LinkNYC Internet Kiosks Being Set To Ubiquitous Surveillance

Hidden code discovered by accident reveal smart city Technocrats’ real purpose for the hundreds of kiosks, basically converting citizens into products as they are surveilled, tracked, hacked and packed into city streets. This is part of the Smart City strategy to implement Technocracy. TN Editor

LinkNYC kiosks have become a familiar eyesore to New Yorkers. Over 1,600 of these towering, nine-and-a-half-foot monoliths — their double-sided screens festooned with ads and fun facts — have been installed across the city since early 2016. Mayor Bill de Blasio has celebrated their ability to provide “the fastest and largest municipal Wi-Fi network in the world” as “a critical step toward a more equal, open, and connected city for every New Yorker, in every borough.”

Anyone can use the kiosks’ Android tablets to search for directions and services; they are also equipped with charging stations, 911 buttons, and phones for free domestic calls.

But even as the kiosks have provided important services to connect New Yorkers, they may also represent a troubling expansion of the city’s surveillance network, potentially connecting every borough to a new level of invasive monitoring. Each kiosk has three cameras, 30 sensors, and heightened sight lines for viewing above crowds.

Since plans for LinkNYC were first unveiled, journalists, residents, and civil liberties experts have raised concerns that the internet kiosks might be storing sensitive data about its users and possibly tracking their movements. For the last two years, the American Civil Liberties Union, Electronic Frontier Foundation, and a small but vocal group of activists — including ReThink LinkNYC, a grassroots anti-surveillance group, and the anonymous Stop LinkNYC coalition — have highlighted the kiosk’s potential to track locations, collect personal information, and fuel mass surveillance.

Now an undergraduate researcher has discovered indications in LinkNYC code — accidentally made public on the internet — that LinkNYC may be actively planning to track users’ locations.

You’re the Product

Plans to replace the city’s payphone booth network with Wi-Fi-enabled kiosks were first announced by de Blasio in 2014. Less than a year later, the city awarded a contract to a chameleon-like consortium of private companies known as CityBridge. It was an attractive deal: LinkNYC kiosks, at no cost to the city, would provide free internet coverage to anyone walking by. CityBridge, in turn, would be responsible for the installation, ownership, and construction of the devices, with plans to earn back its expenses through advertising. The twin 55-inch displays will eventually carry targeted ads derived from the information collected about kiosk users.

These terms raised alarms among internet researchers and privacy experts, who were quick to point out that nothing in life is truly free. “As we know,” Benjamin Dean, a technology policy analyst, told attendees at a New York hacking conference in 2016, “When you’re not paying, you’re not the customer — you’re the product.”

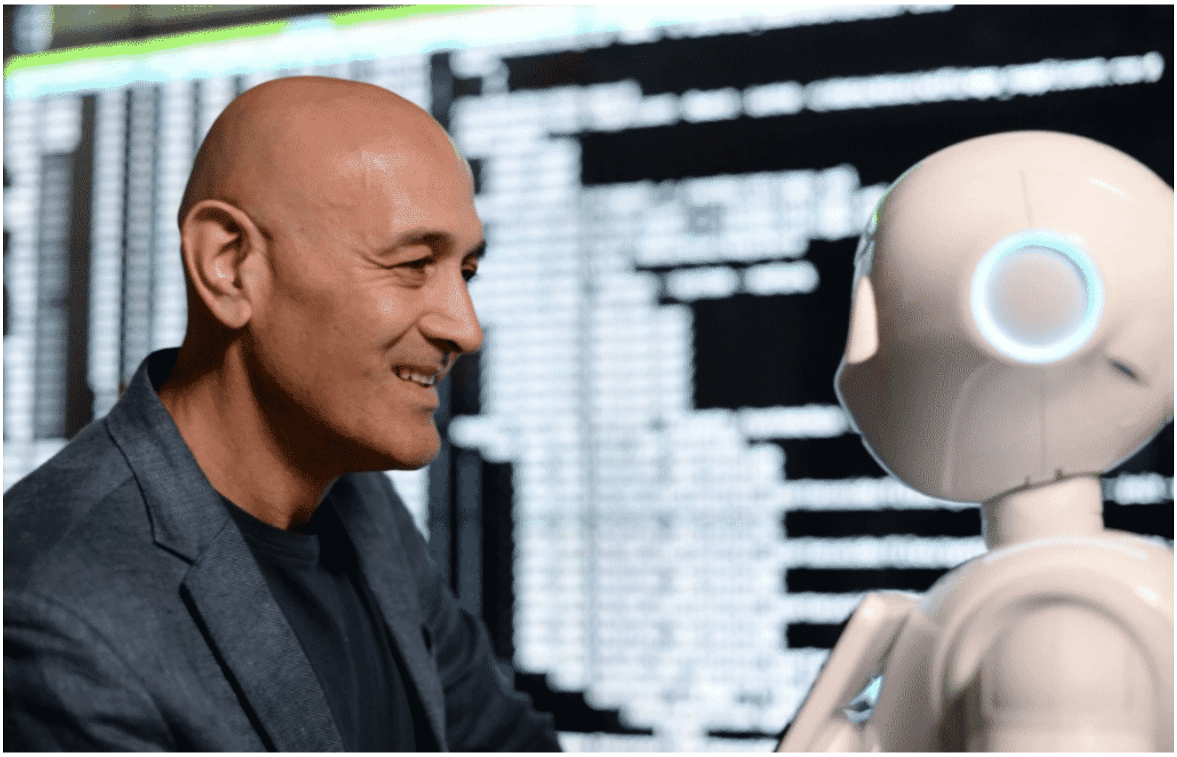
The key player in CityBridge is known as Intersection, and one of Intersection’s largest investors is Sidewalk Labs, with whom it also shares the same offices and staff. Sidewalk Labs CEO Daniel Doctoroff is the chair of Intersection’s board. Sidewalk Labs is owned by Google’s holding company, Alphabet Inc. In other words, the plan to blanket New York City with 7,500 camera-equipped obelisks has been largely underwritten by the company formerly known as Google — a corporation whose business model depends on selling your personal information to advertisers. As Doctoroff, who was also the city’s former deputy mayor of economic development, has said of the kiosks: “By having access to the browsing activity of people using the Wi-Fi — all anonymized and aggregated — we can actually then target ads to people in proximity and then obviously over time, track them through lots of different things, like beacons and location services, as well as their browsing activity. So in effect, what we’re doing is replicating the digital experience in physical space.”

In March 2016, the New York Civil Liberties Union raised multiple concerns with the mayor’s office about LinkNYC’s vast and indefinite data retention and the possibilities for unwarranted NYPD surveillance. The NYCLU asked whether environmental sensors and cameras would be hooked up to NYPD systems, including the Domain Awareness System (built by Microsoft). LinkNYC has since updated its policy to state that it will take reasonable efforts to notify users if their information is being shared with law enforcement.

In May of this year, Charles Meyers, an undergraduate at New York City College of Technology, came across folders in LinkNYC’s public library on GitHub, a platform for managing files and software, that appear to raise further questions about location tracking and the platform’s protection of its users’ data. Meyers made copies of the codebases in question — “LinkNYC Mobile Observation” and “RxLocation” — and shared both folders with The Intercept.

According to Meyers, the “LinkNYC Mobile Observation” code collects the user’s longitude and latitude, as well as the user’s browser type, operating system, device type, device identifiers, and full URL clickstreams (including date and time) and aggregates this information into a database. In Meyers’s view, this code — along with the functions of the “RxLocation” codebase — suggests that the company is interested in tracking the locations of Wi-Fi users in real time. If such code were run on a mobile app or kiosk, he said, the company would be able to make advertisements available in real time based on where and who someone was, and that this would constitute a potential violation of the company’s privacy policy. In 2016, LinkNYC’s privacy policy made it clear that it did not collect information about users’ precise locations. “However,” it states, “we know where we provide WiFi services, so when you use the services we can determine your general location.”

Read full story here…



Head Of British Science Ass’n: AI Greater Concern Than Terrorism Or Climate Change

Many Technocrats who are inventing AI solutions insist that AI will create more jobs than it replaces. Other Technocrats offer Universal Basic Income as a solution to certain displacement. Common sense says AI is a certain train wreck just waiting to happen. Who will you believe? TN Editor

Artificial Intelligence is a greater concern than antibiotic resistance, climate change or terrorism for the future of Britain, the incoming president of the British Science Association has warned.

Jim Al-Khalili, Professor of physics and public engagement at the University of Surrey, said the unprecedented technological progress in AI was ‘happening too fast’ without proper scrutiny or regulation.

Prof Al-Khalili warned that the full threat to jobs and security had not been properly assessed and urged the government to urgently regulate.

Speaking at a briefing in London ahead of the British Science Festivalin Hull next week, he said: “Until maybe a couple of years ago had I been asked what is the most pressing and important conversation we should be having about our future, I might have said climate change or one of the other big challenges facing humanity, such as terrorism, antimicrobial resistance, the threat of pandemics or world poverty.

“But today I am certain the most important conversation we should be having is about the future of AI. It will dominate what happens with all of these other issues for better or for worse.

“If Russian cyber hackers were able to meddle with the 2016 US elections, then what is stopping cyber terrorists from hacking into any future AI controlled power grids, transport systems, banks of military installations.

“Our government has a responsibility to protect society from potential threats and risks.”

Dubbed the Fourth Industrial Revolution, artificial intelligence and robotics have improved exponentially in recent years with British companies like DeepMind leading the way in developing intricate neural networks previously thought impossible.

However last week the Bank of England warned that ‘large swathes’ of Britain’s workforce is now under threat of unemployment as robots and algorithms take over jobs.

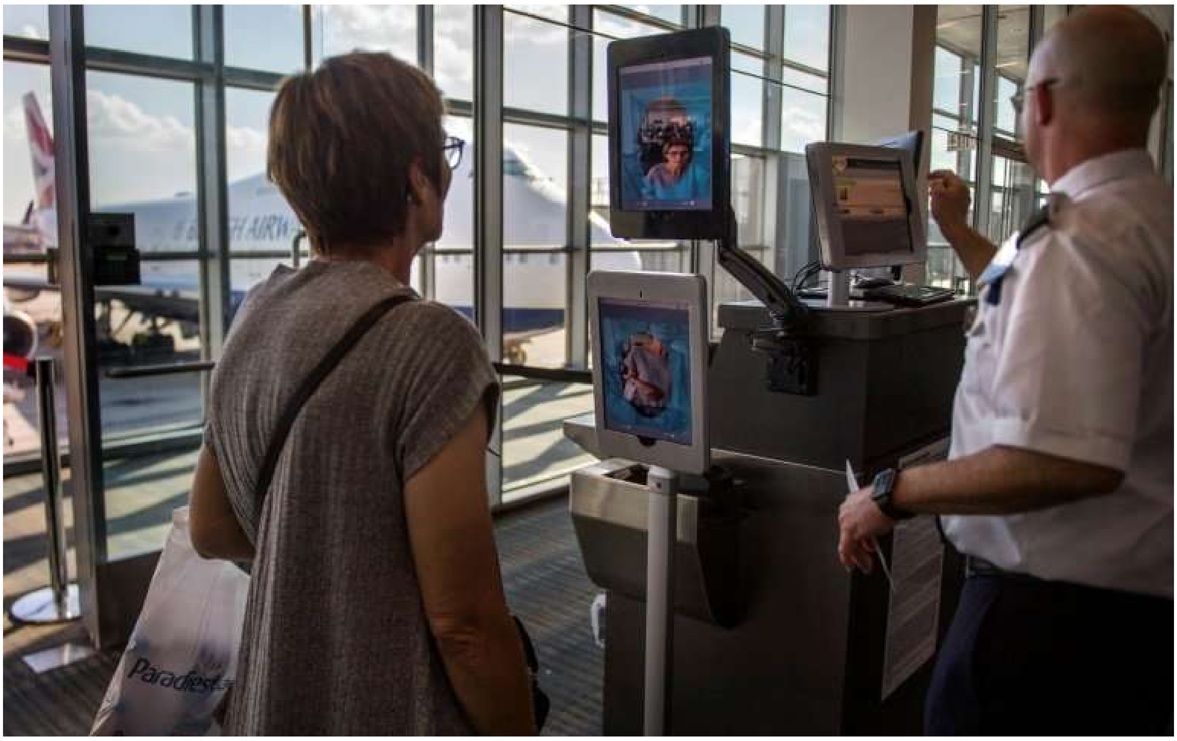
Even industries previously thought immune, such as creative writing, are now being replaced by artificially intelligent programmes and earlier this month M&S announced it was replacing call centre staff with AI.

Prof Al-Khalili added: “Many people are becoming increasingly nervous about what they see as unchecked progress in AI.

“There are valid concerns about the widespread implementation of AI leading to an increase in inequality. Robotics and autonomous systems are predicted to bring about job losses, primarily affecting workers in low-skilled roles, and there is still little research on how the future effects of automation might vary across the UK.

“We are now seeing an unprecedented level of interest, investment and technological progress in the field, which many people, including myself, feel is happening too fast.”

Read full story here…



TSA Bringing Facial Recognition To Airports As ‘User Friendly’

Technocrats at the TSA have no regard for privacy or for their contribution to the creation of a police state. Their sales pitch stresses convenience and speed of check in. However, if TSA has not already created a convoluted system in the first place, such convenience would be moot. Nevertheless, the TSA says, “we believe it will change the face of international travel.” □ TN Editor

As facial recognition technology use generates intense scrutiny, a new system unveiled at Washington’s Dulles airport is being touted as a “user friendly” way to help ease congestion for air travelers.

Officials at Dulles unveiled two new face recognition systems Thursday, one to meet legal requirements for biometric entry-exit records, and a second to help speed processing of travelers arriving on international flights by matching their real-time images with stored photos.

The growing use of facial recognition has ignited debate over surveillance and privacy around the world, but officials told media this system was a way to help reducing annoying lines and wait times without compromising security.

"The technology works," US Customs and Border Protection Commissioner Kevin McAleenan told reporters at an airport unveiling.

"It's fast, it's user-friendly, it's flexible and it's cost-effective. And we believe it will change the face of international travel."

Over time, officials say the biometric recognition system will allow a traveler's face to eliminate the need for a boarding pass.

"No more fumbling with your boarding pass when you have two carry-ons, maybe a kid, no more trying to find a QR code or trying the refresh your screen," McAleenan said.

In one test for the system, McAleenan said the boarding 350 passengers for an Airbus A380 aircraft was completed in 20 minutes, or half the normal time.

At Dulles, officials showed how the new systems, operated with iPads mounted on poles, identified and matched the image of travelers during the boarding process.

Aiming for speed, security

The system is designed to boost security by ensuring that travelers are using their real passports and not forged documents, matching to existing photos from passports or images collected from foreign nationals when they enter.

The Dulles system began operations in mid-August, ahead of the media event, and within three days was credited with the arrest of a man attempting to use a fake passport to enter the United States.

Read full story here…