

Exposed Chinese database shows depth of surveillance state

February 19 2019, by Yanan Wang And Dake Kang



In this Aug. 31, 2018, file photo, a child and a woman wait outside a school entrance mounted with surveillance cameras and barricades with multiple layers of barbed wire in Peyzawat, western China's Xinjiang region. The Chinese database Victor Gevers found online was not just a collection of old personal details. The discovery by Gevers, a Dutch cybersecurity researcher who revealed it on Twitter last week, has given a rare glimpse into China's extensive surveillance of Xinjiang, a remote region home to an ethnic minority population that is largely Muslim. The area has been blanketed with police checkpoints and security cameras that apparently are doing more than just recording what happens. The database Gevers found appears to have been recording people's movements tracked by facial recognition technology, he said, logging more than

6.7 million coordinates in a span of 24 hours. (AP Photo/Ng Han Guan, File)

The Chinese database Victor Gevers found online was not just a collection of old personal details.

It was a compilation of real-time data on more than 2.5 million people in western China, updated constantly with GPS coordinates of their precise whereabouts. Alongside their names, birthdates and places of employment, there were notes on the places that they had most recently visited—mosque, hotel, restaurant.

The discovery by Gevers, a Dutch cybersecurity researcher who revealed it on Twitter last week, has given a rare glimpse into China's extensive surveillance of Xinjiang, a remote region home to an ethnic minority population that is largely Muslim. The area has been blanketed with police checkpoints and [security cameras](#) that apparently are doing more than just recording what happens.

The database Gevers found appears to have been recording people's movements tracked by [facial recognition technology](#), he said, logging more than 6.7 million coordinates in a span of 24 hours.

It illustrates how far China has taken facial recognition—in ways that would raise alarm about [privacy concerns](#) in many other countries—and serves as a reminder of how easily [technology companies](#) can leave supposedly private records exposed to global snoopers.

Gevers found that SenseNets, a Chinese facial recognition company, had left the database unprotected for months, exposing people's addresses, government ID numbers and more. After Gevers informed SenseNets of the leak, he said, the database became inaccessible.

"This system was open to the entire world, and anyone had full access to the data," said Gevers, noting that a system designed to maintain control over individuals could have been "corrupted by a 12-year-old."



In this Nov. 5, 2017, file photo, residents pass by a security checkpoint and surveillance cameras mounted on a street in Kashgar in western China's Xinjiang region. The Chinese database Victor Gevers found online was not just a collection of old personal details. The discovery by Gevers, a Dutch cybersecurity researcher who revealed it on Twitter last week, has given a rare glimpse into China's extensive surveillance of Xinjiang, a remote region home to an ethnic minority population that is largely Muslim. The area has been blanketed with police checkpoints and security cameras that apparently are doing more than just recording what happens. The database Gevers found appears to have been recording people's movements tracked by facial recognition technology, he said, logging more than 6.7 million coordinates in a span of 24 hours. (AP Photo/Ng Han Guan, File)

He said it included the coordinates of places where the individuals had recently been spotted by "trackers"—likely to be surveillance cameras. The stream indicated that the data is constantly being updated with information on people's whereabouts, he said in an interview over a messaging app.

Gevers posted a graph online showing that 54.9 percent of the individuals in the database were identified as Han Chinese, the country's ethnic majority, while 28.3 percent were Uighur and 8.3 percent were Kazakh, both Muslim ethnic minority groups.

A person who answered the phone at SenseNets declined a request for comment. The Xinjiang regional government did not respond to faxed questions.

Xinjiang, which borders central Asia in China's far west, has been subject to severe security measures in recent years as part of what the government says has been a successful program to quash extremist and separatist movements.

The U.S. and other countries have condemned the crackdown, in which an estimated 1 million Uighurs, Kazakhs and other Muslim minorities have been detained in internment camps that the government says are vocational training centers designed to rid the region of latent extremism.

Gulzia, an ethnic Kazakh woman who didn't want her last name used out of fear of retribution, said that cameras were being installed everywhere, even in cemeteries, in late 2017. Now living across the border in Kazakhstan, she told The Associated Press by phone on Monday that she had been confined to house arrest in China and taken to a police station, where they photographed her face and eyes and collected samples of her voice and fingerprints.

"This can be used instead of your ID card to identify you in the future," she said they told her. "Even if you get into an accident abroad, we'll recognize you."



In this Aug. 31, 2018, file photo, children play outside the entrance to a school ringed with barbed wire, barricades and surveillance cameras near a sign which reads: "Please use the nation's common language" indicating the use of Mandarin in Peyzawat, western China's Xinjiang region. The Chinese database Victor Gevers found online was not just a collection of old personal details. The discovery by Gevers, a Dutch cybersecurity researcher who revealed it on Twitter last week, has given a rare glimpse into China's extensive surveillance of Xinjiang, a remote region home to an ethnic minority population that is largely Muslim. The area has been blanketed with police checkpoints and security cameras that apparently are doing more than just recording what happens. The database Gevers found appears to have been recording people's movements tracked by facial recognition technology, he said, logging more than 6.7 million coordinates in a span of 24 hours. (AP Photo/Ng Han Guan, File)

The security clampdown is far heavier in Xinjiang than in most parts of China, though outside analysts and human rights activists have expressed concern that Xinjiang may be a testing ground for techniques that may be creeping into other parts of the country.

Joseph Atick, a pioneer in facial recognition technology, said that [facial recognition](#) products can use algorithms to recognize and track people in a crowd, but that privacy regulations in Europe, for example, make it much harder to launch a wide-scale application such as that of SenseNet.

"The technology around the world is becoming uniform and it is just the political climate that is different and leads to different applications," he said.

According to a company registry, SenseNets was founded in the southern China city of Shenzhen in 2015 and is majority-owned by Beijing-based NetPosa, a technology company specializing in [video surveillance](#). SenseNets' website showcases partnerships with police forces in Jiangsu and Sichuan provinces and the city of Shanghai.

A promotional video boasts about SenseNets' capacity to use facial and body recognition to track individuals' precise movements and identify them even in a crowded or chaotic setting. Another video on its website shows surveillance cameras zeroing in on the path of a runaway prisoner who ends up in an ailing relative's hospital room.

NetPosa's website says it has offices in Boston and Santa Clara, California. The website of NetPosa's U.S. subsidiary touts its products' use in urban anti-terrorism.

In recent years, NetPosa has been buying stakes in American surveillance startups such as Knightscope, a security robot maker. In 2017, NetPosa tried to buy the now-bankrupt California surveillance

camera maker Arecont, but later backed out, court records show.



In this Aug. 31, 2018, file photo, policemen patrol past a building's wall mounted with surveillance cameras in Peyzawat, western China's Xinjiang region. The Chinese database Victor Gevers found online was not just a collection of old personal details. The discovery by Gevers, a Dutch cybersecurity researcher who revealed it on Twitter last week, has given a rare glimpse into China's extensive surveillance of Xinjiang, a remote region home to an ethnic minority population that is largely Muslim. The area has been blanketed with police checkpoints and security cameras that apparently are doing more than just recording what happens. The database Gevers found appears to have been recording people's movements tracked by facial recognition technology, he said, logging more than 6.7 million coordinates in a span of 24 hours. (AP Photo/Ng Han Guan, File)

In 2010 U.S. chip maker Intel announced a strategic partnership with NetPosa and an Intel subsidiary bought a stake in the company, but

NetPosa said in 2015 that Intel had notified the Chinese company of its intent to divest its 4.4 percent stake by 2016.

Gevers said his discovery of the database presented an ethical dilemma. He is the co-founder of GDI Foundation, a Netherlands-based nonprofit that finds and informs entities of online security issues. He has become well-known in recent years for helping to uncover similarly exposed information on databases built with the open source MongoDB database program and left unsecured by their administrators.

GDI generally reports such discoveries to the entity that holds the information. Part of its mission is to remain neutral and not engage in political controversies.

Hours after he revealed his findings on Twitter, Gevers said, he learned that the system might be used to surveil Xinjiang's Muslim minority groups.

He said that made him "very angry."

"I could have destroyed that database with one command," he said. "But I choose not to play judge and executioner because it is not my place to do so."

© 2019 The Associated Press. All rights reserved.

Citation: Exposed Chinese database shows depth of surveillance state (2019, February 19) retrieved 7 May 2024 from

<https://techxplore.com/news/2019-02-exposed-chinese-database-depth-surveillance.html>

<p>This document is subject to copyright. Apart from any fair dealing for the purpose of private study or research, no part may be reproduced without the written permission. The content is provided for information purposes only.</p>
--