Revealed: U.S. Military's Massive Biometric Data System

The U.S. Military is heavy-laden with Technocrats bent on collecting data for the sake of social engineering. Their rapidly growing global dragnet now contains images, fingerprints and DNA data on 7.4 million people. TN Editor

Over the last 15 years, the United States military has developed a new addition to its arsenal. The weapon is deployed around the world, largely invisible, and grows more powerful by the day.

That weapon is a vast database, packed with millions of images of faces, irises, fingerprints, and DNA data — a biometric dragnet of anyone who has come in contact with the U.S. military abroad. The 7.4 million identities in the database range from suspected terrorists in active military zones to allied soldiers training with U.S. forces.

"Denying our adversaries anonymity allows us to focus our lethality. It's like ripping the camouflage netting off the enemy ammunition dump,"

wrote Glenn Krizay, director of the Defense Forensics and Biometrics Agency, in notes obtained by *OneZero.* The Defense Forensics and Biometrics Agency (DFBA) is tasked with overseeing the database, known officially as the Automated Biometric Information System (ABIS).

DFBA and its ABIS database have received little scrutiny or press given the central role they play in U.S. military's intelligence operations. But a newly obtained presentation and notes written by the DFBA's director, Krizay, reveals how the organization functions and how biometric identification has been used to identify non-U.S. citizens on the battlefield thousands of times in the first half of 2019 alone. ABIS also allows military branches to flag individuals of interest, putting them on a so-called "Biometrically Enabled Watch List" (BEWL). Once flagged, these individuals can be identified through surveillance systems on battlefields, near borders around the world, and on military bases.

The presentation also sheds light on how military, state, and local law enforcement biometrics systems are linked. According to Krizay's presentation, ABIS is connected to the FBI's biometric database, which is in turn connected to databases used by state and local law enforcement. Ultimately, that means that the U.S. military can readily search against biometric data of U.S. citizens and cataloged non-citizens. The DFBA is also currently working to connect its data to the Department of Homeland Security's biometric database. The network will ultimately amount to a global surveillance system. In his notes, Krizay outlines a potential scenario in which data from a suspect in Detroit would be run against data collected from "some mountaintop in Asia."

The documents, which are embedded in full below, were obtained through a Freedom of Information Act request. These documents were presented earlier this year at a closed-door defense biometrics conference known as the Identity Management Symposium.

ABIS is the result of a massive investment into biometrics by the U.S. military. According to federal procurement records analyzed by *OneZero,* the U.S. military has invested more than $345 million in biometric database technology in the last 10 years. Leidos, a defense

contractor that primarily focuses on information technology, currently manages the database in question. Ideal Innovations Incorporated operates a subsection of the database designed to manage activity in Afghanistan, according to documents obtained by *OneZero* through a separate FOIA request.

These contracts, combined with revelations surrounding the military's massive biometric database initiatives, paint an alarming picture: A large and quickly growing network of surveillance systems operated by the U.S. military and present anywhere the U.S. has deployed troops, vacuuming up biometric data on millions of unsuspecting individuals.

The military's biometrics program, launched in 2004, initially focused on the collection and analysis of fingerprints. "In a war without borders, uniforms, or defined lines of battle, knowing who is an enemy is essential," John D. Woodward, Jr., head of the DoD's biometrics department, wrote in a 2004 brief.

That year, the Department of Defense contracted Lockheed Martin to start building a biometrics database for an initial fee of $5 million. Progress was slow: by 2009, the DoD Inspector General reported that the biometrics system was still deeply flawed. The department indicated that it was only able to successfully retrieve five positive matches from 150 biometric searches. A later contract with defense industry giant Northrop resulted in similarly disappointing results with reports of "system instability, inconsistent processing times, system congestion, transaction errors, and a 48-hour outage."

By 2016, the DoD had begun to make serious investments in biometric data collection. That year, the Defense Department deputy secretary Robert O. Work designated biometric identification as a critical capability for nearly everything the department does: fighting, intelligence gathering, law enforcement, security, business, and counter-terrorism. Military leaders began to speak of biometric technology as a "game changer," and directives from the DoD not only encouraged the use of the technology by analysts, but also by soldiers on the ground. Troops were instructed to collect biometric data whenever possible.

The same year, a defense company named Leidos, which had acquired a large portion of Lockheed's government IT business, secured a $150 million contract to build and deploy what is now known as the DoD ABIS system.

Read full story here…

'Switcharoo' Leaks: Facebook Stomped Competition While Pitching User Privacy

Bloomberg reports that leaked docs "portray company executives plotting how to convince the public they were serious about improving privacy protections even while their real goal was to snuff out competition." TN Editor

Facebook Inc.'s struggle to regain trust over how it handles user data got more complicated with the release of a trove of internal documents suggesting business considerations outweighed the privacy concerns the company publicly touted when it decided five years ago to cut off tens of thousands of developers from its platform.

The company's "Switcharoo Plan," a nickname bestowed by a Facebook employee in an email, was revealed in thousands of pages of sealed court records described Wednesday in a report by Reuters and posted online by NBC News.

The documents portray company executives plotting how to convince the public they were serious about improving privacy protections even while their real goal was to snuff out competition

The leaked records include internal Facebook emails and memos that were filed under seal in state court in California as part of a lawsuit brought by an aggrieved Silicon Valley app developer. Six4Three LLC's app allowed users to find photos of their Facebook friends in bathing suits.

"These old documents have been taken out of context by someone with an agenda against Facebook, and have been distributed publicly with a total disregard for US law," a Facebook representative said Wednesday.

Six4Three sued Facebook in 2015 after the social media giant cut off its access — along with that of thousands of other app developers — to Facebook user data, thereby destroying the functionality of its app.

The disclosure of the confidential documents comes as Facebook faces increased scrutiny over alleged anti-competitive behavior.

In September, congressional lawmakers probing antitrust issues in Big Tech made extensive document requests of Facebook, including executive communications on company decisions "to deny any specific app or any categories of apps access to Facebook's APIs" as well as moves "to require that any specific app or any categories of apps purchase ads on Facebook in order to maintain access to Facebook APIs"

or other user data.

The companies had produced “tens of thousands” of documents as of mid-October, according to Democratic Representative David Cicilline of Rhode Island, who is leading the probe.

Meanwhile, California went to court Wednesday to force Facebook to cooperate with an investigation into whether the company has violated its users’ privacy and state law. The company said it has ”cooperated extensively” with the state probe.

Facebook had a history of preventing rivals — even ones who weren’t real rivals yet — from using its advertising products. In 2013, Facebook restricted ads for competitive Google products, as well as WeChat, Line and Kakao, the messaging apps popular in Asia. “Those companies are trying to build social networks and replace us,” Chief Executive Officer Mark Zuckerberg said in a 2013 email. “The revenue is immaterial to us compared to any risk.”

Read full story here…

Amazon Co-opting Homeowner's Ring Cameras To Police

Several weeks ago it was reported that over 400 law enforcement agencies had partnered with Amazon's Ring Camera. Ring distributes a free app called the Neighbors App that Ring owners use to store video images in the cloud. Amazon has now bonded its Neighbor's app with police agencies to effectively turn private homeowners into snitches for the police.

While Ring cameras have been used to catch some criminals that come to your door, there are huge privacy concerns because the administrators/ controllers have direct access to all cameras in the system. Currently, police are not given full access to homeowner's installed cameras, and homeowners must volunteer to upload videos to their local police department.

Why would anyone think that Amazon would somehow be benevolent with the data its collects? With a demonstrated history of listening in on its Alexa speakers, who would not expect them to do the same with Ring? Furthermore, who would expect Amazon to offer a 'free' app to both homeowners and police without having an ulterior motive to monetize and/or weaponize the data? And, keep in mind that Amazon is creating and selling the most sophisticated facial recognition software in the world… to the same law enforcement agencies.

Amazon is creating the ultimate surveillance grid for law enforcement that will include millions of homeowners in thousands of cities across America.

A Technocracy News reader in San Bernardino, California forwarded to me an email received from the local Sheriff's office:

> *The San Bernardino County Sheriff's Department is excited to*

> *announce our partnership with Ring and the Neighbors App.* ***Detectives and station personnel from across the county completed their training today and our stations are now live.*** *Station staff are able to receive information and interact with residents through the app. Customers with a Ring camera will be able to share videos with their local Sheriff's station. The Neighbors App connects communities with the goal of creating safer and stronger neighborhoods and one of the benefits is you do not need to own a Ring device to use the app.*

I could find no public notice of the training that is mentioned above, but it clearly was nationwide and it clearly took place. The result is that the system has gone live.

The following article provides more details about how it all works.

Police partnerships with doorbell-camera company raise privacy questions

Dyana Bagby via Reporter Newspapers

In February, the Dunwoody Police Department sent out an upbeat press release announcing it was the first in Georgia to team up with doorbell-camera company Ring to access the company's Neighbors app. The partnership, the department boasted, could help the department crack down on package thieves, stop burglaries and keep neighborhoods safe.

"Leveraging today's technology to help keep our citizens safe is a key focus of our department," Dunwoody Police Chief Billy Grogan said in the release. "Our partnership with Ring and use of the Neighbors app will definitely help in our crime fighting efforts."

The Brookhaven Police Department followed up a month later with its own press release announcing its alliance with Ring.

"Partnering with Ring using the Neighbors app will give officers a

technological advantage when investigating crimes," Brookhaven Police Chief Gary Yandura said in the release.

Dunwoody and Brookhaven are just two of 10 law enforcement agencies in Georgia to team up with Ring, owned by corporate giant Amazon. Across the nation, more than 400 law enforcement agencies have signed on with Ring to gain free access to surveillance video shared by customers to Ring's public social network, named "Neighbors." Through the partnership, law enforcement agencies gain access to the Neighborhood Portal which includes a map of where Ring cameras are located.

Other Georgia law enforcement agencies partnering with Ring including police departments and sheriff's offices in Chamblee, Cobb County, Duluth, Forsyth County, Garden City, Gwinnett County, Sandy Springs and the Savannah Police Department.

"This partnership is another way for us to engage the community and share information in a timely manner," Sandy Springs Deputy Chief of Police Keith Zgonc said in an email. The department teamed up with Ring in April.

For some, the rising number of police partnering with Ring is chilling. They say Ring is creating a nationwide surveillance network that raises serious concerns about privacy and the blurring of police departments with corporations.

"Constant surveillance may sound safe for people who have nothing to fear from a biased criminal justice system, but making the decision to extend Amazon and police surveillance to your home is a potential hazard for people who live and work in your community," said Matthew Gauriglia, policy analyst for the Electronic Frontier Foundation. EFF is an international nonprofit organization "defending civil liberties in the digital world," according to its website.

Ring says its partnerships with law enforcement are just another way to keep communities safer by allowing police and residents to share crime and safety information through the Neighbors app.

“We are proud to work with law enforcement agencies across the country and have taken care to design these programs in a way that keeps users in control,” a spokesperson said in a written statement.

The partnerships claim to ensure anonymity to Ring users by requiring police to make a request to the company for footage they saw on the Neighbors app they want for an investigation. Ring then contacts the homeowner to make the actual request.

“With each request, customers decide whether to share all relevant videos, review and select certain videos to share, take no action (decline), or opt out of all future requests,” Ring says in a FAQ on its website.

Grogan also discounted privacy concerns, saying police are only looking for surveillance footage someone has voluntarily posted to the Neighbors app.

“I understand to some degree some concerns about ‘Big Brother,’ but you also have to understand that none of us have the resources or time to really look at video just randomly just see what people are doing,” Grogan said.

“We have specific purposes, to investigate crimes … other than that we are not looking at video,” he said. “We have no direct access to anything. It’s all voluntary. Nobody has to share anything with us.”

EFF says it’s not as black-and-white as Ring says when it comes to giving their customers the choice to not share video footage with police. Ring acknowledged in a story in Government Technology that if a resident does not want to share their footage, the company will still turn it over if a law enforcement agency has a “valid and binding legal demand.”

Yandura did not say his department has made demands for Ring footage, but said when customers post to the Neighbors app, it essentially becomes part of the public domain.

“Once someone publishes to the app, it’s out there,” Yandura said.

How Ring and the Neighbors app work

Residents can download the free Neighbors app and use it to monitor neighborhood activity, share crime and safety-related videos, photos and text-based posts; and receive real-time safety alerts from their neighbors, local law enforcement and the Ring team, according to a Ring press release.

Ring users are alerted when their doorbell-cameras detect motion from as far away as 30 feet; when someone presses the video-doorbell button; or when the user turns on a "Live View" option through the Ring app.

Those events begin recording a video file that is streamed from the Ring device to the cloud on Amazon Web Services servers, according to the company's privacy notice.

Those who subscribe for $3 a month to Ring Protect Plans can have their videos stored on the cloud for 60 days to watch them later. Those without a plan will have their videos automatically deleted, according to Ring's privacy notice.

Ring's terms of service says the company and its licensees have permanent and wide-ranging rights to keep and use the footage from the cameras, including: "an unlimited, irrevocable, fully paid and royalty-free, perpetual, worldwide right to re-use, distribute, store, delete, translate, copy, modify, display, sell, create derivative works from and otherwise exploit such shared content for any purpose and in any media formats in any media channels without compensation."

This kind of corporate control of homeowner's video surveillance contributes to what EFF calls a "perfect storm of privacy threats."

"Having a Ring camera may seem like a harmless way to protect your packages, but it is helping to create a large surveillance network within your own community that does more than just thwart the work of criminals," Gauriglia said.

When Ring customers continually post footage to the Neighbors app resulting in constant alerts sent to users, fear is generated in communities, EFF says. That leads to more sales of Ring doorbell-cameras and other security devices, adding to an already massive

surveillance network, according to EFF.

“With every update, Ring turns the delivery person or census-taker innocently standing on at the door into a potential criminal,” Gauriglia reported in an Aug. 8 EFF story. “Neighborhood watch apps only increase the paranoia.”

Yandura said there is nothing threatening about the Ring cameras, saying they are like having a “cop on every corner in the city” 24 hours a day.
Grogan said Ring and the Neighbors app are simply keeping communities informed on what is happening in their neighborhoods.

“People know their neighborhoods better than anybody,” he said. “They live there and know what is unusual. … The people that participate are choosing to do that and making the decision to work with police to try to help keep their communities safe.”

How many Ring doorbell-camera users live in Dunwoody and Brookhaven is not known by the police departments, according to the chiefs, and Ring declined to comment on this question.

Yandura did say a Ring representative told him earlier this year that Brookhaven’s 30319 ZIP code had the highest concentration of Ring devices in the state.

Both cities have also invested heavily in surveillance cameras and license plate readers, or LPRs.

Earlier this year, Dunwoody spent about $189,000 to buy 16 LPRs from Georgia Power to post throughout Perimeter Center where most of the city’s crime occurs.

In 2017, Brookhaven entered into a $700,000, three-year lease agreement with Georgia Power to place 44 LPRs throughout the city. The LPRs average 4 million “reads” a month of people driving in and out of the city, Yandura said, and are used to get hits on stolen cars and wanted fugitives.

What’s included in the partnership

Grogan said the department reached out to Ring last year after reading about the company partnering with law enforcement through the Neighbors app.

Yandura said he learned about Ring and the Neighbors app at a conference for the International Association of Chiefs of Police.

After the chiefs agreed their departments would team up with Ring, they were required by the company to sign memorandums of understanding, non-binding agreements that outlined roles and responsibilities. Both cities MOUs stated Ring would provide mutually agreed-upon press releases announcing the partnerships.

The agreements included Ring providing the departments a few free Ring doorbell cameras to give out to residents at community events or homeowners' association meetings.

ast month, the Dunwoody Police Department hosted a "pizza with police" event at City Hall that included free Ring doorbell camera giveaways. Yandura said Brookhaven Police have also handed out four free Ring cameras at community events and HOA meetings.

Emails obtained through the open records request show that Dunwoody Police Department employees were given a special promotion code, "nbdunwoody," after the MOU was signed in February. The code gave them $50 off any purchase of the Ring Classic, Ring Pro, Ring Video Doorbell 2, Floodlight Cam, Spotlight Cam and Ring Protect.

Ring also provided a free webinar to Dunwoody officers to train them on how to use the Neighbors app portal, according to emails.

Those requested by Ring to attend online training included the public information officer, the social media coordinator, an investigative coordinator and a community relations coordinator who "oversees the team that interfaces with the community at events, HOAs, Neighborhood Watch meetings, etc."

These kinds of agreements can weaken a police department's standing in a community where they are supposed to be neutral, Gauriglia said

“Ring-police partnerships also undermine our trust in local police departments,” he said. “We know from reporting that almost everything police put out about Ring, from press releases to the answers to potential questions citizens may have, are scripted and approved by Amazon.”

Grogan denied Amazon or Ring had control over what his department says, including the initial press release announcing the partnership.

“We modified it and removed language we felt sounded too much like an endorsement of the Ring camera,” he said. “Other than that, they have provided no input into any other communication related to the Neighbors by Ring app.”

Yandura also denied the arrangement meant Brookhaven officers were now representing Amazon and Ring.

“No, we are not salesmen and no money is exchanged by the parties,” Yandura said. “We are not promoting one [security company] over another.”

Ring did include in its Dunwoody MOU that it would donate Ring cameras to the Dunwoody Police Department based on the number of Neighbors app downloads that result from their partnership with the city.

“Each qualifying download will count as $10 toward these free Ring cameras,” according to the Dunwoody MOU.
Grogan said his department is not obligated to Ring or Amazon.

“We don’t actively promote one system over another,” he said. “If any other camera company wants to provide free security cameras for us to give out, we will give them out as well.”

Read full story here…