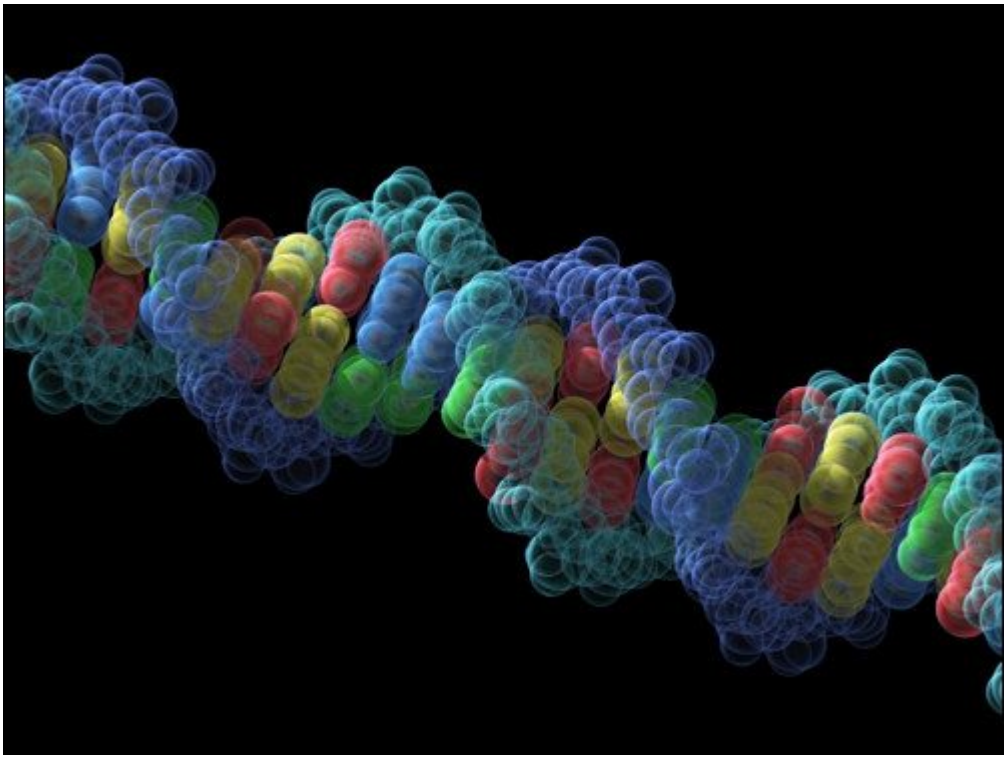


Feds Pressing Ancestry.com For Customers' DNA

TN Note: Technocrats have an insatiable desire for data, and they will pursue it wherever and whenever it exists. DNA is more than just personal data, however, because it associates you with your entire family tree. Other sources of DNA cataloging by the Feds include records at hospitals, blood test labs and your personal doctor's office tests. Of all the other types of data collected (financial, travel, emails, phone calls, etc.), DNA is the most revealing and desirable.

When companies like Ancestry.com and 23andMe first invited people to send in their DNA for genealogy tracing and medical diagnostic tests, privacy advocates warned about the creation of giant genetic databases that might one day be used against participants by law enforcement. DNA, after all, can be a key to solving crimes. It "has serious information about you and your family," genetic privacy advocate Jeremy Gruber told me back in 2010 when such services were just getting popular.

Now, five years later, when 23andMe and Ancestry both have over a million customers, those warnings are looking prescient. “Your relative’s DNA could turn you into a suspect,” warns Wired, writing about a case from earlier this year, in which New Orleans filmmaker Michael Usry became a suspect in an unsolved murder case after cops did a familial genetic search using semen collected in 1996. The cops searched an Ancestry.com database and got a familial match to a saliva sample Usry’s father had given years earlier. Usry was ultimately determined to be innocent and the Electronic Frontier Foundation called it a “wild goose chase” that demonstrated “the very real threats to privacy and civil liberties posed by law enforcement access to private genetic databases.”

The FBI maintains a national genetic database with samples from convicts and arrestees, but this was the most public example of cops turning to private genetic databases to find a suspect. But it’s not the only time it’s happened, and it means that people who submitted genetic samples for reasons of health, curiosity, or to advance science could now end up in a genetic line-up of criminal suspects.

Both Ancestry.com and 23andMe stipulate in their privacy policies that they will turn information over to law enforcement if served with a court order. 23andMe says it’s received a couple of requests from both state law enforcement and the FBI, but that it has “successfully resisted them.”

23andMe’s first privacy officer Kate Black, who joined the company in February, says 23andMe plans to launch a transparency report, like those published by Google, Facebook and Twitter, within the next month or so. The report, she says, will reveal how many government requests for information the company has received, and presumably, how many it complies with.

“In the event we are required by law to make a disclosure, we will notify the affected customer through the contact information provided to us, unless doing so would violate the law or a court order,” said Black by email.

[Read entire story here…]

Private Database Lets Police Skirt License Plate Data Limits

LONG BEACH, Calif. (AP) — For years, police nationwide have used patrol car-mounted scanners to automatically photograph and log the whereabouts of peoples' cars, uploading the images into databases they've used to identify suspects in crimes from theft to murder.

Nowadays, they are also increasingly buying access to expansive databases run by private companies whose repo men and tow-truck drivers photograph license plates of vehicles every day.

Civil libertarians and lawmakers are raising concerns about the latest practice, arguing that there are few, if any, protections against abuse

and that the private databases go back years at a time when agencies are limiting how long such information is stored.

Some argue police should get a warrant from a judge to access the databases, much as they would if they wanted to obtain emails.

“The public is understandably concerned about how this information is going to be used,” said Chuck Wexler, executive director of the Police Executive Research Forum, but for police, the databases, just like surveillance cameras, are an important investigative tool.
License plate scans have been at the forefront of a privacy debate in recent years.

The license plate reader companies say their scans are useless without access to motor vehicle department rolls — which police have. They say lawmakers should focus on strengthening data access laws, rather than eliminating police tools.

The largest firm, Livermore, California-based Vigilant Solutions, has filed a lawsuit or actively lobbied in at least 22 states and the District of Columbia for its technology, said Todd Hodnett, founder of Digital Recognition Network, which provides the data it collects to law enforcement through its sister company Vigilant.

He said as of June that roughly 30,000 law enforcement officers nationwide subscribe to their LEARN database.

Hodnett said when he tells legislators that the data his company gathers is protected, “I can’t tell you how many times I’ve heard legislators say this sounds like a solution in search of a problem.”

The plate readers can collect 1,600 plates an hour. Vigilant has collected scans since 2007 and has more than 3 billion license plates, growing at a rate of 100 million a month from every major metro area. There are roughly 254 million registered vehicles in the U.S.

Law enforcement agencies have acknowledged privacy concerns over how long they store scans — which includes a photo of the vehicle, its plate, and a GPS and time marker — and have voluntarily instituted policies to limit that storage.

The Long Beach, California, police have used the license plate technology since 2005 and in December signed on with Vigilant. The department retains its own scans for two years, primarily because of server space and funding, like many other agencies.

Read full story here…

Accenture and World Bank Call for a Global Universal ID

TN Note: Technocracy specifies a global and universal ID system that will digitally identify every human on earth. Here is the proof of it…

In a new report issued in collaboration with Accenture, the World Bank is calling on governments to work together to implement standardized, cost-effective identity management solutions.

A report synopsis notes that about 1.8 billion adults around the world currently lack any kind of official documentation. That can exclude those individuals from access to essential services, and can also cause serious difficulties when it comes to trans-border identification.

That problem is one that Accenture has been tackling in collaboration with the United Nations High Commissioner for Refugees, which has been issuing Accenture-developed biometric identity cards to populations of displaced persons in refugee camps in Thailand, South Sudan, and elsewhere. The ID cards are important for helping to ensure that refugees can have access to services, and for keeping track of refugee populations.

Moreover, the nature of the deployments has required an economically feasible solution, and has demonstrated that reliable, biometric ID cards can affordably be used on a large scale. It offers hope for the UN's Sustainable Development Goal of getting legal ID into the hands of everyone in the world by the year 2030 with its Identification for Development (ID4D) initiative.

Read original story here…

Pre-Crime 'Predictive Policing' Accelerates Nationwide

Police departments in major American cities are trying to prevent violent crime with the help of an unlikely ally: data mining.

In recent years, law enforcement agencies have been experimenting with "predictive policing," a tool that harnesses computer algorithms to identify individuals likely to commit crimes, The New York Times reports.

It may sound a little bit like "Minority Report," a fictional future where psychics help police catch criminals right before they commit their crimes, but the reality is a bit more mundane.

The Times story details one way in which predictive policing is implemented in Kansas City: "call-ins." Armed with information on recent parolees, high-crime neighborhoods, and personal networks both off- and online — plus more anecdotal information like rumors that police hear on the street — algorithms detect individuals suspected to be influential in criminal groups.

Those individuals are then called in, as a group, to meet with police officials as well as "local and federal prosecutors, plus the police chief and the mayor."

The officials warn that future violent offenses by the attendees, or even their associates, will be punished harshly. And they've got examples to back it up — like a man who was caught with a bullet in his pocket after receiving a call-in warning. He ended up with a 15-year prison sentence.

Police hope that these warnings will trickle down from the suspected leaders to the people they influence.

Predictive policework is rooted in complex mathematical models, but the basic premise is actually quite simple. A foundational paper on modeling crime compares crime to earthquakes to explain the rationale.

Read original article here…

Appeals Court Deals Blow to Lawsuit Limiting NSA's Bulk Call Surveillance

An appeals court in Washington dealt a setback Friday to an activist's lawsuit against the government over the legality of the National Security Agency's call records program, ruling that the plaintiff has not proved his standing to sue.

A three-judge panel of the U.S. Court of Appeals for the District of Columbia Circuit ruled that public-interest lawyer Larry Klayman, the founder of Freedom Watch, has not proved that his own phone records were collected by the NSA — and so has not met a condition of bringing the lawsuit. It sent the case back to a lower court for further deliberation on the issue.

The panel's ruling also reversed a ban on the NSA's collection that had

been imposed — and temporarily stayed — by a district court judge in December 2013.

The strictly procedural ruling does not address the constitutionality or legality of the program.

[Read the federal appeals court ruling that lifts an injunction against the NSA phone call records program]

Congress in June put an end to the program, passing a law that bars the government from collecting phone data and other records in bulk. But the NSA is continuing to do so as it transitions the program to phone companies by December.

Read full article here…

FBI Builds Biometric Database On All Americans

In the last few years, FBI has been dramatically expanding its biometrics programs, whether by adding face recognition to its vast Next Generation Identification (NGI) database or pushing out mobile biometrics capabilities for "time-critical situations" through its Repository for Individuals of Special Concern (RISC). But two new developments—both introduced with next to no media attention—will impact far more every-day Americans than anything the FBI has done on biometrics in the past. Read about the first development below and the second here.

FBI Combines Civil and Criminal Fingerprints into One Fully Searchable Database

Being a job seeker isn't a crime. But the FBI has made a big change in how it deals with fingerprints that might make it seem that way. For the first time, fingerprints and biographical information sent to the FBI for a background check will be stored and searched right along with fingerprints taken for criminal purposes.

The change, which the FBI revealed quietly in a February 2015 Privacy Impact Assessment (PIA), means that if you ever have your fingerprints taken for licensing or for a background check, they will most likely end up living indefinitely in the FBI's NGI database. They'll be searchedthousands of times a day by law enforcement agencies across the country—even if your prints didn't match any criminal records when they were first submitted to the system.

This is the first time the FBI has allowed routine criminal searches of its civil fingerprint data. Although employers and certifying agencies have submitted prints to the FBI for decades, the FBI says it rarely retained these non-criminal prints. And even when it did retain prints in the past, they "were not readily accessible or searchable." Now, not only will these prints—and the biographical data included with them—be available

to any law enforcement agent who wants to look for them, they will be searched as a matter of course along with all prints collected for a clearly criminal purpose (like upon arrest or at time of booking).

This seems part of an ever-growing movement toward cataloguing information on everyone in America—and a movement that won't end with fingerprints. With the launch of the face recognition component of NGI, employers and agencies will be able to submit a photograph along with prints as part of the standard background check. As we've noted before, one of FBI's stated goals for NGI is to be able to track people as they move from one location to another. Having a robust database of face photos, built out using non-criminal records, will only make that goal even easier to achieve.

Read full story here…

Agencies Say They Need Access to Americans' Emails Without a Warrant

A bipartisan bid to reform an electronic-privacy law has the support of the tech community and the White House, but federal law enforcement officials tell Congress the changes would hamper civil prosecution.

Civil law enforcement agencies like the Federal Trade Commission and the Securities and Exchange Commission would not be able to obtain critical information if the law were changed to require criminal warrants for access to data stored on cloud services, according to witnesses from those agencies testifying in front of the Senate Judiciary Committee Wednesday.

The law enforcement officials were reacting to bills from Sens. Mike Lee and Patrick Leahy, and Reps. Kevin Yoder and Jared Polis, that aim to update the Electronic Communications Privacy Act, or ECPA.

In its current form, ECPA protects emails from government snooping for 180 days. When the law was initially drawn up in 1986, email providers routinely removed emails from their servers a month or two after they were delivered; users would generally download the messages they intended to keep. Whatever remains on an email server after 180 days is fair game for government to access, with just a subpoena—not a warrant.

Today, ubiquitous cloud-based email systems like Gmail, which offer gigabytes of storage for free, allow the average user to keep his or her messages—and calendars, contacts, notes, and even location data—on a provider's servers indefinitely.

The ECPA Amendments Act would require law enforcement to get a warrant to access server-hosted information, no matter how old, and would require the government to notify an individual that his or her information was accessed within 10 days, with certain exceptions.
But law enforcement officials expressed opposition to some of the bill's

proposed changes, arguing that its requirement for criminal warrants could leave civil litigators without access to important electronic information.

"The bill in its current form poses significant risk to the American public by impeding the ability of the SEC and other civil law enforcement agencies to investigate and uncover financial fraud and other unlawful conduct," said Andrew Ceresney, director of enforcement at the Securities and Exchange Commission.

Ceresney and Daniel Salsburg—chief counsel for technology, research, and investigation in the FTC's consumer protection branch—said the SEC and FTC are not looking for the authority to obtain data with just a subpoena, and instead proposed a system where they could obtain a court order for access to the data. Such a process would notify the individual being investigated and give him or her the chance to make a case in front of the judge before an order is granted or denied.

Justice Department to Require Warrants for Cell-Phone Tracking Technology
The new policy does not apply to state and local police departments that have used cell-site simulators to track criminals.

But despite their opposition to the proposed change to ECPA, neither the SEC nor the FTC has obtained emails through an administrative subpoena in the past five years, Ceresney and Salsburg said Wednesday.

Ceresney said the decision to avoid subpoenas was made "in deference" to ongoing conversations about ECPA reform. A 2010 federal court order also bound the government's hands by declaring ECPA unconstitutional—a decision the ECPA Amendments Act intends to codify into law—but Ceresney said the SEC does not interpret the court's decision as an impediment to using subpoenas to obtain data.

The civil law enforcement officials' comments about ECPA reform were met with immediate backlash from the tech community, which has come out in strong support of the changes.
"The FTC claims to be a champion of consumer privacy, yet the agency wants access to Americans' data without a warrant," said Berin Szoka,

president of TechFreedom, a technology think tank. “The Commission’s testimony today confirms long-standing rumors that it will only support ECPA reform if it gets a carve-out from the bill’s warrant requirement.

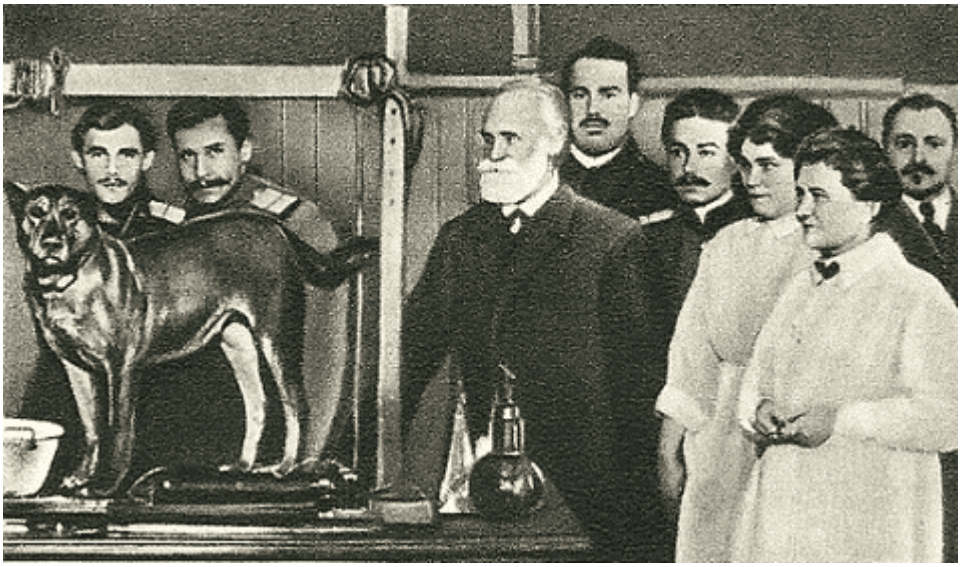
“The FBI is not an alien force imposed on the American people,” the agency’s director says, as feds clash with Silicon Valley over encryption standards.
“This is the issue that has stalled ECPA reform for over five years, despite overwhelming bipartisan support,” Szoka added. “The FTC’s testimony is carefully crafted to sound reasonable, but the agency is simply helping to obstruct the major privacy reform of our generation.”

Julie Brill, an FTC commissioner, released a statement Wednesday indicating she disagreed with Salsburg’s testimony. “I am concerned that a judicial mechanism for civil law enforcement agencies to obtain content from ECPA providers could entrench authority that has the potential to lead to invasions of individuals’ privacy and, under some circumstances, may be unconstitutional in practice,” Brill said.

Google and BSA-The Software Alliance, a prominent tech association, appeared in a separate witness panel before the committee, calling for swift change in order to improve customers’ privacy and alleviate business pressures.

“By creating inconsistent privacy protection for users of cloud services and inefficient and confusing compliance hurdles for service providers, ECPA has created an unnecessary disincentive to move to a more efficient, more productive method of computing,” said Richard Salgado, the director of Google’s law enforcement and information security branch.
This story was updated with a statement from FTC Commissioner Julie Brill.

Story first appeared on NationalJournal.



Obama Issues Executive Order for Use of Behavioral Data

A new executive order from President Obama directs all government agencies to use psychological science and data to help connect more Americans to government programs.

The order instructs government agencies to use “behavioral science”— a tactic used by Obama’s political campaigns to harness data from their supporters to target them effectively.

The program has already existed in an experimental form, but now Obama has formally established the federal “Social and Behavioral Sciences Team,” ordering them to to use psychology and experimental behavior data to make government more user-friendly.

An example of these techniques used during Obama’s campaign was that it was better to affirm a positive message rather than denying a negative message.

According to reports, behavioral science was used to advise the campaign to focus on Obama’s Christianity instead of trying to deny the notion that he was a Muslim. Other tactics included encouraging supporters to act for the campaign in small ways before asking them to commit to bigger goals.

A study released today by the president's office of National Science and Technology reveals that behavioral science has already helped government agencies target individuals.

Oftentimes, studies of individuals' behavior led federal agencies to tweak their approach to adjust and simplify their approach to bring in greater results.

The preview program showed that by tweaking messaging, more service members enrolled in retirement programs and benefits, more students made payments on student loans, and more farmers applied for federal loans.

At one point, the report reveals, the experimental team obtained outside data from uAspire and the National Student Clearinghouse to better target students based on "student-level demographic and academic achievement data."

Other programs targeted at veterans used existing data from the Department of Veterans Affairs, according to the report.

The program demonstrated that more people decided to enroll in health insurance, thanks to specially designed letters to people who had given up on completing their Obamacare enrollment forms.

"When behavioral insights—research findings from behavioral economics and psychology about how people make decisions and act on them—are brought into policy, the returns are significant," the report notes.

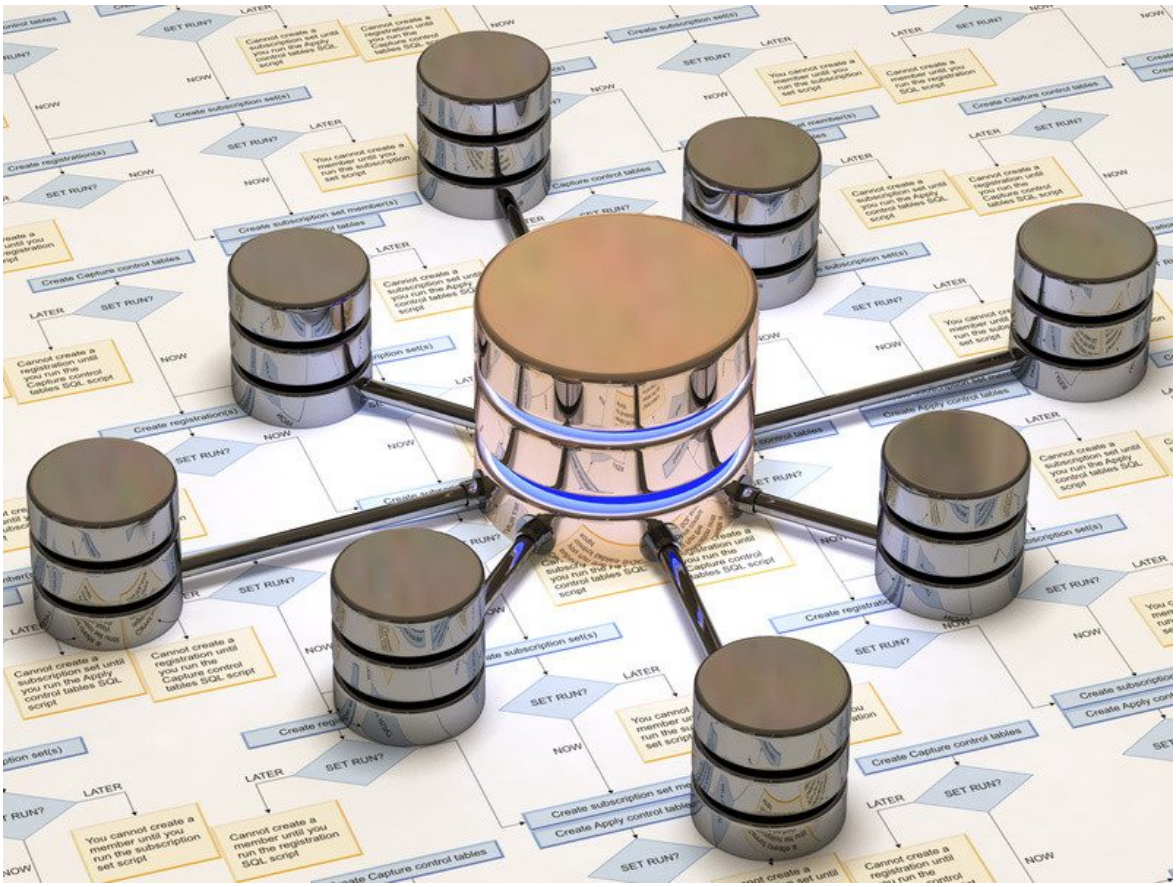
The program, however, will likely lead more government agencies to using and storing data from randomized research trials on everyday Americans to understand their behavior.

Obama's executive order codifies his government experiment into law, allowing every agency to target individuals for greater service and success.

"A growing body of evidence demonstrates that behavioral science insights — research findings from fields such as behavioral economics and psychology about how people make decisions and act on them — can

be used to design government policies to better serve the American people," Obama writes in his executive order.

Story first appeared on Breitbart



Data Dominance: Technocracy's Final Hurdle

Within the last week, stunning revelations prove conclusively that: a) an extensive and comprehensive, multi-faceted database already exists on all Americans and b) The specific purpose of the data is to control and micro-manage the entire population.

In *Technocracy Rising: The Trojan Horse of Global Transformation* I demonstrated that a comprehensive data monitoring system on the entire societal system is the holy grail of Technocracy, without which

absolute control would not be possible.

On July 18, 2015, Paul Sperry wrote in the NY Post, Obama collecting personal data for a secret race database. It is important to note that the mere existence of data by itself does not imply intent. Intention and purpose are only revealed by humans when they seek to find answers to questions posed for whatever reason. In this case, Obama is sifting an existing database to find specific answers relating to race and diversity issues.

The same database could just as easily calculate everyone's carbon footprint, reveal political preferences and involvements, list supporters of Sustainable Development and Global Governance, and much more. Basically, once the data is collected, the sky is the limit as to the kind of questions that can be asked of it.

The scope of data mining revealed includes information on healthcare, housing, home loans, credit cards, employment and education. Other sources (i.e., Ed Snowden's revelations on NSA spying) reveal massive data collections of all emails, phone calls, text and chat messages, social media activity, vehicle license plate readers, facial recognition and energy consumption (via Smart Grid/Smart Meters).

Background

Technocracy was originally proposed and documented in 1934 as a replacement economic system for Capitalism and Free Enterprise, to be based on energy currency instead of monetary currency and supply and demand economic principles. Many observers then and now have concluded that if fully implemented, Technocracy would result in a totalitarian form of scientific dictatorship.

The fifth of the seven key requirements for implementing Technocracy was plainly recorded in the *Technocracy Study Course* in 1934: ***"Provide specific registration of the consumption of each individual, plus a record and description of the individual."***

Control over what? *The Technocrat* magazine (1938) gave a succinct summary of Technocracy's purpose and scope: *"Technocracy is the*

science of social engineering, ***the scientific operation of the entire social mechanism*** *to produce and distribute goods and services to the entire population…"*

The economic nature of Technocracy is revealed throughout their own documents, as well as it is today. For instance, the NYPost article notes Obama's purpose as "racial and *economic* justice."

Free Enterprise calls for the distribution of goods and services based on supply and demand depending on consumer preferences; Technocracy ignores the consumer and makes arbitrary decisions on which goods and services will be created, what they will cost, and to whom they will be distributed. To the technocrat, societal engineering is the ultimate expression of micro-management down to the very last minutiae of existence.

Purpose and Intention

Obama seeks to use the master database of personal information to answer questions about "racial and economic justice." Sperry concludes,

> *"Obama is presiding over the largest consolidation of personal data in US history. He is creating a diversity police state where government race cops and civil-rights lawyers will micromanage demographic outcomes in virtually every aspect of society."*

Such are the unmistakeable markers of Technocracy-in-process.

But the intentional use of data to manipulate society and the people in it is only *just beginning*.

Micromanaging Travel: A Smart Meter For Your Car

On 7/12/2015, Leo Hohmann wrote in WND, "*Feds want to track your every move on road*", which detailed Oregon's new "Vehicle Miles Traveled" tax, or VMT. VMT is predicated on placing a discrete GPS tracking device in every vehicle that will report wirelessly your exact travel route during the reporting period. You would then be sent a tax

bill for your “share” of the road.

A University of Iowa study revealed the Devil in the details of how individual taxation will take place. A customized tax rate will be applied to each vehicle based on its owner’s “carbon footprint”. How would they know what your carbon footprint is? Well, your master profile has all the information needed for the calculation:

– How many and what type of vehicles do you own?
– Do you ride to work on a bicycle or mass transit?
– How much electricity and gas do you use in your home?
– How large is your home?
– Where do you live? In the country? Suburb? Urban dweller?
– How efficient are your appliances?
– How many children do you have?
– How many plane flights do you take?
– How much waste/garbage does your household produce?

The VMT is comparable to a “smart meter” for you car, and is being rolled out by Federal mandate, in similar fashion to the kickstart of Smart Grid in 2009. Twenty-nine states are already proposing legislation to follow in Oregon’s footsteps, and the Department of Transportation is already working within all fifty states to accelerate acceptance.

Hohmann concludes, “*If this sounds like a line straight from the United Nations’ sustainability agenda, that’s because it is*.”

Conclusion and Endgame

So here we have two concrete examples of how data from multiple sources is being combined to force policy issues regulating all of society.

Data is being collected at an unprecedented rate in all of world history. Virtually every piece of digital information in existence is being stored in Federal systems, such as the massive NSA facility in Utah that has capacity to hold 100 percent of all data on the planet. The full societal impact of current data stored has not yet been felt because data analysis technology has not kept pace with storage technology. In fact, current computer technology is completely and permanently inadequate to

analyze such volumes of data in a timely fashion.

This is rapidly changing, however, and the recent advent of quantum computing technology should become fully operational within a 2019-2021 timeframe – that's just 4 to 6 years away from now! Quantum computers operate at the molecular level and can potentially speed up data operations by several orders of magnitude. One writer states that even first generation quantum computers make the fastest desktop computer seem like an abacus by comparison.

Although universities and large computer companies are working non-stop on developing quantum computers, the NSA and DARPA (Defense Advanced Research Projects Agency) are leading the charge, fully expecting to receive the first benefits on behalf of the emerging Technocracy.

Technocracy's final hurdle is data domination. When completed, Technocracy will assert itself over every facet of existence in America. There will be no turning back. Resistance will be punished. Freedom and Liberty will permanently sink back into the dark ages of history.

Will Americans recognize the threat and respond? This writer certainly hopes so, but thus far the response has been minimal.

Special Note

The *only* book in print today that addresses historic and modern Technocracy is ***Technocracy Rising: The Trojan Horse of Global Transformation***. It is highly recommended to purchase and read this book immediately, and then to distribute copies to everyone you know.