Why Sustainable Development Always Has An Insatiable Appetite For More Data

TN Note: Sustainable Development is the reincarnation of historic Technocracy from the 1930s. Technocracy demands that all data be collected from the "social machine" that we call society. The more data available, the better the monitoring and control possibilities. The scientists and engineers who would control Technocracy use a combination of the Scientific Method and Systems Theory (both of which have been bastardized from their original creations) to determine the "best practices" for running society. Note especially the emphasized paragraphs below.

Sustainable development is in the spotlight in 2016, which marks the start of the 2030 Agenda for Sustainable Development, an initiative that is both aspirational and transformative.

The first priority for all national governments in planning for the 17 new Sustainable Development Goals (SDGs), and their 169 associated targets, is to address the strengths and weaknesses of data sources, to swiftly determine how best to address the gaps, as well as the

complexities of measurement. Rapid development of the capacities of national statistical institutions will be critical because, 15 years from now, by the end of the 2030 Agenda, there will be nearly half a billion more people living in the Asia-Pacific region, all of whom should have reliable access to energy, food, water, education and employment.

Data are the lifeblood of decision-making. Without them, designing, monitoring and evaluating policies for sustainable development is almost impossible. The breadth and depth of the new development agenda entails complex decisions about the future of our planet, our communities and our economies. Without appropriate data and information, there is a risk that our sustainable development strategies will be only partially complete, with their contours dictated by what is and is not available. This will not only slow down the process of implementing the SDGs, but also limit their transformational potential. [emphasis added by TN]

Generally, official statistics offer insights about Asia-Pacific development, but these are inadequate for the far-reaching and integrated dimensions of the sustainable development agenda. The World Bank's Statistical Capacity Indicator for the Asia-Pacific region offers good foundations on which to build. On a scale from zero (representing no capacity) to 100 (full capacity), a rating of 79 is assigned for the timeliness of statistics, 70 for the adequacy of source data and 62 for methodologies used. There are, however, individual country scores as low as 20.

We know, for example, that 490 million people in Asia and the Pacific are undernourished. But we don't always know where they are, why they remain hungry, or the impacts of sudden shocks or stress. Nor do we know how well existing policy interventions are working.

We also know that 277 million people in our region have no access to safe drinking water, a problem which affects one in every ten rural residents. What we don't know is how long it takes people to get to water, or the actual volume of clean water available for use.

We know that approximately half a billion people in the countries of Asia and the Pacific do not have access to electricity, but we are uncertain precisely how many. Estimates vary from 427 million to 621 million, depending on the method used. It is also unclear how many more suffer from unreliable access, and whether some population groups have more reliable access than others.

We know that between 1970 and 2014, natural disasters resulted in $1.22 trillion of regional economic losses but, because there is no agreement as to what actually constitutes a natural disaster, how many have occurred and how many people were affected, these figures may be underestimated by as much as 50 per cent. This is compounded by the fact that impressive regional economic growth and social developments in recent years have not been accompanied by similar improvements in environmental protection.

Making data work for development calls for greater and sustained investment in statistics, statistical bodies, institution-building and partnerships. Estimates of the investment required globally to effectively monitor the 2030 Agenda over the next 15 years are approximately $1 billion per year, but the economic, environmental and social costs of failing to make this investment may be, literally, incalculable. [emphasis added by TN]

Read full story here…

Pentagon's Secret Pre-Crime Program To Know Your Thoughts, Predict Your Future

TN Note: This is NOT science fiction. Read every word of this article. Predictive behavior analysis is *the big rage* among technocrats who are bent on "scientific social engineering". The only hindrance to a complete rollout of this technology is the more advanced computing power needed to analyze big data in real-time mode – but it is very close. Total Awareness Society is a long-established requirement for Technocracy.

The US Department of Defense (DoD) wants contractors to mine your social media posts to develop new ways for the US government to infer what you're really thinking and feeling—and to predict what you'll do next.

Pentagon documents released over the last few months identify ongoing classified research in this area that the federal government plans to expand, by investing millions more dollars.

The unclassified documents, which call on external scientists, institutions and companies to submit proposals for research projects, not

only catalogue how far US military capabilities have come, but also reveal the Pentagon's goals: building the US intelligence community's capacity to forecast population behavior at home and abroad, especially groups involved in political activism.

They throw light on the extent to which the Pentagon's classified pre-crime R&D has advanced, and how the US military intends to deploy it in operations around the world.

Could your social media signature reveal your innermost thoughts?

A new Funding Opportunity Announcement document issued by the DoD's Office of Naval Research (ONR) calls for research proposals on how mining social media can provide insight on people's real thoughts, emotions and beliefs, and thereby facilitate predictions of behavior.

The research for Fiscal Year 2016 is part of the Pentagon's Multidisciplinary Research Program of the University Research Initiative (MURI), which was initiated over 25 years ago, regularly producing what the DoD describes as "significant scientific breakthroughs with far reaching consequences to the fields of science, economic growth, and revolutionary new military technologies."

The document calls for new work "to understand latent communication among small groups." Social meaning comes not just from "the manifest content of communication (i.e., literal information), but also from latent content — how language is structured and used, as well as how communicators address each other, e.g., through non-verbal means — gestures, head nods, body position, and the dynamics in communication patterns."

The Pentagon wants to understand not just what we say, but what is "latent" in what we say: "Subtle interactions such as deception and reading between the lines, or tacit understanding between communicators, relative societal position or relationship between communicators, is less about what is said and more about what is latent."

All this, it is imagined, can be derived from examining social media, using new techniques from the social and behavioral sciences.

The Pentagon wants to:

> *"… recognize/predict social contexts, relationships, networks, and intentions from social media, taking into account non-verbal communication such as gestures, micro-expressions, posture, and latent semantics of text and speech."*

By understanding latent communication, the Pentagon hopes to develop insight into "the links between actors, their intentions, and context for use of latent signals for group activity." The idea is to create:

> *"… algorithms for prediction and collection of latent signals and their use in predicting social information."*

These algorithms also need to "accurately detect key features of speech linked to these structural patterns (e.g., humor, metaphor, emotion, language innovations) *and* subtle non-verbal elements of communication (e.g., pitch, posture, gesture) from text, audio, and visual media."

The direct military applications of this sort of information can be gleaned from the background of the administrator of this new research program, Dr. Purush Iyer, who is Division chief of Network Sciences at the US Army Research Laboratory (USARL).

Among the goals of Dr. Iyer's research at the US Army are expanding "Intelligent Networks" which can "augment human decision makers with enhanced-embedded battlefield intelligence that will provide them with tools for creating necessary situational awareness, reconnaissance, and decision making to decisively defeat any future adversarial threats."

Creeping police state

The allure of co-opting Big Data to enhance domestic policing is already picking up steam in the US and UK.

In the US, an unknown number of police authorities are already piloting

a software called ‘Beware’, which analyses people’s social media activity, property records, the records of friends, family or associates, among other data, to assign suspects a so-called “threat-score.”

That “threat-score” can then be used by police to pre-judge if a suspect is going to be dangerous, and to adapt their approach accordingly.

Given the police’s discriminatory track record with shootings of unarmed black people skyrocketing, the extent to which such ‘Minority Report’-style policing could backfire by justifying more discriminatory policing is alarming.

In the UK, Home Secretary Theresa May just last week told the Police ICT Suppliers Summit that polices forces should use predictive analytics to “identify those most at risk of crime, locations most likely to see crimes committed, patterns of suspicious activity that may merit investigation and to target their resources most effectively against the greatest threats.”

Noting that the police have yet to catch up with the “vast quantities of data” being generated by citizens, she complained: “Forces have not yet begun to explore the crime prevention opportunities that data offers.”

In reality, the shift to predictive policing in the UK is well underway, with Greater Manchester, Kent, West Midlands, West Yorkshire and London’s Metropolitan Police having undertaken trials of a software known as “PredPol.”

Read full story here…

Apple Fighting FBI's Demands To Unlock Terrorist's iPhone

TN Note: Unfettered access to all information is Technocracy's dreamscape. Intelligence and law enforcement agencies have tried in vain to force software companies to put "back doors" into their offerings so the Feds could have easy access. This has been fought tooth-and-nail by many (not all) technology companies. This is the latest attempt by the FBI to force Apple to re-write its iPhone security program in order to "crack" the cellphone used by the San Bernardino terrorist, and Apple is fighting back. If the Feds win this case, it will change the face of technology forever.

On Tuesday, a US judge ordered Apple to help the FBI unlock an encrypted iPhone.

The Cupertino, California-based company has reacted furiously.

Apple CEO Tim Cook has published an extremely strongly worded letter, calling the demand "chilling," arguing that it "would undermine the very freedoms and liberty our government is meant to protect."

……

This court case isn't taking place in a vacuum. We're in the middle of a bitter feud between tech companies and law enforcement about the rise in the use of encryption.

In the years after NSA whistle-blower Edward Snowden's revelations about the US government's mass-surveillance programs, there have been a heightened awareness of privacy issues and moves to strengthen protections on consumer products.

Apple has been one of the strongest voices in support of this move, and all new iPhones and Apple devices are now encrypted by default.

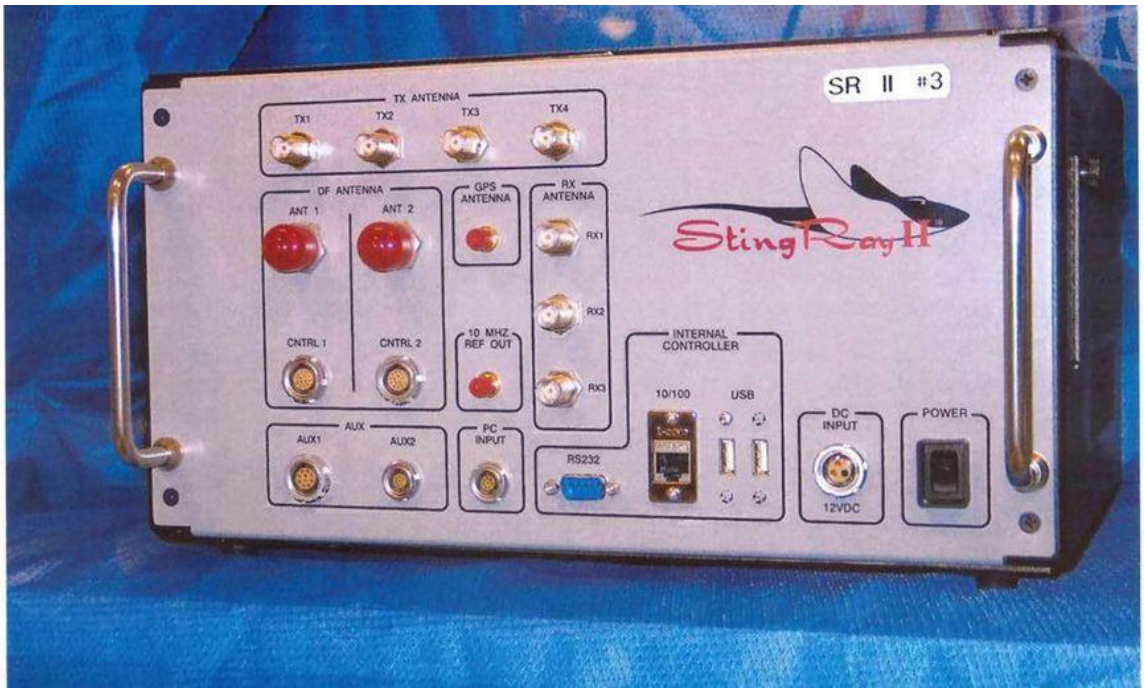
……

[Apple CEO Tim Cook writes]

> *The government suggests this tool could only be used once, on one phone. But that's simply not true. Once created, the technique could be used over and over again, on any number of devices.* ***In the physical world, it would be the equivalent of a master key, capable of opening hundreds of millions of locks — from restaurants and banks to stores and homes. No reasonable person would find that acceptable.***
>
> ***The government is asking Apple to hack our own users and undermine decades of security advancements that protect our customers*** *— including tens of millions of American citizens — from sophisticated hackers and cybercriminals. The same engineers who built strong encryption into the iPhone to protect our users would, ironically, be ordered to weaken those protections and make our users less safe.*
>
> ***We can find no precedent for an American company being forced to expose its customers to a greater risk of attack****. For years, cryptologists and national security experts have been warning against weakening encryption. Doing so would hurt only the well-meaning and law-abiding citizens who rely on companies like Apple*

to protect their data. Criminals and bad actors will still encrypt, using tools that are readily available to them.

Read full story here…



NYPD Routinely Tracked Citizen's Cellphones Without Warrants Since 2008

TN Note: There is no justification for anyone using Stingray technology to secretly track a citizen's cell phone, except that a search warrant is in hand. However, all other citizens in close proximity are also caught in the dragnet, making it a privacy advocate's nightmare. Technocrats see no problem in skirting the law when it suits their purposes.

New York City police have tracked citizens' cellphones over 1,000 times since 2008 without using warrants, according to public records obtained by the New York Civil Liberties Union.

The organization announced on Thursday that the NYPD has typically used “stingrays” after obtaining lower-level court orders, but not warrants, before using the devices. The department also does not have a policy guiding how police can use the controversial devices. This is the first time that the scope of stingray use by the nation’s largest police agency has been confirmed.

The devices, generically known as stingrays, work by mimicking cell towers and tracking a cellphone’s location at a specific time. Law enforcement agencies can use the technology to track people’s movements through their cellphone use. Stingrays can also detect the phone numbers that a person has been communicating with, according to the NYCLU. The devices allow law enforcement to bypass cellphone carriers, who have provided information to police in the past, and can track data about bystanders in close proximity to the intended target.

Read full story here…

U.S. Director Of National Intelligence: We Might Use Smart Home Devices To Spy On You

TN Note: Americans need to see the web of surveillance being spun all around them. “Smart Home” devices that exist in major appliances, thermostats, LED light bulbs and security cameras are all targets for spying. Smart Grid provides WiFi-enabled connectivity to every smart appliance within your home. Every WiFi router and cable modem is also a gateway into private areas.

Note that the Director of National Intelligence is head of all 16 intelligence agencies in the U.S., including the NSA. The position was created by President George W. Bush in 2005, and the first appointee to fill the position was Trilateral Commission member John Negroponte. Negroponte architected and re-organized the intelligence community to provide future monitoring for the coming Technocracy.

If you want evidence that US intelligence agencies aren’t losing surveillance abilities because of the rising use of encryption by tech companies, look no further than the testimony on Tuesday by the director of national intelligence, James Clapper.

As the Guardian reported, Clapper made clear that the internet of things – the many devices like thermostats, cameras and other appliances that are increasingly connected to the internet – are providing ample opportunity for intelligence agencies to spy on targets, and possibly the masses. And it’s a danger that many consumers who buy these products may be wholly unaware of.

“In the future, intelligence services might use the [internet of things] for identification, surveillance, monitoring, location tracking, and targeting for recruitment, or to gain access to networks or user credentials,” Clapper told a Senate panel as part of his annual “assessment of threats”

against the US.

Clapper is actually saying something very similar to a major study done at Harvard's Berkman Center released last week. It concluded that the FBI's recent claim that they are "going dark" – losing the ability to spy on suspects because of encryption – is largely overblown, mainly because federal agencies have so many more avenues for spying. This echoes comments by many surveillance experts, who have made clear that, rather than "going dark", we are actually in the "golden age of surveillance".

Privacy advocates have known about the potential for government to exploit the internet of things for years. Law enforcement agencies have taken notice too, increasingly serving court orders on companies for data they keep that citizens might not even know they are transmitting. Police have already been askingGoogle-owned company Dropcam for footage from cameras inside people's homes meant to keep an eye on their kids. Fitbit data has already been used in court against defendants multiple times.

Read full story here…

Private Company Tracked Iowa Caucusgoers' Cellphones In Real Time To Analyze Voting

TN Note: Dstillery is the company behind this, and it was their first foray into political analysis. Their website boasts, *"Be First in Connecting With Always-On Customers."* The technology is reminiscent of the Jade Helm military exercise in summer 2015 where geo-spatial intelligence was used to model communities via artificial intelligence software. After you are matched with your cell phone, all other data about you is searched out and fed to the AI program: social media, purchases, Internet browsing history, location tracking – all in real-time. Geo-spatial monitoring has led one top expert to conclude that it is comparable to digital slavery. Technocracy heaven has arrived.

Who needs exit polls when you can track caucusgoers' phones?

That's what one company did. Dstillery, which has been called "Picasso in the dark art of digital advertising," turned its intelligence-collection capabilities to the Iowa caucuses last week.

The company used location data to identify more than 16,000 devices at caucus locations across the state.

“We can take a population in a discrete location — in this case a polling, a caucus site — and sample that population and go and then look at characteristics of that population that no one’s been able to discern before, because we have this incredibly rich behavioral view of American consumers based on all the digital behaviors we observe,” Dstillery CEO Tom Phillips said in an interview.

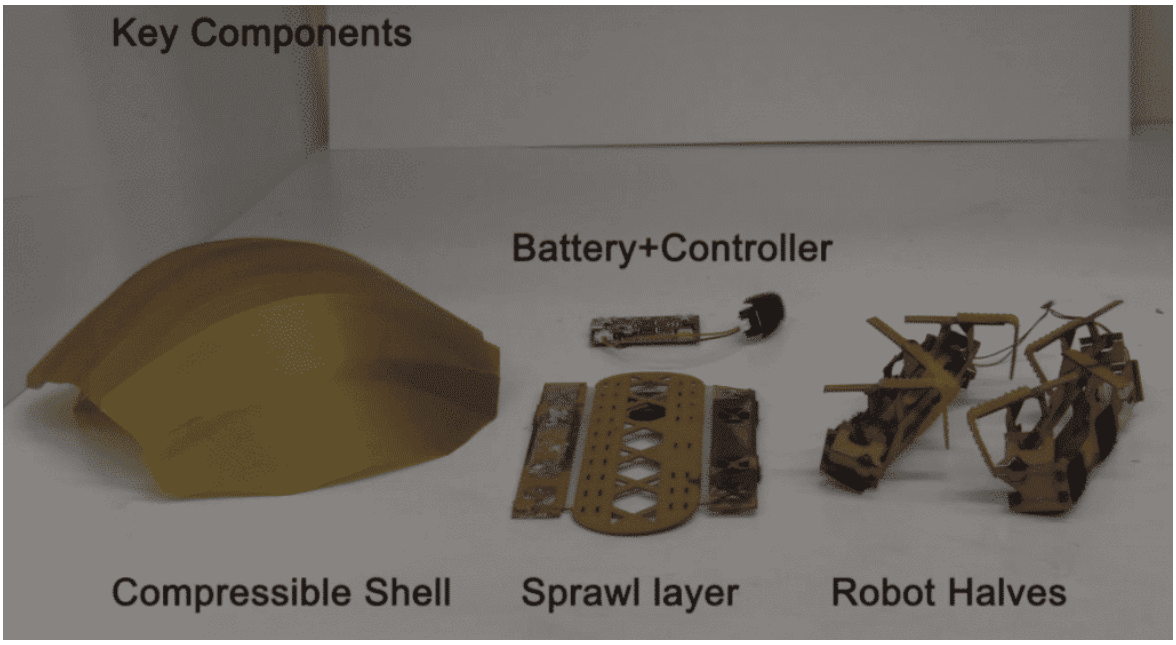
The results are interesting, if scientifically inexact. The company could not tell how individual caucusgoers came down by candidate but could determine, in counties decisively won by certain candidates, the dominant online behaviors of attendees:

- Caucusgoers who were expecting a child or had a young baby tended to be Republican, and they showed up in greater numbers where Florida Sen. Marco Rubio was victorious.
- Other family behaviors – those associated with both working and stay-at-home parents, buyers of kids’ clothing and back-to-school supplies – were high at caucus sites that went to Texas Sen. Ted Cruz. On the Democratic side, they were split between Hillary Clinton and Sen. Bernie Sanders.
- Caucusgoers in counties won decisively by Donald Trump tended to have stronger household interests – grillers, do-it-yourselfers, lawn and garden and hardware. He didn’t do well with business leaders — those whose online behavior indicates they are business owners or executives. More of those folks showed up where Rubio support was decisive.
- Sports fans (NCAA, NFL, NBA, NHL, baseball and fantasy leagues) showed up in greater numbers at caucuses won by Rubio and Sanders. NASCAR fans, however, correlated with Trump and Clinton support.
- Techies – information-technology decision-makers and technology buyers – correlated with Rubio and Sanders support.

In a harbinger of more (slightly spooky) technologies that could be ahead

for political campaigning — if they aren't already in use — Dstillery also cross-referenced which devices had been used on university campuses during the previous two weeks to determine how many caucusgoers were students — roughly 5.4%, according to the analysis. And those voters showed up in greater numbers where Sanders and Rubio scored decisive wins.

Read full story here…



Cockroach Robots: Scientists Discover New Mobility Techniques

TN Note: They will smell, see, touch, sample, run like blazes and they will create intelligent networks so they can "swarm" in unison. Don't bother with bug spray. The purported use of robot cockroaches is for search and rescue in disaster areas, but in the hands of master surveillance organizations, it will be the go-to bug. In the hands of crooks, it will be the perfect reconnaissance tool.

After running roaches through tunnels that were only as high as two pennies stacked flat, researchers at UC Berkeley have designed a cockroach robot that's able to squeeze through tiny spaces at blazing speeds.

Such a roach bot, described in the Proceedings of the National Academy of Sciences, might eventually be deployed as search-and-rescue robobugs in rubble-strewn disaster zones and may cause scientists and engineers to redefine their ideas about the kinds of animals that can inspire "soft robotics."

Study co-author Robert Full, a UC Berkeley biomechanist, has long explored how animals move – he's analyzed how geckos stick to walls and built other roach-inspired running robots. But he soon became intrigued by the insects' ability to wriggle their way into nooks and crannies – even though they technically have a hard, exoskeleton-clad body.

"Animals with exoskeletons like cockroaches can go everywhere, and infest any space, so we wondered, well, how did they do that?" Full said. "So we constructed a series of tight crevices to see what they could do."

The researchers took American cockroaches (Periplaneta americana) – "the one you think you don't have in your house, but you do," Full said – and had them run through a tunnel 12 millimeters high. Then they reduced the tunnel height, down to 9 millimeters, and then 6 millimeters, and then to a tight 4 millimeters – less than a third of their standing body height. Until the last, tightest tunnel, the cockroach basically maintained its high speed, running with its legs spread out out as its body became increasingly smooshed.

"They run really fast even though they're compressed in half, their legs completely splayed out to their side," Full said. "They could still run at 20 body lengths per second, 60 centimeters a second — which if you scale it up is 70 miles an hour for a human."

Read full story here…

How Facebook, Google And Other Internet Titans Are Profiling You And Profiting From It

TN Note: Technocracy lives and breathes data, all of which is necessary for monitoring the social machine. The Technocrat magazine stated in 1938, *"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… "*, and this is exactly what is happening today.

> *Facebook, Google, and the other Internet titans have ever more sophisticated and intrusive methods of mining your data, and that's just the tip of the iceberg.*

The success of the consumer Internet can be attributed to a simple grand bargain. We've been encouraged to search the web, share our lives with friends, and take advantage of all sorts of other free services. In exchange, the Internet titans that provide these services, as well as hundreds of other lesser-known firms, have meticulously tracked our every move in order to bombard us with targeted advertising. Now, this grand bargain is being tested by new attitudes and technologies.

Consumers who were not long ago blithely dismissive of privacy issues are increasingly feeling that they've lost control over their personal information. Meanwhile, Internet companies, adtech firms, and data brokers continue to roll out new technologies to build ever more granular profiles of hundreds of millions, if not billions, of consumers. And with next generation of artificial intelligence poised to exploit our data in ways we can't even imagine, the simple terms of the old agreement seem woefully inadequate.

In the early days of the Internet, we were led to believe that all this data would deliver us to a state of information nirvana. We were going to get new tools and better communications, access to all the information we could possibly need, and ads we actually wanted to receive. Who could possibly argue with that?

For a while, the predictions seemed to be coming true. But then privacy goalposts were (repeatedly) moved, companies were caught (accidentally) snooping on us, and hackers showed us just how easy it is to steal our personal information. Advertisers weren't thrilled either, particularly when we adopted mobile phones and tablets. That's because the cookies that track us on our computers don't work very well on mobile devices. And with our online activity split among our various devices, each of us suddenly appeared to be two or three different people.

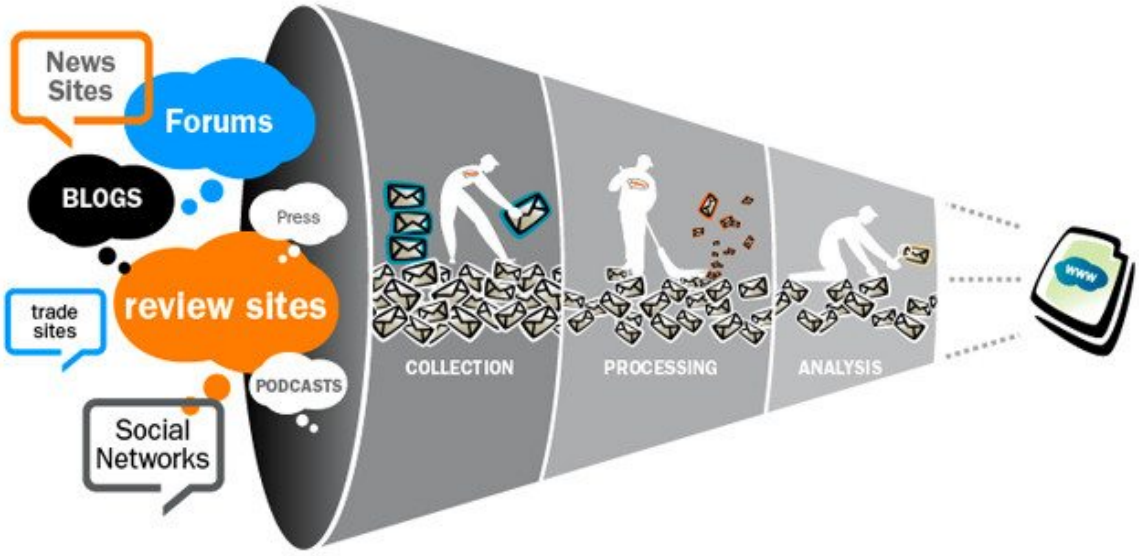
This wasn't a bad thing for consumers, because mobile phones emit data that enable companies to learn new things about us, such as where we go, who we meet, places we shop, and other habits that help them recognize and then predict our long-term patterns.

But now, new cross-device technologies are enabling the advertising industry to combine all our information streams into a single comprehensive profile by linking each of us to our desktop, mobile phone, and iPad. Throw in wearable devices like a Fitbit, connected TVs, and the Internet of Things, and the concept of cross-device tracking expands to potentially include anything that gives off a signal.
The ad industry is drooling over this technology because it can follow and target us as we move through our daily routines, whether we are searching on our desktop, surfing on our iPad, or out on the town with our phone in hand.

There are two methods to track people across devices. The more precise technique is deterministic tracking, which links devices to a single user when that person logs into the same site from a desktop computer, phone, and tablet. This is the approach used by Internet giants like Facebook, Twitter, Google, and Apple, all of which have enormous user bases that log into their mobile and desktop properties.
A quick glance at Facebook's data privacy policy shows it records just about everything we do, including the content we provide, who we communicate with, what we look at on its pages, as well as information about us that our friends provide. Facebook saves payment information, details about the devices we use, location info, and connection details. The social network also knows when we visit third-party sites that use its services (such as the Like button, Facebook Log In, or the company's measurement and advertising services). It also collects information about us from its partners.

Most of the tech giants have similar policies and they all emphasize that they do not share personally identifiable information with third parties. Facebook, for example, uses our data to deliver ads within its walled garden but says it does not let outsiders export our information. Google says it only shares aggregated sets of anonymized data.

Read the full story…



Homeland Security Seeks State-Of-The-Art Automated Social Media Analytics Software

TN Note: DHS can draw on intelligence information from any other agency, but feels that it needs yet more advanced software tools to analyze social media in order to find evil-doers. The RFI gives lip-service to "protect the privacy, civil rights and civil liberties of individuals involved in open source and social media communications" but the intent to spy on all Americans is clear. Data collection and monitoring is the heartbeat of Technocracy, because one of the first rules of engineering states that you cannot control what you cannot monitor.

The Department of Homeland Security wants businesses to present their cutting-edge social media analytics services next month — especially technology that could enhance criminal investigations, traveler screenings and situational awareness.

In a new request for information, DHS said it is looking for open source analytics tools that can make internal operations more efficient and

reduce costs through “advanced analytic automation,” across the department, all while using “privacy, civil rights and civil liberties-protecting analytic methods.”

Respondents have until Feb. 9 to submit descriptions of their analytics capabilities, including geospatial processing, foreign and spoken language processing, and keyword, image and video analysis, among other elements.

DHS plans to ask 30 “exemplars of social media analytics capabilities in the market place” to present technology that could help analysts find patterns “in the context of homeland security investigative, screening and/or homeland security mission related situation awareness missions.”

Those groups will be asked to present on Feb. 26, the RFI said.

The solicitation also asked respondents to describe the way they “protect the privacy, civil rights and civil liberties of individuals involved in open source and social media communications,” including factors such as data removal methods, “role based access to information, user audit, system logging, policy enforcing mechanisms, encryption, etc.”

The announcement comes weeks after federal social media screening policies came under fire, especially in light of the San Bernardino shootings, when it was widely reported that one of the shooters had posted public pro-ISIS messages on Facebook. (Federal Bureau of Investigation director James Comey subsequently said those were private, direct communications.)

DHS policies in particular were criticized last month when Congress blasted the department for not examining immigrants’ social media accounts closely and routinely when granting visas, *The Hill* reported.

Read the full story here…

NSA Harvesting Millions Of Faces From Internet Images

TN Note: The NSA has been slapped every which way by Congress to quit indiscriminate spy operations on Americans, but technocrats as they are, they ignore Congress and continue on their mission. Remember that the NSA is fully controlled (e.g., both funding and operations) by the Director of National Intelligence, who is currently James R. Clapper. Since George W. Bush established the agency in 2005 and handed all of the nation's intelligence agencies over to it, two DNIs have been members of the Trilateral Commission: **John Negroponte** (3/2005-2/2007) and **Adm. Dennis C. Blair** (1/2009-5/2010). One can safely conclude that the entire intelligence community, including the NSA, is acting on behalf of those attempting to implement Technocracy in our nation.

The National Security Agency is harvesting huge numbers of images of people from communications that it intercepts through its global surveillance operations for use in sophisticated facial recognition programs, according to top-secret documents.

The spy agency's reliance on facial recognition technology has grown significantly over the last four years as the agency has turned to new software to exploit the flood of images included in emails, text messages, social media, videoconferences and other communications, the N.S.A. documents reveal. Agency officials believe that technological advances could revolutionize the way that the N.S.A. finds intelligence targets around the world, the documents show. The agency's ambitions for this highly sensitive ability and the scale of its effort have not previously been disclosed.

The agency intercepts "millions of images per day" — including about 55,000 "facial recognition quality images" — which translate into "tremendous untapped potential," according to 2011 documents obtained from the former agency contractor Edward J. Snowden. While once focused on written and oral communications, the N.S.A. now considers facial images, fingerprints and other identifiers just as important to its mission of tracking suspected terrorists and other intelligence targets, the documents show.

"It's not just the traditional communications we're after: It's taking a full-arsenal approach that digitally exploits the clues a target leaves behind in their regular activities on the net to compile biographic and biometric information" that can help "implement precision targeting," noted a 2010 document.

One N.S.A. PowerPoint presentation from 2011, for example, displays several photographs of an unidentified man — sometimes bearded, other times clean-shaven — in different settings, along with more than two dozen data points about him. These include whether he was on the Transportation Security Administration no-fly list, his passport and visa status, known associates or suspected terrorist ties, and comments made about him by informants to American intelligence agencies.

It is not clear how many people around the world, and how many Americans, might have been caught up in the effort. Neither federal privacy laws nor the nation's surveillance laws provide specific protections for facial images. Given the N.S.A.'s foreign intelligence mission, much of the imagery would involve people overseas whose data

was scooped up through cable taps, Internet hubs and satellite transmissions.

Because the agency considers images a form of communications content, the N.S.A. would be required to get court approval for imagery of Americans collected through its surveillance programs, just as it must to read their emails or eavesdrop on their phone conversations, according to an N.S.A. spokeswoman. Cross-border communications in which an American might be emailing or texting an image to someone targeted by the agency overseas could be excepted.

Read full story here…