeks ago, Shou Zi Chew sat down with WIRED to tell us how he’s trying to make TikTok better. Is the company’s CEO for real—or just a really good politician?

DEXTER THOMAS

2054, Part IV: A Nation Divided

“The people are in the streets. We can’t ignore them any longer. Really, we have little choice. Either we heal together, or we tear ourselves apart.” An exclusive excerpt from *2054: A Novel.*

ELLIOT ACKERMAN

Give Me Propaganda or Give Me Death

When Russia went to war, I faced a choice: Flee to a world where the truth might kill me—or seek peace in censored oblivion.

VADIM SMYSLOV

Nvidia Hardware Is Eating the World

Tech companies can’t get enough of this tech company. Earnings are off the charts. WIRED probes the mind of its CEO, Jensen Huang.

LAUREN GOODE

2054, Part V: From Tokyo With Love

“Had this all been contrived? Had his life become a game in which everyone knew the rules but him?” An exclusive excerpt from *2054: A Novel.*

ELLIOT ACKERMAN

The World’s Most Important Industry Has a New Captain—and She’s Piloting It Into the 21st Century

Meet Marina Hadjipateras: Greek shipping heiress, successful venture capitalist, and the woman trying to transform the $14 trillion shipping industry.

VIRGINIA HEFFERNAN