U.S. Surveillance Tech Is Propping Up Authoritarian Regimes

This article is correct to state: “But if human rights concerns aren’t enough to move U.S. policymakers, there’s another reason to act: Exporting surveillance equipment enables digital authoritarianism and hurts U.S. national interests.” However, TN readers know that Technocrats don’t care about U.S. national interests! TN Editor

NSO Group, an Israeli cyberintelligence firm, makes spyware that it sells to a variety of government clients around the world. It has denied that those surveillance products were involved in the torture and murder of Washington Post journalist Jamal Khashoggi, although it has neither confirmed nor denied selling its products to the Saudi government — elements of which, the CIA has concluded, ordered the killing.

That may raise eyebrows, but this intermingling of privately sold technology and authoritarian regimes is hardly an outlier. Throughout the world, despots are also probably monitoring Internet traffic, communications and behavior — in many cases using surveillance technology supplied by U.S. and other Western companies.

Take, for instance, recent reporting: The U.S. firm Gatekeeper Intelligent Security sold facial-recognition technology to the Saudi government. The system identifies the faces of drivers and passengers in cars, even with blacked-out or tinted windows. The technology has also been sold to regimes in the United Arab Emirates, and "when combined with facial recognition and number-plate readers," Forbes wrote, "it's designed to help authorities track individuals of interest." This is only the latest in reports about Western firms selling surveillance technology to authoritarian regimes.

From facial recognition software to GPS trackers to computer hacking tools to systems that monitor and redirect flows of Internet traffic, contemporary surveillance technologies enable "high levels of social control at a reasonable cost," as Nicholas Wright puts it in Foreign Affairs. But these technologies don't just aid and enable what Wright and other policy analysts have called "digital authoritarianism." They also promote a sovereign and controlled model of the Internet, one characterized by frequent censorship, pervasive surveillance and tight control by the state. The United States could be a world leader in preventing the spread of this Internet model, but to do so, we must reevaluate the role U.S. companies play in contributing to it.

One way to address the spread of these tools head on is the use of export controls. Such policies have been in the news more than usual recently, not least because the Trump administration has pushed to tighten regulations on American export of emerging technologies such as the chips used in supercomputers that develop artificial intelligence. The administration's proposed controls would place new limits on what kinds of technology can be sold and to whom. But when it comes to preventing export of surveillance technology to human rights abusers, the United States lags behind, particularly when it comes to Internet-based surveillance equipment.

Initial movement to prevent the spread of this type of surveillance equipment came through the 2013 Wassenaar Arrangement, a 41-member multilateral arms-control agreement in which the United States participates. The primary goal of the Wassenaar Arrangement was and still is to limit the sale and trafficking of dual-use technologies — those

that could have both a civilian and military use. For instance, network penetration software — digital tools used to break into a wireless or physical network — is used by security researchers to probe for vulnerabilities just as it's used by governments and militaries to intercept enemy communications. The Wassenaar Arrangement is not a treaty and therefore lacks binding power, but member states agree to establish and enforce export controls on items on the arrangement control list, which is updated every December.

One of the December 2013 additions to the control list was "IP network communications surveillance systems." These are systems that classify, collect and can inspect all the digital traffic flowing through a network — what a hacker might use to intercept your email login at a coffee shop, or what a government might use to track the online activities of activists, at scale. Governments entered into negotiations on the Wassenaar Arrangement with a clearly defined human rights goal in mind: preventing despots and bad actors from obtaining technology that they could use to commit abuses domestically. Most Wassenaar participants, including every country in the European Union, have restricted the distribution of this technology. The United States, on the other hand, has not.

The sale of technologies such as spyware and facial-recognition systems to human rights abusers — which Wassenaar ventured to stop — enables insidious social control and encroachment on basic civil liberties. But if human rights concerns aren't enough to move U.S. policymakers, there's another reason to act: Exporting surveillance equipment enables digital authoritarianism and hurts U.S. national interests.

Read full story here…

The Brave New World Of Surveillance Capitalism

Unchecked surveillance-for-profit is upon us, but is driven as much by Technocracy as by Capitalism itself. Technocrats are data-hoarders who can never get enough data nor exhaust their drive for analysis of collected data. TN Editor

Certain radical critiques of capitalism posit that it must necessarily monetize everything in time. The basic argument is that capitalism inherently requires infinite economic growth to function properly, but we are in a world of finite resources. As traditional resources used to feed the furnace are exhausted, more aspects of life that were previously outside of the money economy must be drawn into it – including abstract things like behavior, relationships and even thoughts.

The merits of such theories are debatable. What is beyond debate is that human thoughts and relationships are already in the advanced stages of monetization. Prof. Shoshana Zuboff, a leading expert in the field of business administration in information technology settings since the 1980s, coined the idea of "surveillance capitalism" (in the April 2015 edition of the Journal of Information Technology) to describe this

phenomenon – the observation and recording of as much personal data as possible to create highly effective targeted advertisements.

Surveillance capitalism and privacy

Google is one of the best and oldest examples of surveillance capitalism in action. Their ostensibly "free" services, like Search and Gmail, have always been monetized by the data they collect from users. Same story with Facebook. These systems are opaque at best for the end user. You can never be entirely sure exactly what or how much data they're collecting, how detailed a personal profile they're building on you, what it is being used for or whose hands it is passing through. Thus the "surveillance" aspect – it's as if you have hidden cameras recording you all the time as you move about virtual space.

The purpose of all this is nothing more sinister than advertising. The deeper a marketing company can get inside your head, the more effectively they can advertise to you. The lack of regard for personal privacy and fair disclosure in this process has always been troubling, but most of the tech companies that have surveillance capitalism as their central revenue model are simply concerned with making money by selling things in the most ruthlessly efficient way possible.

Unfortunately, that isn't the only way in which this technology can be used.

The extremes of surveillance capitalism

While surveillance capitalism for marketing purposes is creepy, it becomes truly dangerous when these tools and database assets wind up in the hands of political actors with bad intentions.

One familiar example is the use of targeted advertising by foreign intelligence agencies to sow political and social unrest. The Internet Research Agency, a notorious Russia-based "troll farm", has been linked to at least 270 fake Facebook accounts purporting to be tied to American

social movements. These fake groups, with names like “Aztlan Warriors” and “Black Elevation”, not only fomented dissent by spreading misinformation online but managed to remotely organize actual meetings and protests in American cities. The Internet Research Agency was found to have purchased at least 3,500 targeted Facebook ads to draw users into their groups.

Of course, these techniques have been employed in domestic politics as well. Cambridge Analytica’s illicit access to the data of 87 million Facebook users was put to use in targeted ad campaigns in the 2016 presidential election in the United States. In other countries, it has been put to use in propping up authoritarian regimes by profiling dissidents, magnifying cults of personality and organizing smear campaigns.

Read full story here…

Home Tech Is Getting Smarter

And Creepier

With every new Smart Home device installed, more information about you is being secretly collected, categorized, analyzed and sold. 'Decentralized surveillance' provides a pool of data that can be used to manipulate human behavior. TN Editor

One day, finding an oven that just cooks food may be as tough as buying a TV that merely lets you change channels.

Internet-connected "smarts" are creeping into cars, refrigerators, thermostats, toys and just about everything else in your home. CES 2019, the gadget show opening Tuesday in Las Vegas, will showcase many of these products, including an oven that coordinates your recipes and a toilet that flushes with a voice command.

With every additional smart device in your home, companies are able to gather more details about your daily life. Some of that can be used to help advertisers target you — more precisely than they could with just the smartphone you carry.

"It's decentralized surveillance," said Jeff Chester, executive director for the Center for Digital Democracy, a Washington-based digital privacy advocate. "We're living in a world where we're tethered to some online service stealthily gathering our information."

Yet consumers so far seem to be welcoming these devices. The research firm IDC projects that 1.3 billion smart devices will ship worldwide in 2022, twice as many as 2018.

Companies say they are building these products not for snooping but for convenience, although Amazon, Google and other partners enabling the intelligence can use the details they collect to customize their services and ads.

Whirlpool, for instance, is testing an oven whose window doubles as a display. You'll still be able to see what's roasting inside, but the glass can now display animation pointing to where to place the turkey for

optimal cooking.

The oven can sync with your digital calendar and recommend recipes based on how much time you have. It can help coordinate multiple recipes, so that you're not undercooking the side dishes in focusing too much on the entree. A camera inside lets you zoom in to see if the cheese on the lasagna has browned enough, without opening the oven door.

As for that smart toilet, Kohler's Numi will respond to voice commands to raise or lower the lid — or to flush. You can do it from an app, too. The company says it's all about offering hands-free options in a setting that's very personal for people. The toilet is also heated and can play music and the news through its speakers.

Kohler also has a tub that adjusts water temperature to your liking and a kitchen faucet that dispenses just the right amount of water for a recipe.

For the most part, consumers aren't asking for these specific features. After all, before cars were invented, people might have known only to ask for faster horses. "We try to be innovative in ways that customers don't realize they need," Samsung spokesman Louis Masses said.

Whirlpool said insights can come from something as simple as watching consumers open the oven door several times to check on the meal, losing heat in the process.

"They do not say to us, 'Please tell me where to put (food) on the rack, or do algorithm-based cooking,'" said Doug Searles, general manager for Whirlpool's research arm, WLabs. "They tell us the results that are most important to them."

Samsung has several voice-enabled products, including a fridge that comes with an app that lets you check on its contents while you're grocery shopping. New this year: Samsung's washing machines can send alerts to its TVs — smart TVs, of course — so you know your laundry is ready while watching Netflix.

Other connected items at CES include:

— a fishing rod that tracks your location to build an online map of where you've made the most catches.

— a toothbrush that recommends where to brush more.

— a fragrance diffuser that lets you control how your home smells from a smartphone app.

These are poised to join internet-connected security cameras, door locks and thermostats that are already on the market. The latter can work with sensors to turn the heat down automatically when you leave home.

Read full story here…

Amazon Ring Security Cameras Present Oxymoron

Your unencrypted and unprotected Ring video stream is openly available to Ring staffers in Ukraine, and to others who can discover your email address. Technocrats have no ethical boundaries or concern for the

rights of others when it comes to data. TN Editor

The “Smart Home” of the 21st century isn’t just supposed to be a monument to convenience, we’re told, but also to protection, a Tony Stark-like bubble of vigilant algorithms and internet-connected sensors working ceaselessly to watch over us. But for some who’ve welcomed in Amazon’s Ring security cameras, there have been more than just algorithms watching through the lens, according to sources alarmed by Ring’s dismal privacy practices.

Ring has a history of lax, sloppy oversight when it comes to deciding who has access to some of the most precious, intimate data belonging to any person: a live, high-definition feed from around — and perhaps inside — their house. The company has marketed its line of miniature cameras, designed to be mounted as doorbells, in garages, and on bookshelves, not only as a means of keeping tabs on your home while you’re away, but of creating a sort of privatized neighborhood watch, a constellation of overlapping camera feeds that will help police detect and apprehend burglars (and worse) as they approach. “Our mission to reduce crime in neighborhoods has been at the core of everything we do at Ring,” founder and CEO Jamie Siminoff wrote last spring to commemorate the company’s reported $1 billion acquisition payday from Amazon, a company with its own recent history of troubling facial recognition practices. The marketing is working; Ring is a consumer hit and a press darling.

Despite its mission to keep people and their property secure, the company’s treatment of customer video feeds has been anything but, people familiar with the company’s practices told The Intercept. Beginning in 2016, according to one source, Ring provided its Ukraine-based research and development team virtually unfettered access to a folder on Amazon’s S3 cloud storage service that contained every video created by every Ring camera around the world. This would amount to an enormous list of highly sensitive files that could be easily browsed and viewed. Downloading and sharing these customer video files would have required little more than a click. The Information, which has aggressively covered Ring’s security lapses, reported on these practices last month.

At the time the Ukrainian access was provided, the video files were left unencrypted, the source said, because of Ring leadership's "sense that encryption would make the company less valuable," owing to the expense of implementing encryption and lost revenue opportunities due to restricted access. The Ukraine team was also provided with a corresponding database that linked each specific video file to corresponding specific Ring customers.

At the same time, the source said, Ring unnecessarily provided executives and engineers in the U.S. with highly privileged access to the company's technical support video portal, allowing unfiltered, round-the-clock live feeds from some customer cameras, regardless of whether they needed access to this extremely sensitive data to do their jobs. For someone who'd been given this top-level access — comparable to Uber's infamous "God mode" map that revealed the movements of all passengers — only a Ring customer's email address was required to watch cameras from that person's home. Although the source said they never personally witnessed any egregious abuses, they told The Intercept "if [someone] knew a reporter or competitor's email address, [they] could view all their cameras." The source also recounted instances of Ring engineers "teasing each other about who they brought home" after romantic dates. Although the engineers in question were aware that they were being surveilled by their co-workers in real time, the source questioned whether their companions were similarly informed.

Ring's decision to grant this access to its Ukraine team was spurred in part by the weaknesses of its in-house facial and object recognition software. Neighbors, the company's disarming name for its distributed residential surveillance platform, is now a marquee feature for Ring's cameras, billed as a "proactive" neighborhood watch. This real-time crime-fighting requires more than raw video — it requires the ability to make sense, quickly and at a vast scale, of what's actually happening in these household video streams. Is that a dog or your husband? Is that a burglar or a tree? Ring's software has for years struggled with these fundamentals of object recognition. According to the most recent Information report, "Users routinely complained to customer support about receiving alerts when nothing noteworthy was happening at their

front door; instead, the system seemed to be detecting a car driving by on the street or a leaf falling from a tree in the front yard."

Computer vision has made incredible strides in recent years, but creating software that can categorize objects from scratch is often expensive and time-consuming. To jump-start the process, Ring used its Ukrainian "data operators" as a crutch for its lackluster artificial intelligence efforts, manually tagging and labeling objects in a given video as part of a "training" process to teach software with the hope that it might be able to detect such things on its own in the near future. This process is still apparently underway years later: Ring Labs, the name of the Ukrainian operation, is still employing people as data operators, according to LinkedIn, and posting job listings for vacant video-tagging gigs: "You must be able to recognize and tag all moving objects in the video correctly with high accuracy," reads one job ad. "Be ready for rapid changes in tasks in the same way as be ready for long monotonous work."

Read full story here...

UPDATE: AT&T Stops Selling Location Data Amid Calls For Fed Investigation

AT&T was caught red handed and exposed this week by Motherboard. for selling customer location data, an egregious violation of privacy laws. Today, AT&T says they have stopped selling data because they now know a Federal investigation is being ramped up. If history is a guide, AT&T will resume selling after the heat and attention have passed. AT&T is a classic example of Technocracy in action. TN Editor

AT&T said Thursday that it will stop selling its customers' location data to third-party service providers after a report this week said the information was winding up in the wrong hands.

The announcement follows sharp demands by federal lawmakers for an investigation into the alleged misuse of data, which came to light when Motherboard revealed a complex chain of unauthorized information sharing that ended with a bounty hunter successfully tracking down a reporter's device.

AT&T had already suspended its data-sharing agreements with a number of so-called "location aggregators" last year in light of a congressional probe finding that some of Verizon's location data was being misused by prison officials to spy on innocent Americans. AT&T also said at the time that it would be maintaining those of its agreements that provided clear consumer benefits, such as location sharing for roadside assistance services.

But AT&T's announcement Thursday goes much further, pledging to terminate all of the remaining deals it had – even the ones that it said were actively helpful.

"In light of recent reports about the misuse of location services, we have decided to eliminate all location aggregation services – even those with clear consumer benefits," AT&T said in a statement. "We are

immediately eliminating the remaining services and will be done in March."

In characteristic fashion, T-Mobile CEO John Legere tweeted Tuesday that his firm would be "completely ending location aggregator work" in March. Verizon said in a statement Thursday that it, too, was winding down its four remaining location-sharing agreements, which are all with roadside assistance services – after that, customers would have to give the company permission to share their data with roadside assistance firms. A Sprint spokeswoman didn't immediately respond to a request for comment.

The announcements reflect a major victory for privacy advocates who have slammed corporate America over its handling of consumers' personal information, often to their personal and economic expense.

"Carriers are always responsible for who ends up with their customers' data – it's not enough to lay the blame for misuse on downstream companies," said Sen. Ron Wyden (D., Ore.) in a statement. "The time for taking these companies at their word is long past. Congress needs to pass strong legislation to protect Americans' privacy and finally hold corporations accountable when they put your safety at risk by letting stalkers and criminals track your phone on the dark web."

Other critics said Americans have an "absolute right" to their privacy of their data.

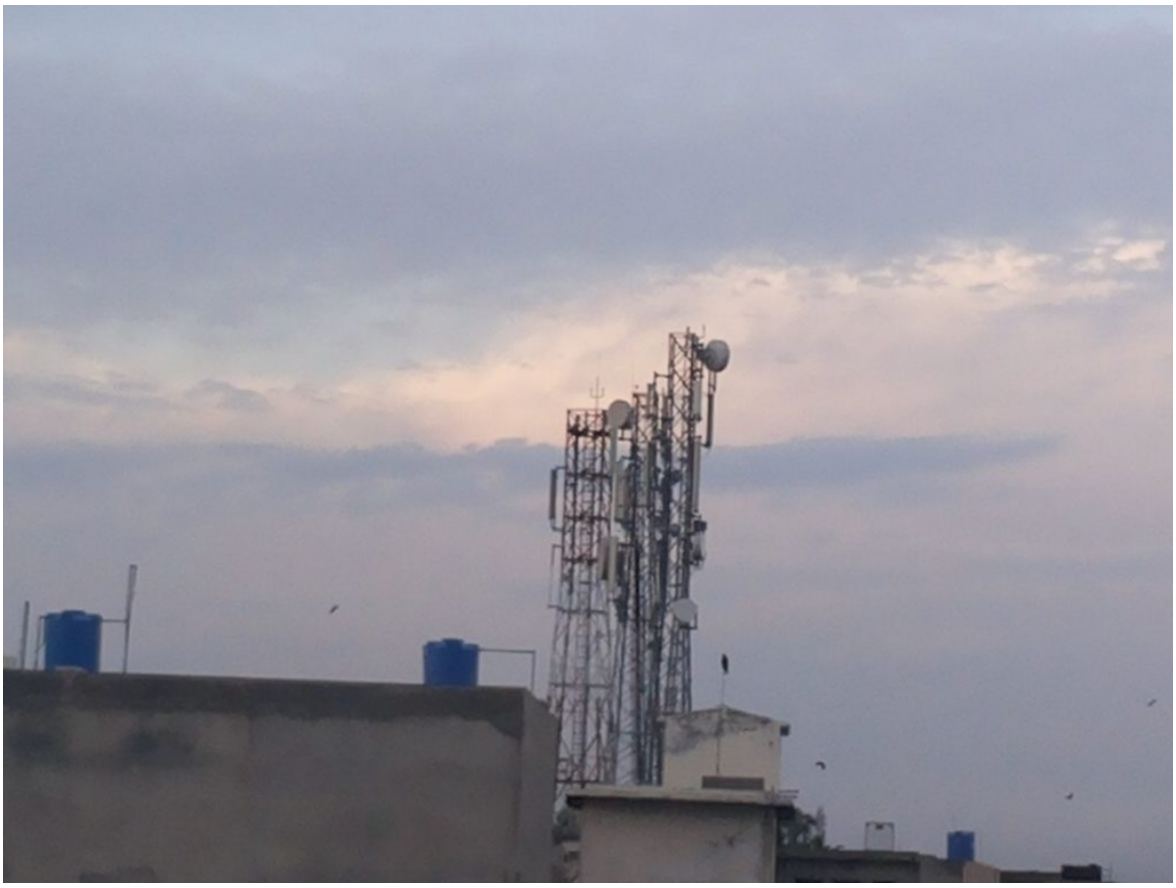
"I'm extraordinarily troubled by reports of this system of repackaging and reselling location data to unregulated third-party services for potentially nefarious purposes," Sen. Kamala Harris (D., Calif.) said in a statement after the Motherboard report was published. "If true, this practice represents a legitimate threat to our personal and national security."

Harris called on the Federal Communications Commission to immediately open an investigation.

Motherboard reported that major U.S. wireless carriers T-Mobile, AT&T, and Sprint have been selling the location data of their customers in an

unregulated market in which Americans' personal information travels through several layers of third-party entities that buy the location data but are not authorized to handle such information.

Read full story here...



How T-Mobile, Sprint & AT&T Sell Your Smartphone Geo-Location Data

Are you happy that every Tom, Dick and Harry in the world can pinpoint your location and track your whereabouts like the CIA? Mega-carriers apparently gain huge profits by selling your location data to private, and often shady, data mining companies, who in turn sell it to others. This

makes mockery of every privacy agreement ever offered by these companies. TN Editor

T-Mobile, Sprint, and AT&T are selling access to their customers' location data, and that data is ending up in the hands of bounty hunters and others not authorized to possess it, letting them track most phones in the country.

Nervously, I gave a bounty hunter a phone number. He had offered to geolocate a phone for me, using a shady, overlooked service intended not for the cops, but for private individuals and businesses. Armed with just the number and a few hundred dollars, he said he could find the current location of most phones in the United States.

The bounty hunter sent the number to his own contact, who would track the phone. The contact responded with a screenshot of Google Maps, containing a blue circle indicating the phone's current location, approximate to a few hundred metres.

Queens, New York. More specifically, the screenshot showed a location in a particular neighborhood—just a couple of blocks from where the target was. The hunter had found the phone (the target gave their consent to Motherboard to be tracked via their T-Mobile phone.)

The bounty hunter did this all without deploying a hacking tool or having any previous knowledge of the phone's whereabouts. Instead, the tracking tool relies on real-time location data sold to bounty hunters that ultimately originated from the telcos themselves, including T-Mobile, AT&T, and Sprint, a Motherboard investigation has found. These surveillance capabilities are sometimes sold through word-of-mouth networks.

Whereas it's common knowledge that law enforcement agencies can track phones with a warrant to service providers, IMSI catchers, or until recently via other companies that sell location data such as one called Securus, at least one company, called Microbilt, is selling phone geolocation services with little oversight to a spread of different private industries, ranging from car salesmen and property managers to bail bondsmen and bounty hunters, according to sources familiar with the

company's products and company documents obtained by Motherboard. Compounding that already highly questionable business practice, this spying capability is also being resold to others on the black market who are not licensed by the company to use it, including me, seemingly without Microbilt's knowledge.

Motherboard's investigation shows just how exposed mobile networks and the data they generate are, leaving them open to surveillance by ordinary citizens, stalkers, and criminals, and comes as media and policy makers are paying more attention than ever to how location and other sensitive data is collected and sold. The investigation also shows that a wide variety of companies can access cell phone location data, and that the information trickles down from cell phone providers to a wide array of smaller players, who don't necessarily have the correct safeguards in place to protect that data.

"People are reselling to the wrong people," the bail industry source who flagged the company to Motherboard said. Motherboard granted the source and others in this story anonymity to talk more candidly about a controversial surveillance capability.

Your mobile phone is constantly communicating with nearby cell phone towers, so your telecom provider knows where to route calls and texts. From this, telecom companies also work out the phone's approximate location based on its proximity to those towers.

Although many users may be unaware of the practice, telecom companies in the United States sell access to their customers' location data to other companies, called location aggregators, who then sell it to specific clients and industries. Last year, one location aggregator called LocationSmart faced harsh criticism for selling data that ultimately ended up in the hands of Securus, a company which provided phone tracking to low level enforcement without requiring a warrant. LocationSmart also exposed the very data it was selling through a buggy website panel, meaning anyone could geolocate nearly any phone in the United States at a click of a mouse.

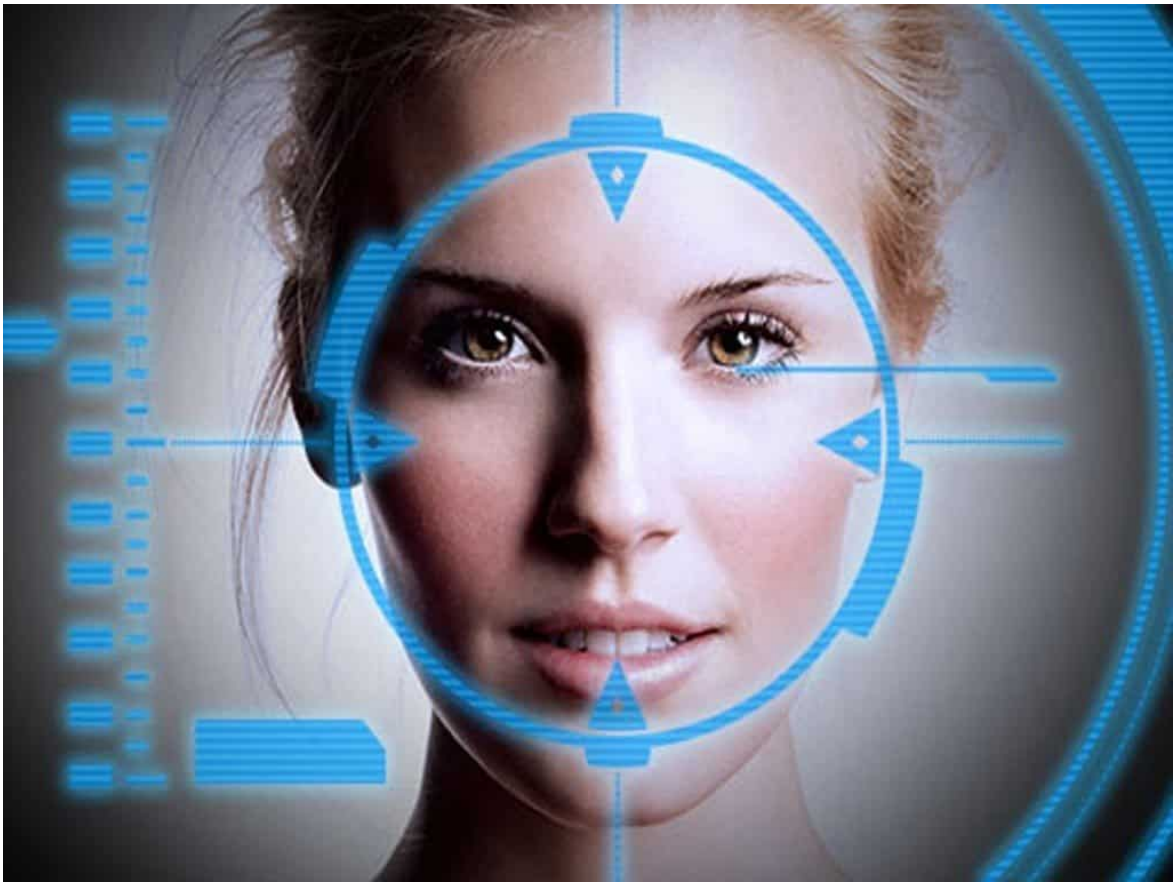
There's a complex supply chain that shares some of American cell phone

users' most sensitive data, with the telcos potentially being unaware of how the data is being used by the eventual end user, or even whose hands it lands in. Financial companies use phone location data to detect fraud; roadside assistance firms use it to locate stuck customers. But AT&T, for example, told Motherboard the use of its customers' data by bounty hunters goes explicitly against the company's policies, raising questions about how AT&T allowed the sale for this purpose in the first place.

"The allegation here would violate our contract and Privacy Policy," an AT&T spokesperson told Motherboard in an email.

In the case of the phone we tracked, six different entities had potential access to the phone's data. T-Mobile shares location data with an aggregator called Zumigo, which shares information with Microbilt. Microbilt shared that data with a customer using its mobile phone tracking product. The bounty hunter then shared this information with a bail industry source, who shared it with Motherboard.

Read full story here…



Technocrat Survey Shows American Approval Of Facial Recognition Tech

Surveys are propaganda, vary widely with the nature of questions asked, and yet are then compared to other studies to demonstrate trends. Just watch to see who promotes or demotes a given survey and you will determine who has an axe to grind. TN Editor

A growing number of Americans are OK with the facial recognition technology, especially if it increases public safety, according to a national survey released Monday.

Conducted on a national poll of 3,151 U.S. adults in December, the survey found only one in four Americans believe the federal government should strictly limit the use of facial biometrics technology.

The survey also indicates Americans are more likely to support any

apparent tradeoff to their own privacy caused by facial recognition technology if it benefits law enforcement, reduces shoplifting or speeds up airport security lines.

Only 18 percent of those polled said they agreed with strict limitations on facial recognition tech if it comes at the expense of public safety, compared to 55 percent who disagreed with such limitations.

“People are often suspicious of new technologies, but in this case, they seem to have warmed up to facial recognition technology quite quickly,” said Daniel Castro, director of the Center for Data Innovation, a nonprofit, nonpartisan research institute that conducted the survey.

“Perhaps most importantly, Americans have made it clear they do not want regulations that limit the use of facial recognition if it comes at the cost of public safety,” Castro said.

The findings indicate a potential shift in public thinking.

A September 2018 study by the Brookings Institution found half of Americans favored limitations of the use of facial recognition by law enforcement, while 42 percent felt it invaded personal privacy rights.

Further, Americans appear more comfortable with facial recognition as its accuracy improves. The Center for Data Innovation survey found 59 percent of Americans agree with the use of facial recognition technology if the software is right 100 percent of the time compared to 39 percent who agreed with the technology if it is right 80 percent of the time.

“The survey results suggest that one of the most important ways for police to gain public support for using facial recognition technology in their communities is to use the most accurate tools available,” said Castro. “People are willing to get behind police use of facial recognition technology as long as it is accurate and makes their communities safer.”

Read full story here…

Amazon Convinces FBI To Try Its Facial-Recognition Software

After being lashed by its own employees for selling facial recognition software to law enforcement, Technocrat Jeff Bezos doubled-down on his efforts to penetrate all levels of government, the FBI being the latest win. TN Editor

The software allows the FBI to go through video surveillance footage much faster than agents can.

The FBI is piloting Amazon's facial matching software—Amazon Rekognition—as a means to sift through mountains of video surveillance footage the agency routinely collects during investigations.

The pilot kicked off in early 2018 following a string of high-profile counterterrorism investigations that tested the limits of the FBI's technological capabilities, according to FBI officials.

For example, in the 2017 mass shooting in Las Vegas carried out by

Stephen Paddock, the law enforcement agency collected a petabyte worth of data, much of it video from cellphones and surveillance cameras.

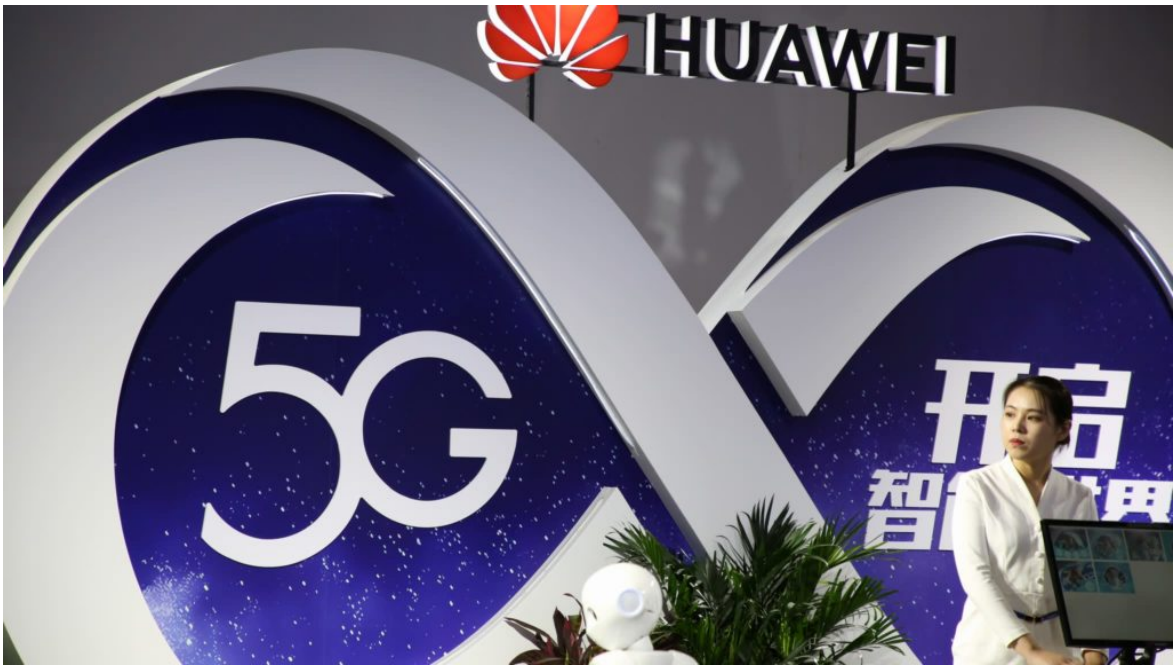
“We had agents and analysts, eight per shift, working 24/7 for three weeks going through the video footage of everywhere Stephen Paddock was the month leading up to him coming and doing the shooting,” said FBI Deputy Assistant Director for Counterterrorism Christine Halvorsen.

Halvorsen made those remarks in November at the Amazon Web Services re:Invent conference in Las Vegas, where she described how the FBI is using Amazon’s cloud platforms to carry out counterterrorism investigations. She said Amazon Rekognition could have gone through the same trove of data from the Las Vegas shooting “in 24 hours”—or three weeks faster than it took human FBI agents to find every instance of Paddock’s face in the mountain of video.

“Think about that,” Halvorsen said, noting that technology like Amazon Rekognition frees up FBI agents and analysts to apply their skills to other aspects of the investigation or other cases.

“The cases don’t stop, the threats keep going,” Halvorsen added. “Being able to not pull people off that and have computers do it is very important.”

Read full story here…



Huawei: Doors Are Slamming Shut Around The World

Chinese Technocrats are experiencing isolation as Huawei is falling out of favor in the West due to its surveillance connections to the Chinese government. This will press China closer to military warfare. TN Editor

Huawei is coming under pressure in two more key European markets — the latest in a series of problems the Chinese company faces around the world.

Telecommunications firm Orange has ruled out using Huawei products in its core 5G network in France, and Germany's Deutsche Telekom says it's reviewing purchases of Huawei equipment.

The Chinese company, which sells smartphones and telecommunications gear, faces increased scrutiny in the United States and other countries, where officials have warned of potential national security risks from using Huawei products.

The recent arrest of its chief financial officer, Meng Wanzhou, has raised additional questions about Huawei. Meng has been released on bail in

Canada, but she now faces a lengthy legal battle over whether she should be extradited to the United States, where prosecutors accuse her of helping Huawei get around sanctions on Iran.

This newspaper explains the Middle East to international audiences
Situating the headquarters of this regional newspaper in a hub that skillfully combines education, business, creativity and innovation helps it compete.

Huawei's CFO is out on bail, but the crisis sparked by her arrest is snowballing Orange (ORAN), the largest telecoms operator in France, on Friday ruled out using Huawei equipment in its core 5G network in the country.

"We don't foresee calling on Huawei for 5G," Orange CEO Stephane Richard said Friday. "We are working with our traditional partners — they are Ericsson and Nokia."

Meanwhile, Deutsche Telekom (DTEGY) said it was taking the discussion about the security of network elements from Chinese manufacturers "very seriously."

"We are pursuing a multi-vendor strategy for the network elements used (manufacturers primarily Ericsson, Nokia, Cisco, Huawei)," it said in a statement. "Nevertheless we currently reevaluate our procurement strategy."

Huawei did not immediately respond to a request for comment sent outside business hours in China.

The announcement from Deutsche Telekom — coupled with news from SoftBank this week that it might also drop Huawei equipment — could also factor into the pending merger between T-Mobile (TMUS) and Sprint (S). Deutsche Telekom is majority owner of T-Mobile while Softbank owns Sprint.

Reuters reported Friday that the deal between the two US phone companies could now get approval from federal regulators who vet deals for national security risks. According to Reuters, the use of Huawei

equipment has been part of the review.

Read full story here…

Is Amazon The Embodiment Of Orwellian Surveillance?

Amazon has exhibited patterns of Orwellian control with its own employees as well as the general public. The question is, is Jeff Bezos off the rails with Technocracy and the "science of social engineering" that requires tracking of everything in the known environment? TN Editor

"We know that no one ever seizes power with the intention of relinquishing it," came a warning from George Orwell's novel, *1984*, that is rapidly, wickedly, becoming prophecy with new Amazon eye-in-the-sky technology and a dark and disturbing twist. The American Civil Liberties Union (ACLU) is poking that eye with a sharp stick.

And Jeff Bezos is not feeling the love.

In what appears to be Bezos's latest strategic move in the quest to replace God as knower of all things is a hybrid monster of facial recognition software and a doorbell camera widget manufactured by Ring, a company that Amazon bought earlier this year.

In a gross assault on the right to privacy, a patent filed months ago essentially describes a product that captures information on people who as much as walk past a doorbell, sending real-time information to police databases. It also will allow customers the ability to upload to law enforcement photos of anyone they deem might be a sketchy individual.

What does a non-sketchy, normal person wear when ringing a doorbell?

Jacob Snow, a technology and civil liberties attorney for the ACLU, is fired up and fighting:

> *"It's rare for patent applications to lay out, in such nightmarish detail, the world a company wants to bring about. Amazon is dreaming of a dangerous future …"*

Or perhaps Bezos dreams of ruling the world.

Biometrics Bastardization

But attaining an unlimited collection of facial snapshots is just the beginning. A deeper dive into the patent application reveals that Amazon is prepping to expand its unlimited munitions stash of photos with other biometrics. And what it plans to extract from unsuspecting folks will horrify freedom-loving Americans.

Amazon plans to advance data collection that will include fingerprint scans, skin-texture analysis, DNA information to rival that of Ancestry.com, palm-vein analysis, hand geometry, iris recognition, odor/scent recognition, voice recognition, and if you have a hitch in the giddy-up, it will be able to track that as well.

An authoritarian surveillance police state in the making?

But let's talk about Rekognition, another program Amazon sold to law enforcement agencies and pitched to Immigration and Customs Enforcement (ICE). It's fatally flawed against people of color. A test found the program misidentified 28 lawmakers as police suspects, including six members of the Congressional Black Caucus. Oops, discriminatory, much?

On top of concerns by activists, community leaders, and politicians, 450 of Amazon's employees signed a letter of protest to Bezos to "demand that we stop" sales of the controversial software immediately, and one brave soul published, anonymously, a heartfelt call to arms in an editorial on **Medium:**

> *"Amazon talks a lot about values of leadership. If we want to lead, we need to choose between people and profits. We can sell dangerous surveillance systems to police, or we can stand up for what's right. We can't do both."*

Absolute Surveillance

As critics fear Amazon is pushing for a world policed and governed through automation, Bezos software continues to rack up sales, potentially removing human judgment from the law enforcement tool kit.

Read full story here…