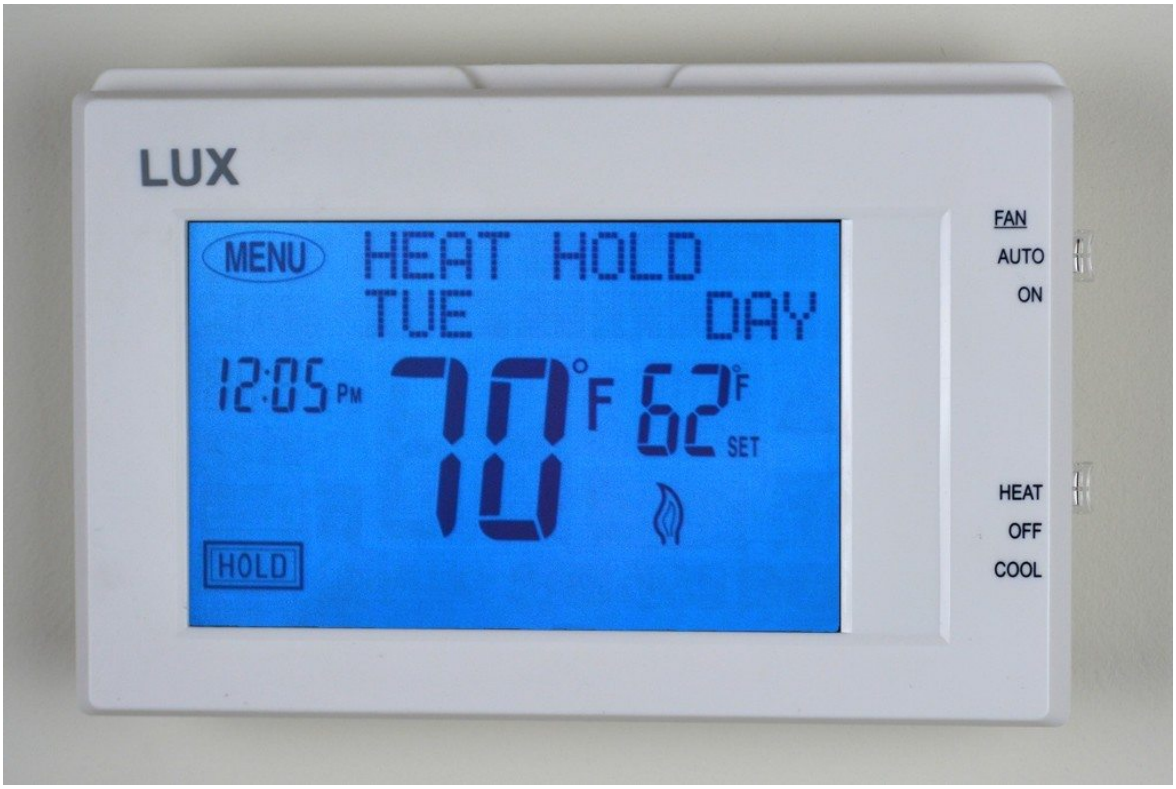


Smart Meters Can Be Used To Spy On Your Home And Your Data Sold Anywhere

TN Note: Smart meters are NOT about making life more convenient for you. They are a key component of implementing Technocracy and every shred of data that can be harvested from your home is fair game for anyone with connections and money to buy it. Indeed, they will "balance the load" but they never told you that they would balance it on your back, not theirs.

Families who have digital smart energy meters installed in their homes could find the devices are being used to spy on their habits, campaigners have warned.

A Mail investigation has discovered how marketing firms are targeting data collected by smart meters, which reveal how customers use their gas and electricity, and hoping to turn the information they provide in to a steady stream of cash.

Experts say the devices might be used to provide companies with clues to information about customers' lives which can be used for profit.

Privacy campaigners fear that in the most extreme cases sensitive data could be sold onto healthcare companies which could try and sell specially targeted goods and services to these customers.

Firms must ask customers' permission before examining in depth data or selling it on to third parties.

But experts fear that many customers who sign up for a smart meter may not be aware of how their data will be used.

A spokesman for privacy campaign group Big Brother Watch said: 'A smart meter will monitor your homes energy consumption, creating a honeypot of data which energy insurance and marking companies will inevitably be hungry for.

'These companies will be monitoring our every move whilst in the home.

'Energy is an essential which we all use, exploiting that data for alternative purposes such as marketing, advertising is a concern and should be flagged in clear language to anyone thinking about installing a smart meter in their home.'

Under Government plans, 50 million homes will be fitted with a smart meter by 2020 in a £11bn drive. Currently around 5,000 properties a day are being fitted with one.

The gadgets allow customers to see on a screen how much exactly their energy costs as they use it.

Information is fed directly to energy companies removing the need for meter readings or estimated bills.

Energy firms benefit too, because they can easily see when demand for gas and electricity is at its highest and jack up energy prices accordingly.

Alternatively, they can lower costs when demand is low.

Although energy firms will have to foot the bill for providing the devices, they are not allowed to directly charge customers for installing smart meters.

But they are expected to claw back these costs in other ways.

xperts say firms are eying up the steady stream of data that the devices provide about customers' lifestyles as a way of making a profit.

Personal data has been dubbed the 'new oil' by marketing firms, who say that the clues it provides about our lifestyles and spending habits.

Companies can use this information to reap huge profits by selling the data on or hitting customers with targeted deals.

Gas and electricity firms will be able to use smart meters to collect information about how customers use energy as frequently as every half hour.

This could reveal details such as which rooms and gadgets clients use most regularly, as well as when homeowners are in or out and even what time they are going to bed or how many cups of tea we make.

A family whose meter showed their home is losing a lot of heat compared to other neighbouring homes, might be a ripe target for insulation or a new boiler.

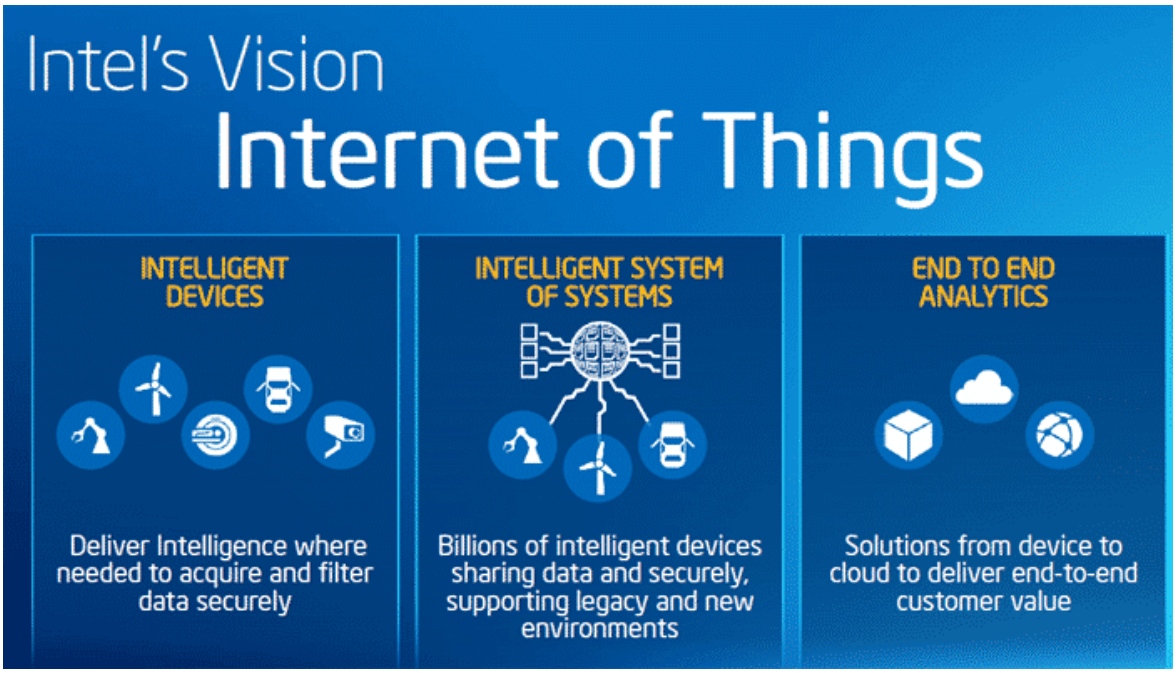
By contrast someone who uses a lot of energy at peak prices could be identified as a profitable customer and offered extra perks to keep them on the company's books.

A document by data firm Pitney Bowes describes smart meters as a 'once in a generation business opportunity for energy providers'.

It says its software will allow energy firms to use smart meters to 'clearly identify the most profitable customers' and 'optimise customer contact by using smart meter data to get relevant offers to the right customers at the right time through their preferred channel'.

It will also help firms to 'cross-sell, up-sell and retain customers'.

[Read full story here…]



Internet of Things Will Actually Start Connecting With Next Generation WI-FI

TN Note: Implementing the Internet of Things (IOT) has suffered because Wi-Fi technology has lagged behind. Almost everyone with a Wi-Fi router in their home knows that there are plenty of "dead" spots in the house. The new Wi-Fi standard will completely erase those inconveniences while making a strong signal possible to all corners of your property. Plus, city-wide Wi-Fi will allow things to be connected the the larger Internet grid. This technology is essential to the implementation of Technocracy.

There are plenty of blockades between now and the connected-device future that's been so long on the horizon. One of these is Wi-Fi, which has limitations that keep connected devices from connecting quite as efficiently as they could. Now, there's a plan in place to fix it.

The Wi-Fi Alliance, the organization that dictates and advances Wi-Fi standards, has announced the latest iteration of its increasingly indispensable technology. Called HaLow, it promises to double the range of standard 2.4GHz Wi-Fi connections, while also doing a better job of penetrating walls, floors, and other obstacles that can make your Wi-Fi sputter and skulk.

It manages this deftness and range by operating on the 900MHz band, a chunk of spectrum that's better suited for small data payloads and low-power devices than the relatively intensive, battery-straining 2.4GHz and 5GHz bands on which most current Wi-Fi routers operate. To cut through the numbers and specs and standards for a moment: It's Wi-Fi for smartwatches and Internet-enabled coffee makers and whatever other connected appliance might suit your deranged fancy.

"For a consumer, you might imagine someone who wants to deploy a water sensor in their basement to detect flooding or a motion sensor at the end of their driveway to warn them of someone arriving late at night," says Kevin Robinson, Wi-Fi Alliance vice-president of marketing. "In both of these cases, Wi-Fi HaLow will deliver power-efficient connectivity to the home access point (and the Internet) despite the challenging environment caused by obstructions in the device's path or ranges involved."

At this point you might be wondering why we'd need such a thing, when so much of what we've just described is already capably handled by Bluetooth, the connectivity tech of choice for most low-powered, online devices. You're right to wonder! There are a few potential answers, the most important of which being that Wi-Fi connects devices directly to the Internet, not just to another device. That may not seem so important now, but it will be critical as wearables, in particular, strive to become truly untethered. Eventually, connected devices need to transition from Pinocchio to real boy. HaLow should help that process.

Also, unlike Bluetooth, Wi-Fi Halow's ambitions extend quite a bit further than than your living room.

"Wi-Fi HaLow is well suited to meet the unique needs of the Smart

Home, Smart City, and industrial markets," says Edgar Figueroa, Wi-Fi Alliance President and CEO. "[It] expands the unmatched versatility of Wi-Fi to enable applications from small, battery-operated wearable devices to large-scale industrial facility deployments."

That's partly because, Robinson pointed out, in addition to the various security and interoperability features found in the Wi-Fi you know, HaLow will also share its ability to "support thousands of devices per access point." That means a business that requires huge numbers of environmental monitoring stations across multiple facilities would have a simple, integrated way to keep track of them.

Read full story here…

Spycams To Read Your Emotions And Moods

TN Note: Young technocrats in training are developing real-world systems to identify a person and then "read" his emotional state. Homeland Security, DARPA and the FBI are already hot on the trail of this technology. The obvious problem is that if the software errs, the error will still be attached to your profile. Stuff like this could mark you for the rest of your life.

Bill Hedgcock knows it sounds a little creepy.

Tucked into the white ceiling tiles, the ceiling camera he had installed at the Pappajohn Business Building at the University of Iowa scans the faces of all who pass under it and instantly calculates their moods — collecting readings for joy, frustration, confusion, fear, anger and sadness.

"We nicknamed it 'the creepy study,' because we just wanted to be out about it, just so everyone's aware," said Hedgcock, an associate professor of marketing. "It sounds creepy."

The facial encoding data is part of a larger student research project underway in the Tippie College of Business that uses automated technology to read emotions by measuring slight movements in the facial muscles, such as a movement of the eyebrow or a widening of a lip.

Hedgcock believes the University of Iowa is the world's only business school with this kind of real-time software that converts images of people's faces into readings for different moods. If it works, experts see huge potential for facial encoding in the worlds of marketing, advertising and political campaigns.

But that's no sure bet. Hedgcock makes it clear that the technology's accuracy remains unproven — it's one reason why his students have spent months picking it apart, getting a better understanding of the technology's limitations.

If his students eventually deem the technology a stinker, it's no big deal, Hedgcock says. But if the process is proven and adopted by marketing firms, his students will have a leg up when they go on the job hunt.

"If it does work, they walk out there and they know something that no one else knows how to do," he says. "It's not written in a textbook. It doesn't exist anywhere."

Hedgcock wanted to emphasize privacy with his students, so the camera doesn't record video or images of the people it measures. It simply kicks out data measuring what it sees, and it sees a lot — millions of rows of data so far.

Students have used the mood measurements in a variety of ways. From the first-floor camera, they crunched the data to see if the weather affects mood and if mood affects food sales at the business school's snack bar.

Do sunny skies make people happier? Do people purchase more caffeine when they're down?

But students say the best use of the technology isn't in a generic space such as a hallway on campus. People walking to and from classes or meetings aren't exactly the most expressive.

Students say the technology is likely most effective with a more specific aim, such as judging reaction to a short advertisement or a political debate — occasions more likely to elicit an emotional response.

Students paired up with Frank N. Magid Associates, a market research firm with offices in Marion, Ia. The company is known for its work gauging viewer sentiment about local television stations and their on-air personalities.

While it may never fully replace more conventional methods of judging consumer preference such as surveys and dial tests, Magid leaders say they believe facial encoding could be a supplement to their current suite of measurement tools.

Read the full story here...

Crime-Fighting Robots Hitting The Streets In California

TN Note: The Police State and Total Surveillance Society are joined at the hip. Automated police robots are currently only used as threat assessment and surveillance collection devices, but there will be a time when force/intervention features will be added. These robots are driven by AI, of course, and communicate everything the see, hear and think back to a central computer for analysis. This is a bad trend but one that will greatly further the aspirations of technocrats everywhere.

The robots might one day rise up and take over, but a Palo Alto startup called Knightscope has developed a fleet of crime-fighting machinery it hopes to keep us safe.

Knightscope's K5 security bots resemble a mix between R2D2 and a Dalek from Doctor Who – and the system behind these bots is a bit

Orwellian. The K5's have broadcasting and sophisticated monitoring capabilities to keep public spaces in check as they rove through open areas, halls and corridors for suspicious activity.

The units upload what they see to a backend security network using 360-degree high-definition and low-light infrared cameras and a built-in microphone can be used to communicate with passersby. An audio event detection system can also pick up on activities like breaking glass and send an alert to the system as well.

Malls and office buildings are also starting to employ the K5 units as security assistants. Knightscope couldn't name names, but tells TechCrunch the robots are being used at a number of tech companies and a mall in Silicon Valley at the moment.

CEO Stacey Dean Stephens, a former law enforcement agent, came up with the idea to build a predictive network to prevent crime using robots. He and his co-founder William Li have raised close to $12 million in funding so far from Konica Minolta and others to build on the idea.

While Knightscope doesn't think its robots will replace mall cops or security guards in the near future, the company does see them as assistants to human security teams. The startup currently rents each five-foot, 300-pound K5 unit out for $6.25 per hour (or less than minimum wage). However, teenagers or others tempted to kick or push the robots over may be shocked to find the robots can talk back to them, capture their behavior on film and alert authorities behind the scenes as well.

Read full story here…

IoT: Within 20 Years, Every Physical Item Will Have An Embedded Chip

TN Note: The Internet of Things (IoT) is going to revolutionize every business operation and every field of endeavor. With RFID chips planted in everything, the geo-spatial, real-time tracking of every physical thing (including humans) will be possible. Couple that with a little creative AI software and you have the perfect recipe for full-blown Technocracy.

The hype around the Internet of Things has been rising steadily over the past five years. In tech analyst Gartner's Hype Cycle for Emerging Technologies report in 2015, the IoT is at the peak of "inflated expectations", particularly for areas like the smart home, which involve controlling your lights, thermostat or TV using your mobile phone.

But the era of sensors has only just dawned, according to renowned technology investor and internet pioneer Marc Andreessen. In 10 years, he predicts mobile phones themselves could disappear.

“The idea that we have a single piece of glowing display is too limiting. By then, every table, every wall, every surface will have a screen or can project,” he told the Telegraph. “Hypothetically you walk upto a wall, sit at a table and [talk to] an earpiece or eyeglasses to make a call. The term is ambient or ubiquitous computing.”

Which is why he has invested $25m into Californian startup Samsara, which is the first of a new generation of “internet of things” devices that solves huge industrial problems, rather than turning your fridge or your toothbrush into a portal to the web.

“This second wave of companies, they don’t want to just do “internet of things”,” Andreessen said. “They are showing up three years later, saying ok I know exactly how this is going to get used. It’s for real businesses in industrial environments.”

Gartner backs this claim – it predicts that businesses alone will double spending on internet of things units by 2020, going from $767 billion to more than $1.4 trillion.

Read full story here…

French Trains Test Software To Spot Suspicious Behavior

TN Note: A Total Surveillance Society is a key element for implementing Technocracy on a global basis, and terrorism will be the ready excuse to do so. Note that AI, coupled with biometric/facial recognition technology, will do most of the heavy lifting.

Software that monitors suspicious behaviour and luggage could eventually be integrated into 40,000 surveillance cameras across France, a railway firm said Wednesday, as the country tightens security after last month's deadly Paris attacks.

Public transport authorities are looking to technology to better predict warning signs among passengers in the wake of the shootings and bombings that left 130 people dead.

New software being tested by France's state-owned SNCF tracks changes in body temperature, raised voices and jerky body movements that can indicate heightened levels of anxiety, the rail firm's general secretary Stephane Volant told AFP.

"We are testing to work out what flags up people with a negative intention, an aggressor, or a groper," he said, but added what was also being ascertained was the level of "social acceptability" of such software.

Cameras that detect packages left unattended for too long were also under evaluation, Volant said, adding the experiments had the full backing of the law.

Another strand of SNCF's strategy was the possibility of equipping its staff with wearable cameras to identify fare dodging or suspect behaviour, and in the spring it will launch an app that allows passengers to raise an alert from their smartphones.

A law is also under consideration in France to give SNCF security agents

powers to perform security pat-downs and search passengers' luggage.

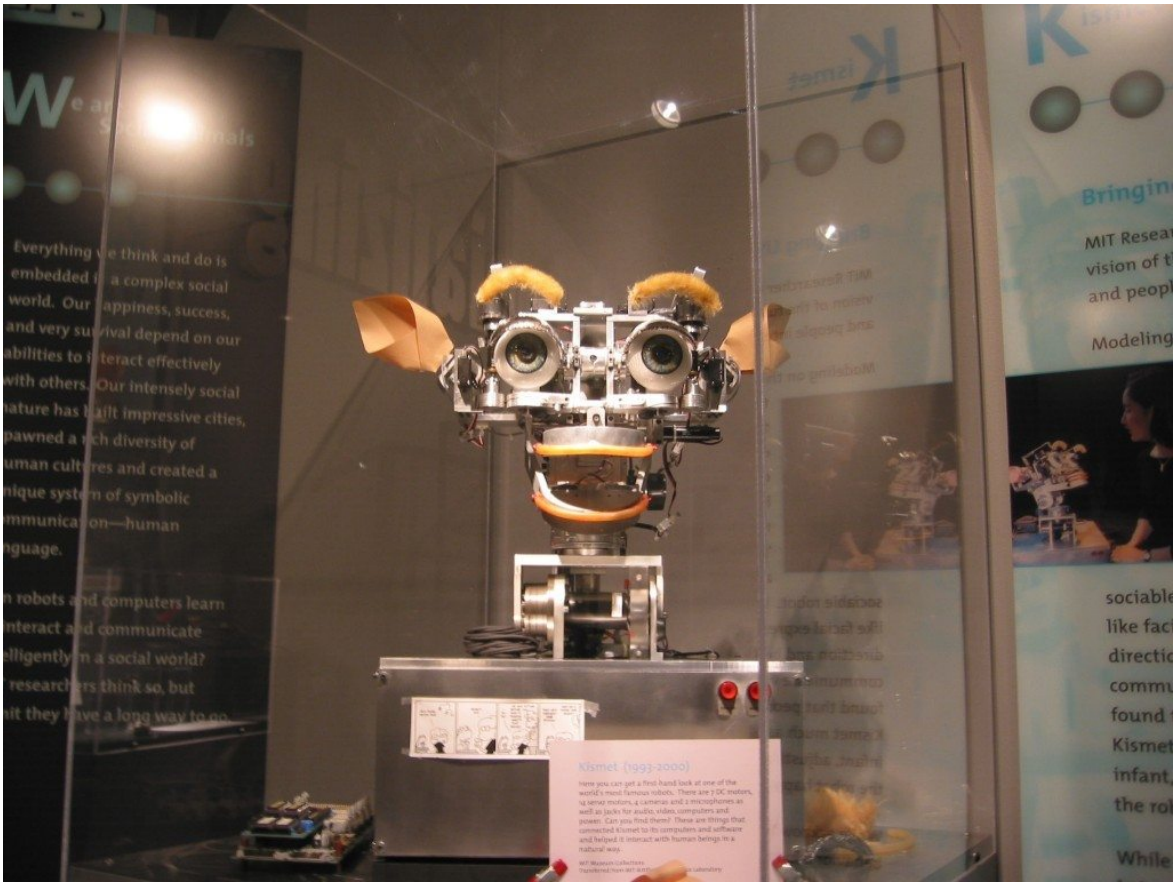
France will install security gates at stations in Paris and Lille for the Thalys cross-Europe rail services by December 20 in one of a raft of measures introduced after the Paris attacks, minister Segolene Royal said Tuesday.

A Thalys train from Amsterdam to Paris was attacked by a heavily armed man in August, but he was overpowered by passengers.

The high-speed Thalys service links Paris with Lille in northern France, the Belgian capital, Brussels, Amsterdam in the Netherlands and the western German city of Cologne.

Passengers boarding those trains do not currently have to pass through security checks, unlike for the cross-Channel Eurostar train services to Britain, which have airport-style security.

Read full story here…



2015 Was A Breakthrough Year For Artificial Intelligence

TN Note: The growth of AI is staggering. In 2012, a tech startup named CrowdFlower sold some 2 million spreadsheet data rows to customers to use in training their AI systems. In 2015, they have sold almost 100,000,000. The field is accelerating according to a geometric progression. Much of AI is being applied to simple, linear tasks like image recognition, but the larger applications remain in analysis of so-called big data – and this is precisely where Technocracy will enter into its own.

After a half-decade of quiet breakthroughs in artificial intelligence, 2015 has been a landmark year. Computers are smarter and learning faster than ever.

The pace of advancement in AI is “actually speeding up,” said Jeff Dean, a senior fellow at Google. To celebrate their achievements and plot the

year ahead, Dean and many of the other top minds in AI are convening in Montreal this week at the Neural Information Processing Systems conference. It started in 1987 and has become a must-attend event for many Silicon Valley companies in the last few years, thanks to the explosion in AI. NIPS was where Facebook Chief Executive Officer Mark Zuckerberg chose in 2013 to announce the company's plans to form an AI laboratory and where a startup named DeepMind showed off an AI that could learn to play computer games before it was acquired by Google.

There should be plenty to discuss this week. The unprecedented advancements in AI research this year can be attributed to a confluence of nerdy factors. For one, cloud computing infrastructure is vastly more powerful and affordable, with the ability to process complex information. There are also more plentiful datasets and free or inexpensive software development tools for researchers to work with. Thanks to this, a crucial class of learning technology, known as neural networks, have gone from being prohibitively expensive to relatively cheap.

That's led to rapid uptake by the tech industry's largest companies, including Google, Facebook, and Microsoft. Each operates its own AI lab that conducts important research in the field and publishes much of it for the academic community to build upon. This year, Google researchers nabbed the cover of scientific journal Nature with a system that can learn to play and master old Atari games without directions. Facebook built a way to let computers describe images to blind people; Microsoft showed off a new Skype system that can automatically translate from one language to another; and IBM singled out AI as one of its greatest potential growth areas.

Startups are also contributing meaningfully to AI. Preferred Networks is making AI systems that will go into industrial robots made by Japan's Fanuc, and Indico Data Labs worked with a Facebook researcher to teach a computer how to paint faces using its own sort of imagination.

Read full story here…

NSA Phone Surveillance Has Not Ended

TN Note: So far in 2015, the NSA has suffered rulings from two federal courts to cease various data collection schemes that target American citizens at large. Has this curtailed the NSA? No. They simply side-step the orders and keep on collecting more data. This is further evidence that Technocrats within the Executive Branch have literally gone rogue and are ignoring Congress and the Judiciary, apparently believing that their cause is higher than anyone or anything else in existence.

At 11:59 P.M. on Saturday night, the U.S. National Security Agency supposedly yanked the cord on its bulk telephone records collection, thereby ending an expansive surveillance program that the nation's intelligence community put in place in the wake of the September 11, 2001 terror attacks.

“There will be no analytic access to the collected metadata after this time,” the Office of the Director of National Intelligence (ODNI) said in a statement.

The public learned of the agency’s spying program after Edward Snowden—ex-NSA contractor and whistleblower extraordinaire—leaked information about it to news outlets in 2013. That revelation provoked an uproar among privacy advocates, and Congress eventually reacted by replacing parts of the U.S.A. Patriot Act, which authorized the privacy-invasive program, with a seemingly-less-intrusive piece of legislation, the U.S.A. Freedom Act, over the summer.

It would be wrong to conclude, however, that this moment signaled the demise of the agency’s surveillance powers. Rather, the NSA has transitioned to a new system. The reformed scheme addresses the most controversial aspects of the collection program, but questions remain about its implementation. Here’s everything you need to know about the change.

What happened at midnight on Saturday?

When the clock struck midnight, a 6-month-long “orderly transition” period for the NSA expired. After the Freedom Act became law in early June, the agency was granted a 180-day grace period to get its affairs in order before putting an end to the bulk phone metadata collection program authorized by a particular portion—Section 215—of the Patriot Act. Under the new guidelines, the NSA no longer may directly collect and hold data about the domestic phone records of U.S. citizens.

Instead, telecom companies will retain and access the data on their customers. The NSA may then seek warrants from the secretive courts created by the Foreign Intelligence Surveillance Act (FISA) in order to compel these companies to hand over pertinent information on terrorism suspects and affiliates. The requests are not done in bulk, but rather require “specific selectors” such as the phone number of an individual. The NSA then has up to 180-days to query the telecom companies for more data—on socially connected persons of interest, so-called one-to-two degree “hops” on their networks—before seeking a renewed

authority from a FISA court.

There are exceptions to these items though.

What kinds of exceptions?

Notably, the NSA's bulk collection database still exists. The agency has requested permission to keep its records for the past five years intact through Feb. 29, 2016. This will ostensibly allow the agency to make sure nothing has gone awry during the transition. Access will be "limited to technical personnel and solely for the purpose of verifying that the new targeted production mechanism authorized by the USA FREEDOM Act is working as intended," ODNI said in a statement. The database is "hands off" for analysts. Additionally, it's worth noting that the NSA must retain these records until all lawsuits regarding the original program are resolved.

What's inside the database?

As mentioned, the database contains metadata. It includes information on phone calls such as who, when, and how long—for instance, the identity of the sender and recipient, the duration, and the time and date. Metadata does not include the content of conversations. However, that doesn't make it any less of a treasure trove for dot-connecting investigators.

Read full story here…

NSA Whistleblower Ed Snowden Demonized By CIA following Paris Attacks

TN Note: Ed Snowden made powerful enemies when he exposed the unconstitutional schemes of the Intelligence community, and they are still hissing at him. This article has it correct, that Snowden "*revealed to the world was that the U.S. government is monitoring the Internet communications and activities of everyone else: hundreds of millions of innocent people under the largest program of suspicionless mass surveillance ever created, a program that multiple federal judges have ruled is illegal and unconstitutional.*"

Decent people see tragedy and barbarism when viewing a terrorism attack. American politicians and intelligence officials see something else: opportunity.

Bodies were still lying in the streets of Paris when CIA operatives began exploiting the resulting fear and anger to advance long-standing political agendas. They and their congressional allies instantly attempted to heap blame for the atrocity not on Islamic State but on several preexisting

adversaries: Internet encryption, Silicon Valley's privacy policies and Edward Snowden.

The CIA's former acting director, Michael Morell, blamed the Paris attack on Internet companies "building encryption without keys," which, he said, was caused by the debate over surveillance prompted by Snowden's disclosures. Sen. Dianne Feinstein (D-Calif.) blamed Silicon Valley's privacy safeguards, claiming: "I have asked for help. And I haven't gotten any help."

Former CIA chief James Woolsey said Snowden "has blood on his hands" because, he asserted, the Paris attackers learned from his disclosures how to hide their communications behind encryption. Woolsey thus decreed on CNN that the NSA whistleblower should be "hanged by the neck until he's dead, rather than merely electrocuted."
In one sense, this blame-shifting tactic is understandable. After all, the CIA, the NSA and similar agencies receive billions of dollars annually from Congress and have been vested by their Senate overseers with virtually unlimited spying power. They have one paramount mission: find and stop people who are plotting terrorist attacks. When they fail, of course they are desperate to blame others.

The CIA's blame-shifting game, aside from being self-serving, was deceitful in the extreme. To begin with, there still is no evidence that the perpetrators in Paris used the Internet to plot their attacks, let alone used encryption technology.

CIA officials simply made that up. It is at least equally likely that the attackers formulated their plans in face-to-face meetings. The central premise of the CIA's campaign — encryption enabled the attackers to evade our detection — is baseless.

Even if they had used encryption, what would that prove? Are we ready to endorse the precept that no human communication can ever take place without the U.S. government being able to monitor it? To prevent the CIA and FBI from "going dark" on terrorism plots that are planned in person, should we put Orwellian surveillance monitors in every room of every home that can be activated whenever someone is suspected of

plotting?

The claim that the Paris attackers learned to use encryption from Snowden is even more misleading. For many years before anyone heard of Snowden, the U.S. government repeatedly warned that terrorists were using highly advanced means of evading American surveillance.

Then-FBI Director Louis Freeh told a Senate panel in March 2000 that "uncrackable encryption is allowing terrorists — Hamas, Hezbollah, Al Qaeda and others — to communicate about their criminal intentions without fear of outside intrusion."

Or consider a USA Today article dated Feb. 5, 2001, eight months before the 9/11 attack. The headline warned "Terror groups hide behind Web encryption." That 14-year-old article cited "officials" who claimed that "encryption has become the everyday tool of Muslim extremists."

Even the official version of how the CIA found Osama bin Laden features the claim that the Al Qaeda leader only used personal couriers to communicate, never the Internet or telephone.

Within the Snowden archive itself, one finds a 2003 document that a British spy agency called "the Jihadist Handbook." That 12-year-old document, widely published on the Internet, contains instructions for how terrorist operatives should evade U.S. electronic surveillance.

In sum, Snowden did not tell the terrorists anything they did not already know. The terrorists have known for years that the U.S. government is trying to monitor their communications.

Read full story here…

How You Can Beat Government And Hacker Surveillance

With pervasive and invasive surveillance all around us, it is not necessary for you to play the victim. While many simply throw up their hands and say there is no escape, others are taking concrete action to keep their personal and private data out of the belly of the beast.

Your communications and personal data belong to you and you alone. You wouldn't allow anyone into your home to just snoop around, so why would you tolerate unauthorized government snatching of everything you say in messages, email or phone calls? And, if the government isn't bad enough, hackers and other miscreants are waiting to steal your personal data every chance they get. It's time to get smart and tough about this, and start taking responsibility for our own data security.

The sad fact of intrusive surveillance is that virtually everything you do on the Internet ends up in government hands. That is, every email, text,

message or phone call, including the content from all social media like Facebook, Twitter and Instagram.

NSA whistleblower Edward Snowden forever put this to rest with his now-verified revelations of massive NSA data collection efforts. The Electronic Frontier Association published a detailed timeline of NSA Spying on Americans.

Smart Internet programmers are starting to fight back, and you can too! In this article, I will give you several options and techniques to make yourself as invisible as possible to prying eyes. The answers lie in sophisticated new encryption techniques that make what you send and say incomprehensible to anyone other than the intended recipient.

Signal by Open Whisper Systems (Click here to view)

This is a free messaging and phone app for iPhone or Android only, and the only such app that was endorsed by Edward Snowden himself. High-level encryption cloaks everything you type and say, and can only be deciphered by the intended recipient. Messages are transmitted directly to the receiving party, and thus are never stored on a central server. The company boasts that even they cannot see what you do, and they specifically state that no government or private entity has a "back door".

Signal incorporates a built-in calling feature that scrambles your phone call so that eavesdroppers hear only unintelligible gibberish.

Use Signal to replace Facebook Messenger, SMS texting, Skype chats and calls, and other messaging apps.

Wickr (Click here to view)

This free app provides top-secret messaging that encrypts everything. Like Signal, messages are fully encrypted and are never stored on a central server, but rather are delivered directly to the recipient's phone or computer. What sets Wickr apart is that each message has a sender-defined expiration date that causes the message to vanish when its time

is up. When I say “vanish” I mean just that – It disappears from both sender and receiver and then gets “shredded” on the respective devices. Because deleted files can easily be recovered after the fact, “shredding” overwrites the deleted files with ones and zeroes so that recovery becomes impossible no matter who attempts it.

Wickr does not provide encrypted calling, but the company claims that it is working on such a feature.

Use Wickr to replace Facebook Messenger, SMS texting, Skype chats and other messaging apps. It is totally conceivable to combine usage of both Wickr and Signal to provide a comprehensive messaging/calling solution. Use Signal as your default messaging/calling app, and then use Wickr when you need top-secret encryption that leaves no traces of your messages.

StartMail (Click here to view)

Forget free email services like Gmail or Yahoo! They are free because they harvest your data and sell it to the highest bidders, including the U.S. government. StartMail will cost you $59.95 per year, but it provides automatic PGP encryption to every email that you send, so that only the intended recipient can view it. There is no “back door” because the company and servers are based in Europe, where privacy laws are much tougher than they are in the U.S.

Use StartMail to replace any email service, especially those that say they are “free” but really are costing you everything.

If you are just looking for an email with a better privacy statement than Gmail, then take a look at FastMail, which is operated by Mozilla; note that Fastmail is not encrypted, however.

StartPage (Click here to view)

This is a private search engine that does not save your searches nor identify you to the targeted search entity. Rather, it uses a “proxy server” to recast your search as not coming from you. This effectively hides your identity.

All of the popular search engines and especially Google, record every search you make on the Internet, including personal identifiers like your IP address. Your IP address, of course, pinpoints you as specifically as your phone number, social security number, driver's license number or home address. Once you are duly identified, these snoops keep 100% of your activity in permanent files. According to StartPage,

> *"Those searches reveal a shocking amount of personal information about you, such as your interests, family circumstances, political leanings, medical conditions, and more. This information is modern-day gold for marketers, government officials, black-hat hackers and criminals – all of whom would love to get their hands on your private search data."*

If you want to defeat Google, et al, then use StartPage search engine.

LocalActivist.net (Click here to view)

This is a fully encrypted and private network for activists who work in close-knit groups. It provides tools for communication, collaboration, document management and file sharing for each specific group. It is member-supported and subsequently does not run ads or collect any marketing information from your activities.

If you are actively involved in your community to turn back the tide of Technocracy (including Agenda 21, Sustainable Development, Smart Grid, Smart Growth, etc.), then don't conduct your business in public. When you use services like Facebook, Twitter, Linkedin, etc., nothing is hidden from your opponent's eyes. During WWII, a popularized intelligence phrase was "Loose lips sink ships." Accordingly, LocalActivist's motto is, "What you say here, stays here."

Other considerations

It is up to you to practice "clean computing" on all your electronic devices. Always use a good virus protection program to protect against viruses, malware and phishing attacks. If a clandestine keylogger program is running, then every keystroke you type is being sent to

someone with bad intentions for your data. Keyloggers are hard to detect and remove, but there are resources that can help, for instance, this article on the KimKomando web site.

Always use strong passwords and remember them with a password manager, such as 1Password or Dashlane. Both are easy to use and will store all of your passwords and vital information in encrypted format.

A word about credit cards. Whenever you make a local purchase with your debit or credit card, the details of your purchase, including your location, are being recorded and tracked. When you pay in cash, there is no tracking possible. Thus, when considering any local purchase, think about the wisdom of paying cash in certain instances.

A word about cell phones. Your cell phone itself becomes a very effective tracking device. When not at home or office, always turn off the wifi feature on your phone and don't use apps that record or post your location information.

A word about public wifi. When you connect your phone, tablet or laptop to a public wifi (e.g., Starbucks, a restaurant or public library), be very aware that you are at risk of being hacked. If you are confident that you have the proper firewall, anti-hacking and virus software installed, then go ahead. If not, then don't connect in the first place.

This is not an exhaustive look at Internet security, but it will take care of some of the more important issues. I suggest that you make a simple written plan of action, and take one item at a time to master it – then move on to the next one. Yes, there are potential inconveniences and habits that need to be changed, but they are far from insurmountable.

For every person who protects their Internet presence by taking advantage of the latest encryption technology, the Technocrat's dream of total data domination falls a little bit shorter. So, start protecting yourself today and give a Technocrat a headache at the same time.