SHADOWDRAGON: INSIDE THE SOCIAL MEDIA SURVEILLANCE SOFTWARE THAT CAN WATCH YOUR EVERY MOVE

The tool is the product of a growing industry whose work is usually kept from the public and utilized by police.

Michael Kwet

September 21 2021, 5:03 p.m.

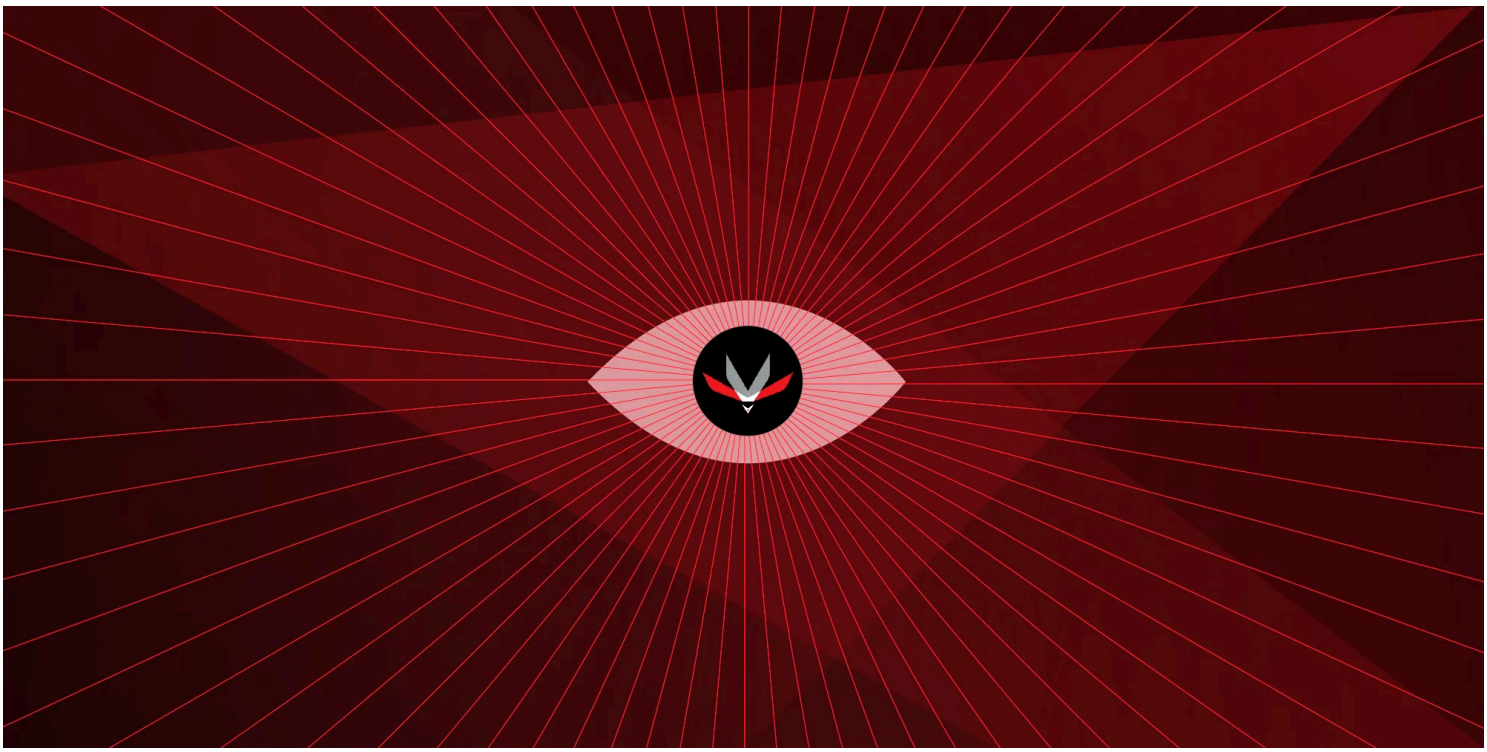


Illustration: The Intercept

A MICHIGAN STATE POLICE CONTRACT, obtained by The Intercept, sheds new light on the growing use of little-known surveillance software that helps law enforcement agencies and corporations watch people's social media and other website activity.

The software, put out by a Wyoming company called ShadowDragon, allows police to suck in data from social media and other internet sources, including Amazon, dating apps, and the dark web, so they can identify persons of interest and map out their networks during investigations. By providing powerful searches of more than 120 different online platforms and a decade's worth of archives, the company claims to speed up profiling work from months to minutes. ShadowDragon even claims its software can automatically adjust its monitoring and help predict violence and unrest. Michigan police acquired the software through a contract with another obscure online policing company named Kaseware for an "MSP Enterprise Criminal Intelligence System."

The inner workings of the product are generally not known to the public. The contract, and materials published by the companies online, allow a deeper explanation of how this surveillance works, provided below.

ShadowDragon has kept a low profile but has law enforcement customers well beyond Michigan. It was purchased twice by the U.S. Immigration and Customs Enforcement agency in the last two years, documents show, and was reportedly acquired by the Massachusetts State Police and other police departments within the state.

Michigan officials appear to be keeping their contract and the identities of ShadowDragon and Microsoft from the public. The Michigan.gov website does not make the contract available; it instead offers an email address at which to request the document "due to the sensitive nature of this contract." And the contract it eventually provides has been

heavily redacted: The copy given to David Goldberg, a professor at Wayne State University in Detroit had all mentions of ShadowDragon software and Microsoft Azure blacked out. What's more, Goldberg had to file a Freedom of Information Act request to obtain the contract. When the state website did offer the contract, it was unredacted, and I downloaded it before it was withdrawn.

Last year, The Intercept published several articles detailing how a social media analytics firm called Dataminr relayed tweets about the George Floyd and Black Lives Matter protests to police. The same year, I detailed at The Intercept how Kaseware's partner Microsoft helps police surveil and patrol communities through its own offerings and a network of partnerships.

This new revelation about the Michigan contract raises questions about what digital surveillance capabilities other police departments and law enforcement agencies in the U.S. might be quietly acquiring. And it comes at a time when previously known government social media surveillance is under fire from civil rights and liberties advocates like MediaJustice and the American Civil Liberties Union. It also raises the specter of further abuses in Michigan, where the FBI has been profiling Muslim communities and so-called Black Identity Extremists. In 2015, it was revealed that for years, the state police agency was using cell site simulators to spy on mobile phones without disclosing it to the public.

"They endanger Black and marginalized communities."

"Social media surveillance technologies, such as the software acquired by Michigan State Police, are often introduced under the false premise that they are public safety and accountability tools. In reality, they endanger Black and marginalized

communities," Arisha Hatch, vice president and chief of campaigns at civil rights nonprofit Color of Change, wrote in an email.

Michigan State Police spokesperson Shanon Banner said in an email that "the investigative tools available to us as part of this contract are only used in conjunction with criminal investigations, following all state and federal laws." The founder of ShadowDragon, Daniel Clemens, wrote that the company provides only information that is publicly available and does not "build products with predictive capabilities."

A Shadowy Industry

Kaseware and ShadowDragon are part of a shadowy industry of software firms that exploit what they call "open source intelligence," or OSINT: the trails of information that people leave on the internet. Clients include intelligence agencies, government, police, corporations, and even schools.

Kaseware, which is partnered to ShadowDragon and Microsoft, provides a platform for activities that support OSINT and other elements of digital policing, like data storage, management, and analysis. Its capabilities range from storing evidence to predictive policing. By contrast, the two ShadowDragon products acquired by the Michigan State Police are more narrowly tailored for the surveillance of people using social media, apps, and websites on the internet. They run on the Kaseware platform.

To understand how Kaseware and ShadowDragon work together, let us consider each in turn, starting with ShadowDragon.

Screenshot: The Intercept

ShadowDragon: Social Media Surveillance

The Michigan State Police purchased two of ShadowDragon's OSINT intelligence tools to run on the Kaseware platform: SocialNet and OIMonitor.

SocialNet was invented by cybersecurity consulting firm Packet Ninjas in 2009. Clemens, Packet Ninja's founder and CEO, went on to start ShadowDragon as a sister company in 2016, licensing the cyber intelligence and investigative tools developed by Packet Ninjas over the prior decade.

At the time of SocialNet's creation, investigators were left to search social media networks for clues manually. If a person made a public post on Twitter or Facebook, for example, an investigator was free to look online, but they had to personally log onto and search one social

network at a time, post by post, for people who might be suspects and for their friends and other associates.

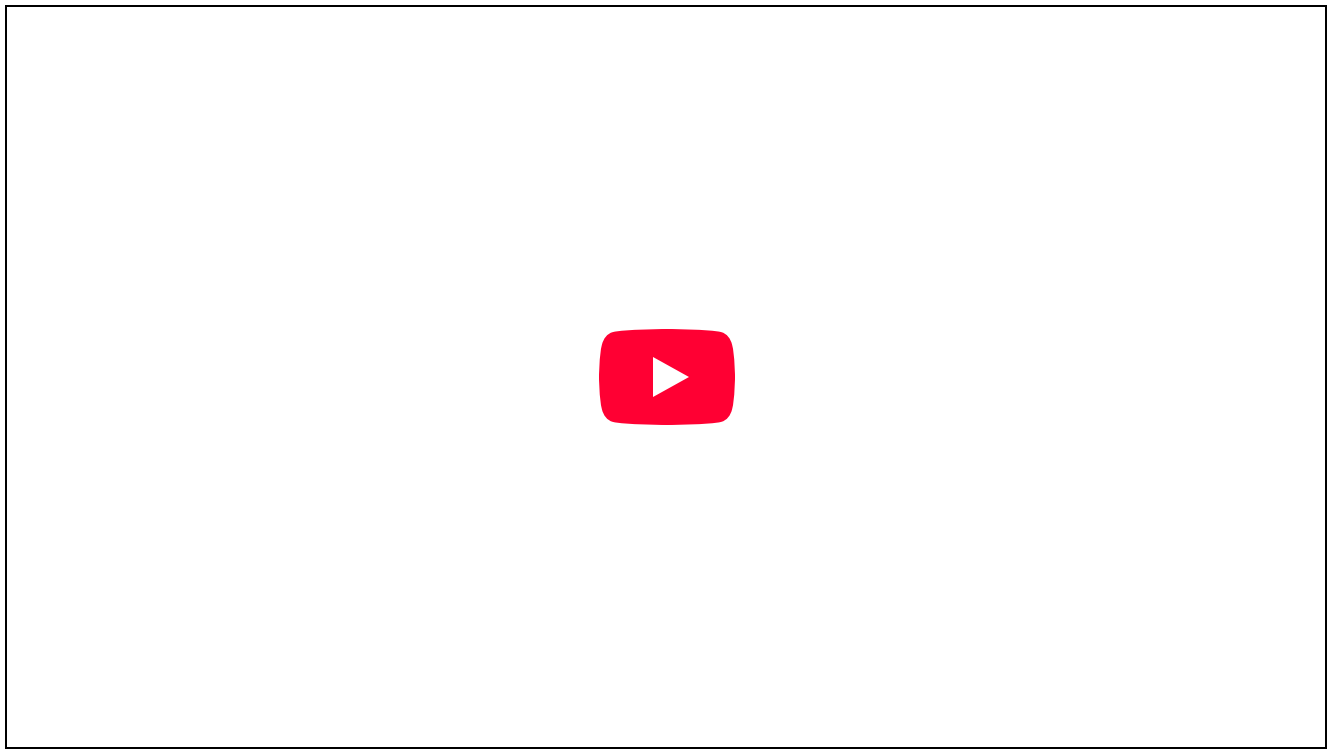
“What used to take us two months in a background check or an investigation is now taking between five to 15 minutes.”

Alerted to this problem by a friend from Pretoria, South Africa-based Paterva, makers of the Maltego OSINT platform, Clemens decided to build SocialNet. As he put it in an interview, “the idea [behind SocialNet] was, let’s throw a net out into all of the social media platforms, the social media universe, and see what we get back.” Clemens has claimed in a company video that “when the FBI started using [SocialNet], they did an evaluation” and concluded “what used to take us two months in a background check or an investigation is now taking between five to 15 minutes.”

Today, SocialNet says it pulls data from more than 120 social media networks, websites, and platforms, as well as from the dark web, data dumps, and RSS feeds. A full list of sources isn’t available, but a company promotional video and listing at the Maltego website gives an indication of which websites fall into their surveillance net:

> *AOL Lifestream* | *Amazon* | *Ameba* | *Aodle* | *BabyCenter* | *BitChute* | *BlackPlanet* | *Blogger* | *Busted! Mugshots* | *Buzznet* | *Cocolog* | *Companies House* | *Crunchbase* | *Dailymotion* | *DeviantArt* | *Ebay* | *Etsy* | *Facebook* | *Flickr* | *Foursquare* | *Gab* | *GitHub* | *Goo* | *Google* | *Google+* | *Gravatar* | *Hatena* | *Huffington Post* | *ICQ* | *IMVU* | *ImageShack* | *Imgur* | *Instagram* | *Instructables* | *Jugem* | *Kik* |*LinkedIn* | *LiveJournal* | *Livedoor* | *Mail.ru* | *Menuism* | *MeWe* | *MySpace* | *Naijapals* | *Netlog* | *OK Cupid* | *Okru* | *Olipro Company* | *Pandora* | *Pastebin* | *PayPal* | *PGP* | *Photobucket* | *Pinterest* | *Plurk* | *POF* | *PornHub* | *QQ* | *Reddit* | *ReverbNation* |

> *Seesaa | Skype | SoundCloud | SourceForge | Spotify | Sprashivai | Steam | Sudani | Telegram | Tinder | TripAdvisor | Tumblr | Uplike | Vimeo | Vine | Virus Total | VK | Voat | Weibo | Xing | Yahoo | Yelp | YouTube | Zillow*



The video also shows "public and local" IP addresses as a source of data for SocialNet.

SocialNet searches for information that is publicly available across these websites and pulls it in when there is a match. But it is difficult to know with precision which data it pulls. In the promotional video, some categories of information appear, such as BlackPlanet users; Busted! mugshots; Bing search results; Amazon comments, products, users, and wishlists; and so on. Clemens said the company has "crawlers that scrape information from the public websites. Nothing proprietary or private is provided to us by the platform companies."

On its website, ShadowDragon also claims to conduct "chat protocol monitoring (WhatsApp, Telegram, etc.)" as well as "dialog protocol monitoring (IRC, etc.)." For these services, it's also unclear exactly what

kinds of information can be pulled or how it's done. Clemens said they don't intercept any private chats, and they can confirm whether a specific phone number has a WhatsApp account if the user's privacy settings allow it.

In a March 2019 blog post, Clemens referenced an "integration into monitoring Telegram," which, along with WhatsApp, had become "a go-to when there are disruptions." He also claimed to have added "some interesting OSINT capabilities in our SocialNet platform for more hardened and encrypted/secure communication protocols. (Please ping us on this)." Although Telegram has said its instant messages are "heavily encrypted," it also offers widely available groups and channels.

Clemens said the company is able to monitor chat platforms like Telegram through public sources of information, which reveal, for example, "if you respond to a public thread of Twitter or public Telegram group." He added, "We don't evade any encryption implementations because we're not interested in weakening the technical security for other platforms." Clemens declined to elaborate on what "capabilities" SocialNet has "for more hardened and encrypted/secure communication protocols."

In fact, ShadowDragon seems to strive toward total information awareness. In an interview about investigations, Clemens has stated, "I want to know everything about the suspect: Where do they get their coffee, where do they get their gas, where's their electric bill, who's their mom, who's their dad?"

The precise inner workings of SocialNet are off limits to the public, as it is expensive software that is sold at the discretion of the company. Nevertheless, some online resources give an indication of how it works.

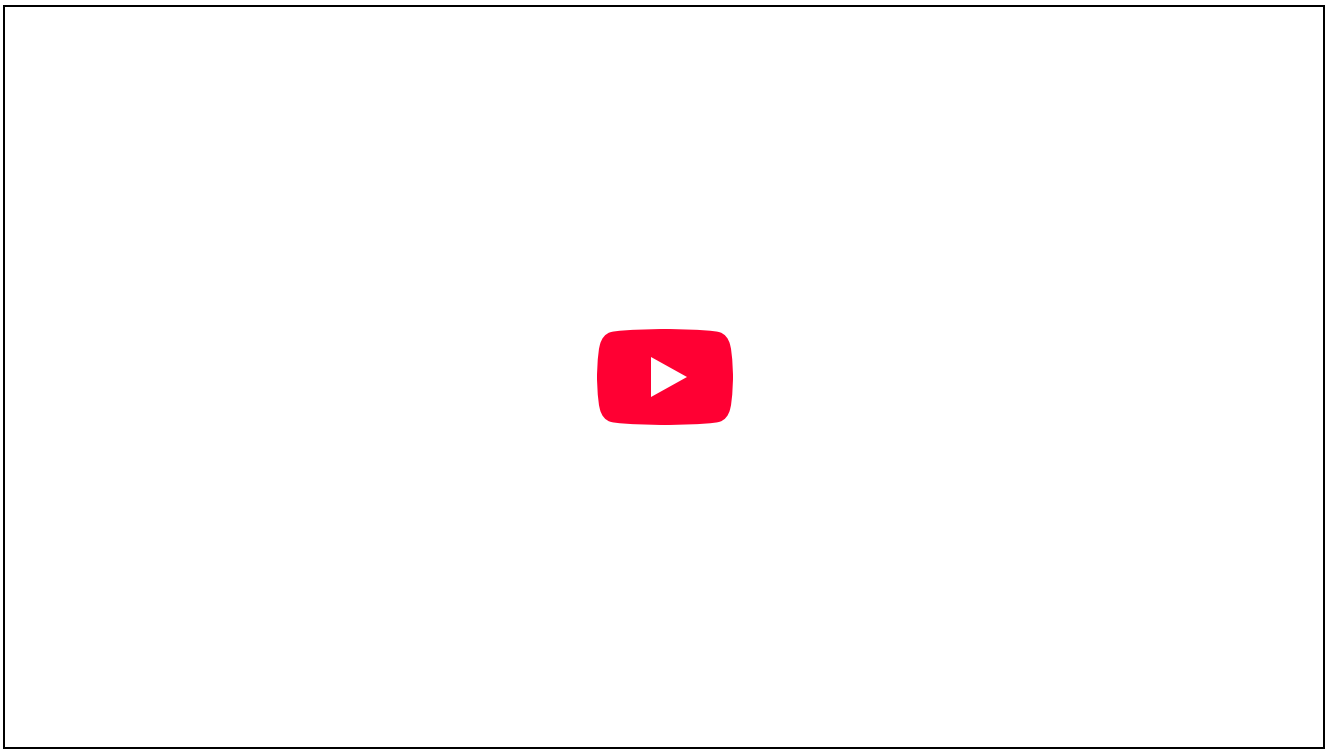
With its surveillance net cast across the internet, SocialNet can be used to perform investigations on persons and networks of interest,

according to publicly available marketing materials. Investigators can run search queries for names, email addresses, phone numbers, aliases, or other information to begin to identify persons of interest, determine their physical location, ascertain their "lifestyles," and analyze their broader networks (such as friends and friends of friends).

"I want to know everything about the suspect: Where do they get their coffee, where do they get their gas, where's their electric bill, who's their mom, who's their dad?"

The materials also show how SocialNet organizes information for the analyst, visually mapping social network graphs and suggesting links between persons of interest and their networks. Timelines can be created to help sort out evidence and piece together clues into a broader picture of what the investigator is trying to uncover. Physical locations can be uncovered or inferred.

An online tutorial from 2011 depicts an investigator using SocialNet to hunt down possible targets by cross-referencing their company domain names with their email addresses, then finding a friend who two targets might have in common. The demonstration suggests that the investigator might want to "social engineer" — or trick — the mutual friend into speaking to the targets.



The other ShadowDragon tool purchased by the Michigan State Police, OIMonitor, sends alerts in response to the sort of data captured by SocialNet, a company engineer says in an online video.

Other company materials say OIMonitor can go further, helping to detect potential crime before it happens and performing other advanced feats. One video explains OIMonitor can "automate and customize monitoring parameters." In another video, a ShadowDragon representative provides an example of a corporation looking to protect its physical venue or executives. The corporation would "build out an entire dossier of attack patterns, of things people say that's bad or something threatening," and OIMonitor "just alerts them when it sees the criteria that they've set and that they have experience recognizing as a problem."

Clemens told me that "customers come to us for the ability to identify and analyze previous patterns of behavior and relationships using only public information. We disagree with predictive policing and so we don't build products with predictive capabilities or even suggestions."

Yet their own website says, in the description for the "Predicting Violence" video, "Clever security teams use OIMonitor to find indicators of unrest and violence before they start. Because riots don't start in a vacuum; there are always indicators." It's also unclear if information pulled from ShadowDragon may be pooled with other data and used by clients for predictive policing on other systems (Clemens declined to comment on that).

Hatch raised an alarm about the civil rights implications of ShadowDragon's software, stating, "It could be used to incorrectly identify Black people as criminal suspects and out social justice activists who wish to remain anonymous for fear of being harassed by police and white nationalists."

ShadowDragon also appears to be hoarding information that users and platforms wanted to delete. OIMonitor provides clients with access to ShadowDragon's private "historical archive from 2011 to today," and it saves monitoring results in case the data disappears from the web, according to one company video.

"It could be used to incorrectly identify Black people as criminal suspects and out social justice activists."

In a case example given by the company, running the phone number of a suspect through the ShadowDragon software "popped up with an old Foursquare account" he had logged into at his mother's house 10 years ago. After looking for the suspect for a month, the investigators were able to find him the following day.

In addition to police, ShadowDragon services corporate clients, and it can be potentially used for worker surveillance. In a blog post, the company advertised the ability to use OIMonitor for employee background checks by employers. Clemens declined to respond to questions about using ShadowDragon for worker surveillance.

Kaseware: An End-to-End Investigative Platform

Compared with ShadowDragon, Kaseware, the other software company contracting with Michigan State Police, is more sweeping in scope, handling more aspects of police work and venturing into the controversial realm of algorithmic crime fighting.

In 2009, Kaseware's founders were working at the FBI, where, the company says, they transformed its 1980s mainframe system into an award winning, modern, web-enabled platform called Sentinel. Soon thereafter, some of the designers of Sentinel left the FBI to build Kaseware, based out of Denver and launched in 2016 as a cloud "software as a service" product for government and corporations.

Kaseware is a centralized online platform where law enforcement authorities, intelligence agencies, and corporations can dump their surveillance data. Once on the platform, the surveillance can be monitored, mapped, and otherwise analyzed using tools built specifically for Kaseware. The company touts the system's speed and ability to integrate diverse sources of information for command-and-control centers, saying it handles investigations and security monitoring in an "end-to-end" way: from the ingestion of raw surveillance at one end to the conclusion of an investigation at the other. Its diverse set of capabilities are similar to Microsoft's Domain Awareness System.

Kaseware claims to streamline a wide range of law enforcement drudgery: generating reports, managing workloads, facilitating video conferences, and querying information from the controversial federal records clearinghouse National Crime Information Center. A redacted portion of the MSP contract says it can "integrate with FBI eGuardian system via file exchange." The eGuardian system allows the FBI to collect and share Suspicious Activity Reports, or SAR, from different agencies across the United States. As the ACLU notes, the system gives law enforcement officials broad discretion to collect information about commonplace activities and to store it in criminal intelligence files without evidence of wrongdoing.

A cornerstone Kaseware feature is its ability to ingest and analyze massive amounts of data. Files, records, logs, disc images, and evidence are pulled into the platform, which can also handle evidence from "recordings, body cameras, closed-circuit television (CCTV) cameras and other sources." The company claims it can help hunt down a perpetrator's physical location.

Screenshot: The Intercept

Kaseware marketing materials say its platform ingests zip codes, addresses, GPS coordinates, geotags, satellite imagery, and data from internet-connected devices, correlating it with "socioeconomic trends and environmental events to create layered maps" to reveal "illegal activity" and — crucially, for civil rights advocates — conduct "predictive policing."

Predictive policing, or the use of statistics that quantifies past crimes to predict future ones, has been heavily criticized by legal scholars and activists on grounds that the systems generate discrimination and harm. Two scholars tested the PredPol predictive policing software for Oakland, California, and found its software would target Black people at twice the rate as white people. This is because Black people are overrepresented in Oakland's drug crime databases, leading to disproportionate policing of low-income communities and communities of color.

The Michigan State Police told me, "We do not use the predictive policing function of the Kaseware platform." However, it is worth noting the capability is there, and the software has been sold to other clients who may be making use of it.

Kaseware also touts its access to open source intelligence across its marketing literature. Its platform utilizes OSINT tools like ShadowDragon "to instantly search hundreds of open web, dark web, deep web and social media sources to access crucial data on cybercriminals' names, keywords, emails, aliases, phones numbers and more." Clients "can also import social media information for forensic analysis alongside other case details, including photos, followers, likes, friends and post connections."

It's unclear if Kaseware has special access to information or services with the companies listed in the way that Dataminr, for example, is

provided access to Twitter's "firehose," a database of every public tweet from the moment it was posted. Twitter's senior director of global public policy strategy, Nick Pickles, told me in an email that "we're not able to disclose details of our commercial agreements," but it is "safe to say that" Kaseware is "on our radar." Another Twitter spokesperson, Katie Rosborough, did not answer questions about Kaseware or ShadowDragon, saying only that Twitter's public programming interface is not available for law enforcement purposes. Partners like Dataminr historically have not used that interface.

Contracts and Deployments

The Michigan State Police contract redacts every mention of ShadowDragon, SocialNet, OIMonitor, and Microsoft Azure in the contract shared with the public. David Goldberg's FOIA request was "partially denied" citing exemptions to the act to protect "trade secrets, or financial or proprietary information"; to "protect the security or safety of persons or property, or the confidentiality, integrity, or availability of information systems"; and to protect "the identity of a person who may become a victim of a cybersecurity incident as a result of the disclosure of identifying that person" or that person's "cybersecurity-related practices."

As I reported at The Intercept, through its Public Safety and Justice division, Microsoft provides an extensive array of services to police forces across the world via its own products and that of partners (like Kaseware), who typically operate on the Azure Cloud. Microsoft services the U.S. and Israeli militaries with its HoloLens augmented reality goggles. Its carceral solutions include its own Digital Prison Management Solution based on its Domain Awareness System surveillance platform built with the New York Police Department years ago. Together with its partners, Microsoft's products and services extend

across the carceral pipeline, from juvenile detention and pretrial through prison and parole.

Kaseware's Mark Dodge, a former Naval intelligence and CIA officer, helped develop Microsoft's Domain Awareness System for the NYPD.

Kaseware's Chief Business Officer Mark Dodge, a former Naval intelligence and CIA officer, told me in interviews prior to this year that before working at Kaseware, he had worked at Accenture, where he helped develop Microsoft's Domain Awareness System for the NYPD. He said he also did work for Singapore, which runs the Microsoft DAS, and "a couple others," including in London. Dodge then had a brief stint with Microsoft partner Axon, the industry leader in Taser stun guns and body cameras — illustrating how circles in the intelligence, police, and corporate surveillance industry intersect.

The length of the MSP contract is five years, from January 31, 2020, to January 31, 2025. The Kaseware license costs $340,000 annually, while SocialNet and OIMonitor cost $39,000 each, bringing the package to $418,000 per year, or $2,090,000 over five years. The state of Michigan redacted the contract values of ShadowDragon features. The MSP opted for a two-day training session at $3,000, which ShadowDragon says constitutes a "big deep dive on threat assessment and sentiment analysis."

The total cost of the MSP contract is $3,293,000.

The sum paid to Microsoft for its Azure Government Cloud services is bundled into the "Licensing & Support Services" portion of the contract, and there is no indication how much of that money Microsoft receives.

Because most of their contracts are not made public or difficult to access, it's hard to discern how pervasive Kaseware and ShadowDragon are in the world.

The first ShadowDragon contract with the U.S. Immigration and Customs Enforcement agency was awarded to IT firm C & C International Computers & Consultants, Inc. on July 16, 2020, at a cost of $289,500. The second was for a contract awarded to cybersecurity firm Panamerica Computers on August 31, 2021 at a cost of $602,056. Both were for the use of SocialNet.

ShadowDragon's SocialNet, OIMonitor, and malware investigation product MalNet is also being deployed by IT firm ALTEN Calsoft Labs and Cloudly in Asia — "especially India" — as "solutions for industries such as Government, Banking, Financial Services, Healthcare and many other verticals." ALTEN is headquartered in Bangalore, India, and has offices in the U.S., Europe, and Singapore. Cloudly is a cybersecurity, intelligence, and surveillance firm based in Silicon Valley.

With offices in the U.S. and Denmark, ShadowDragon claims a market presence in "North America, Europe, the Middle East, Asia and Latin America."

When asked about potential human rights abuses by clients, Clemens said the company vets "all in-bound requests for our products to ensure they're not used to conduct human rights violations."

Dodge, in the interviews predating this story, told me Kaseware had about 30 customers as of June 2020 but does not disclose most of them. The Winslow, Arizona, Police Department rolled out a Kaseware Computer Aided Dispatch and Records Management System in 2018, and the Wickenburg, Arizona, Police Department was at least considering it.

Kaseware states its platform "is now used by police departments around the world, Fortune 100 Companies, and many international non-profit organizations."

Kaseware did not respond to a request for comments for this article.

Human Rights: A World of All-Seeing Public Surveillance

With Kaseware and ShadowDragon, we live in a world where the public's online behavior can be monitored across the internet and accessed at the click of a button to determine who we are, who we know, what our "lifestyle" is like, where we are located, and more.

These capabilities fundamentally change police powers, said Eric Williams, managing attorney at the Detroit Justice Center's Economic Equity Practice: "It is qualitatively different when you go from the police being able to check information" a little at a time "to artificial intelligence being able to analyze everything that you've done online."

The potential for discriminatory applications is enormous. Williams noted that searches made by big data tools are "inevitably biased against people of color, poor people" and the like. He said that activists from Black Lives Matter, unions, and the #MeToo movement may be targeted by these technologies, "depending on who is in charge of them."

Phil Mayor, a senior staff attorney at the ACLU of Michigan, said of ShadowDragon, "mapping of the relationships between

"This presents the scary possibility of law enforcement of our

people risks suspicion by association" and "is likely to entrench systemic racism and is a threat to everyone's privacy. … This presents the scary possibility of law enforcement of our daily lives that would be unimaginable until recently."

daily lives that would be unimaginable until recently."

There is virtually no transparency behind what Kaseware and ShadowDragon do, or how the Michigan State Police and other clients might be using their products, where they are deployed, for what purpose, and who gets access. Likewise for how these tools impact activists, the poor, and marginalized communities, who are disproportionately the targets of police surveillance.

"It's deeply concerning that this kind of technology is being purchased and used by law enforcement without public discussion," Mayor told me. "Before engaging in new forms of surveillance of citizens, law enforcement should be coming to the polity and asking what we expect in terms of our privacy rather than making those decisions for us."

Williams echoed this, stating, "It is problematic that public money is being spent on surveillance, of a particularly intrusive type, and the public is unaware of it." Even if the police want to keep their surveillance methods hidden, "the public has a right to know, and should know, given the lack of laws we have governing a lot of electronic surveillance."

In the U.S., as many as 70 percent of police forces use social media to gather intelligence and monitor the public. Yet the law does little to constrain these kinds of tools and practices.

“There’s not a lot of regulations on this,” Williams said, “and we can’t begin to have a discussion on how it should be regulated if we’re not aware that it’s happening.” He added that he favors a ban on the technology, given its opaque deployment and intrusive nature.

Dragnet social media surveillance needs to be urgently addressed by lawmakers, who should step in and ban this attack on civil rights and liberties immediately.

RELATED

How the LAPD and Palantir Use Data to Justify Racist Policing

Powerful Mobile Phone Surveillance Tool Operates in Obscurity Across the Country

Twitter Surveillance Startup Targets Communities of Color for Police

The Microsoft Police State: Mass Surveillance, Facial Recognition, and the Azure Cloud

The Intercept_