Origins of Google

By

Anthony Patch

Today, I will take you back in time to the origins of many well-known technology companies, including Google, displaying their existence as it relates to today's parabolic explosion of the interrelated AI (artificial intelligence), more accurately labeled 'cognitive intelligence', and, blockchain serving as I've coined the process of "raising the IQ of AI". Virtually, the underpinnings of the present "beast system" of Revelation 13: 16-17:

[16] And he causes all, both small and great, rich and poor, free and bond, to receive a mark in their right hand, or in their foreheads: [17] And that no man might buy or sell, save he that had the mark, or the name of the beast, or the number of his name.

The NSA (National Security Agency) describes digital information systems as both a great source of vulnerability and as powerful tools and weapons for national security. The agency advocates the need for US cyber intelligence to maximize in-depth knowledge of potential and actual adversairies, so they (intelligence agencies) can identify every potential leverage points that can be exploited for deterrence or retaliation. A networked deterrence requiring the US intelligence community as a whole to develop a deep understanding and specific knowledge about the particular networks involved and their patterns of linkages, including types and strengths of bonds, as well as using cognitive and behavioral science to help predict patterns. This describes the theoretical architecture for modelling data obtained from surveillance and social media mining on potential adversaries and counterparties.

Please refer to the many articles I have constructed and published within the past issues of Entangled magazine illustrating how quantum computing is used in the discovery of patterns deeply hidden within 'Big Data'. Mining for what I refer to as the "golden nuggets of data" buried within the increasing granularity of data streaming in from the edges of computing, including nanocomputers functioning as sensors throughout the world's environment.

In demonstration of the deliberate obfuscation in the building out of the beast system, I would like to point toward the US Defense Science Board Task Force receiving briefings and reports commissioned by Bush appointee James Clapper, then Undersecretary of Defense for Intelligence and under Obama as Director of National Intelligence, in which capacity he lied under oath to Congress by claiming in March, 2013 that the NSA does not collect *any* data at all on American citizens.

The Defense Science Board (DSB) *Task Force on Defense Intelligence* published its report on *Counterinsurgency (COIN), Intelligence, Surveillance and Reconnaissance (IRS) Operations.* The report named 24 countries in South and Southeast Asia, North and West Africa, the Middle East and South America, which would pose "possible COIN challenges" for the US military in coming years. These included Pakistan, Mexico, Yemen, Nigeria, Guatemala, Gaza/West Bank, Egypt, Saudi Arabia, Lebanon, among other "autocratic regimes." The report argued that "economic crises, climate change, demographic pressures, resource scarcity, or poor governance could cause these states (or others) to fail or become so weak that they become targets for aggressors/insurgents." From there, the "global information infrastructure" and "social media" can rapidly "amplify the speed, intensity, and momentum of events" with regional implications. "Such areas could become sanctuaries from which to launch attacks on the US homeland, recruit personnel, and finance, train, and supply operations."

As readers of my Entangled magazine, and members of my radio audience, you no doubt see the handwriting on the wall. Not only with respect to citizens of countries other than the US, but to those within its own borders. And, given the international influence of US-centric technology companies like Google, no one is immune from worldwide virtual surveillance operations conducted by and within every nation.

The imperative in this context is to increase the US military's capacity for left of bang operations—before the need for a major armed forces commitment—to avoid insurgencies, or pre-empt them while still in incipient phase. Noting that the Internet and social media are critical sources of social network analysis data in societies that are not only literate, but also connected to the Internet. Thus, a requirement for monitoring the blogosphere and other social media across many different cultures and languages to prepare for population-centric operations.

The Pentagon continually seeks to increase its capacity for behavioral modeling and simulation to better understand and anticipate the actions of a population based on foundation data on populations, human networks, geography, and other economic and social characteristics. Such population-centric operations will also increasingly be needed in nascent resource conflicts, whether based on water-crises, agricultural stress, environmental stress, or rents from mineral resources. This includes monitoring population demographics as an organic part of the natural resource framework.

Other areas for augmentation are overhead video surveillance, high resolution terrain data, cloud computing capability, and data fusion for all forms of intelligence in a consistent spatio-temporal framework for organizing and indexing the data, developing social science frameworks that can support spatio-temporal encoding and analysis, distributing multi-form biometric authentication technologies, such as fingerprints, retina scans and DNA samples to the point of service of the most basic administrative processes in order to tie identity to all of an individual's transactions. On an ongoing basis, the Pentagon develops anthropological, socio-cultural, historical, human geographical, educational, public health, and many other types of social and behavioral science data and information in developing a deep understanding of populations.

Again, please recall the extensive explanations and coverage I have provided within Entangled magazine and on my radio programs regarding the SWS (Sentient World Simulation) originating in 2006 out of Purdue University.
https://www.krannert.purdue.edu/academics/mis/workshop/ac2_100606.pdf

In 2012, then NSA chief General Keith Alexander was emailing Google's founding executive Sergey Brin to discuss information sharing for national security. In those emails, obtained under Freedom of Information by investigative journalist Jason Leopold, Gen. Alexander described Google as a "key member of (the US military's) Defense Industrial Base." Brin's jovial relationship with the former NSA chief now makes perfect sense given that Brin had been in contact with representatives of the CIA and NSA, who partly funded and oversaw his creation of the Google search engine, since the mid-1990s.

In July 2014, the US Army formed a panel on the creation of a "rapid acquisition cell" to advance the US Army's "cyber capabilities" as part of the Force 2025 (http://www.arcic.army.mil/Initiatives/force-2025-beyond.aspx) transformation initiative. The overarching goal of this panel is captured within this citation: "many of the Army's 2025 technology goals can be realized with commercial technology available or in development today," re-affirming that "industry is ready to partner with the Army in supporting the new paradigm." Around the same time, most of the media was trumpeting the idea that Google was trying to distance itself from Pentagon funding, but in reality, Google had switched tactics to independently develop commercial technologies which would have military applications in satisfying the Pentagon's transformation goals.

Google bought the satellite mapping software Keyhole from the CIA's own venture capital firm In-Q-Tel in 2004. The focus at the time was and remains upon identifying, researching and evaluating new start-up technology firms that were/are believed to offer tremendous value to the CIA, the NGA (National Geospatial-Intelligence Agency), and the DIA (Defense Intelligence Agency). Indeed, the NGA had confirmed that its intelligence obtained via Keyhole was used by the NSA to support US operations in Iraq from 2003 onwards. Keyhole is now known as Google Earth Enterprise.

In 2007, the *Washington Post* reported that Google was "in the beginning stages" of selling advanced "secret versions" of its products to the US government. "Google has ramped up its sales force in the Washington area in the past year to adapt its technology products to the needs of the military, civilian agencies and the intelligence community," the *Post* reported. The Pentagon was already using a version of Google Earth developed in partnership with Lockheed Martin to "display information for the military on the ground in Iraq," including "mapping out displays of key regions of the country" and outlining "Sunni and Shiite neighborhoods in Baghdad, as well as US and Iraqi military bases in the city. Neither Lockheed nor Google would say how the geospatial agency uses the data." Google aimed to sell the government new "enhanced versions of Google Earth" and "search engines that can be used internally by agencies."

Please note my reporting of Lockheed as one of the first commercial purchasers of D-Wave System's newly produced 128-qubit quantum computer, again fully detailed within Entangled magazine and on my radio programs.

White House records leaked in 2010 showed that Google executives had held several meetings with senior US National Security Council officials. Alan Davidson, Google's government affairs director, had at least three meetings with officials of the National Security Council in 2009, including White House senior director for Russian affairs Mike McFaul and Middle East advisor Daniel Shapiro. It also emerged from a Google patent application that the company had deliberately been collecting 'payload' data from private wifi networks that would enable the identification of "geolocations." In the same year, we now know, Google had signed an agreement with the NSA giving the agency open-ended access to the personal information of its users, and its hardware and software, in the name of cyber security—agreements quickly replicated with hundreds of telecoms CEOs around the country.

Thus, it is not just Google that is a key contributor and foundation of the US military-industrial-intelligence complex: it is the entire Internet, and the wide range of private sector companies—many nurtured and funded under the mantle of the US intelligence community (or powerful financiers embedded in that community)—which sustain the Internet and the telecoms infrastructure; it is also the myriad of start-ups selling cutting edge technologies to the CIA's venture firm In-Q-Tel, where they can then be adapted and advanced for applications across the military intelligence community. Ultimately, the global surveillance apparatus and the classified tools used by agencies like the NSA to administer it, have been almost entirely made by external researchers and private contractors like Google, which operate outside the Pentagon.

This structure allows the Pentagon to rapidly capitalize on technological innovations it would otherwise miss, while also keeping the private sector at arms length, at least ostensibly, to avoid uncomfortable questions about what such technology is actually being used for.

The Pentagon is about war, whether overt or covert. By helping build the technological surveillance infrastructure of the NSA, firms like Google are complicit in what the military-industrial-intelligence complex does best: kill for cash.

As the nature of mass surveillance suggests, its target is not merely terrorists, but by extension, terrorism suspects and potential terrorists, the upshot being that entire populations—especially political activists—must be targeted by US intelligence surveillance to identify active and future threats, and to be vigilant against hypothetical populist insurgencies both at home and abroad. Predictive analytics and behavioral profiles play a pivotal role here. Something CI (Cognitive Intelligence) was built upon and continues raising its IQ (Intelligence Quotient) through ongoing build out of the blockchain system forming the infrastructure of the beast system labeled the SWS (Sentient World Simulation). It should be noted here that a close partner software developer to D-Wave Systems is Palantir (https://www.palantir.com/) in the operation of the SWS.

Mass surveillance and data-mining as now conducted by a business subsidiary of D-Wave Systems, Quadrant (https://quadrant.ai/) which has a distinctive operational purpose in assisting with the lethal execution of special operations, selecting targets for the CIA's drone strike kill lists via dubious algorithms, for instance, along with providing geospatial and other information for combatant commanders on land, air and sea, among many other functions. A single social media post on Twitter or Facebook is enough to trigger being placed on secret terrorism watch-lists solely due to a vaguely defined hunch or suspicion; and can potentially even land a suspect on a kill list.

The push for indiscriminate, comprehensive mass surveillance by the military-industrial-intelligence complex—encompassing the Pentagon, intelligence agencies, defense contractors, and supposedly friendly tech giants like Google and Facebook—is therefore not an end in itself, but an instrument of power, whose goal is self-perpetuation. But there is also a self-rationalizing justification for this goal: while being great for the military-industrial-intelligence complex, it is also, supposedly, great for everyone else. While in actuality, these data systems are for the ruling elite hell-bent in serving their god, Satan himself.

And now, in conclusion of what undoubtably will be an on-going series of articles on technology giants such as Google, is the pièce de résistance entitled:

What can you do with a Web in your Pocket?

Authors: Sergey Brin Rajeev Motwani Lawrence Page Terry Winograd

Abstract:

The amount of information available online has grown enormously over the past decade. Fortunately, computing power, disk capacity, and network bandwidth have also increased dramatically. It is currently possible for a university research project to store and process the entire World Wide Web. Since there is a limit on how much text humans can generate, it is plausible that within a few decades one will be able to store and process all the human-generated text on the Web in a shirt pocket. The Web is a very rich and interesting data source. In this paper, we describe the Stanford WebBase, a local repository of a significant portion of the Web. Furthermore, we describe a number of recent experiments that leverage the size and the diversity of the WebBase. First, we have largely automated the process of extracting a sizable relation of books (title, author pairs) from hundreds of data sources spread across the World Wide Web using a technique we call Dual Iterative Pattern Relation Extraction. Second, we have developed a global ranking of Web pages called PageRank based on the link structure of the Web that has properties that are useful for search and navigation. Third, we have used PageRank to develop a novel search engine called Google, which also makes heavy use of anchor text. All of these experiments rely significantly on the size and diversity of the WebBase.

http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.36.2806&rep=rep1&type=pdf

Two decades ago, the US intelligence community worked closely with Silicon Valley in an effort to track citizens in cyberspace. And Google is at the heart of that origin story. Some of the research that led to Google's ambitious creation was funded and coordinated by a research group established by the intelligence community to find way to track individuals and groups online.

The intelligence community hoped that the nations leading computer scientists could take non-classified information and user data, and combine it with what would become known as the internet, and begin to create for-profit, commercial enterprises to suit the needs of both the intelligence community and the public. They hoped to direct the supercomputing revolution from the start in order to make sense of what millions of human beings did inside this digital information network. That collaboration has made a comprehensive public-private mass surveillance state possible today.

The story of the deliberate create of the modern mass-surveillance state includes elements of Google's surprising, and largely unknown, origin. It is a somewhat different creation story than the one the public has heard, and explains what Google cofounders Sergey Brin and Larry Page set out to build, and why.

However, this isn't just about the origin story of Google. It's the story of the mass-surveillance state, and the government money that funded it all.

In the mid 1990s, the intelligence community in America began to realize that they had an opportunity. The supercomputing community was just beginning to migrate from university settings into the private sector, led by investments from a place that would come to be known as Silicon Valley.

A digital revolution was underway. One that would transform the world of data gathering and how we make sense of massive amounts of information. The intelligence community wanted to shape Silicon Valley's supercomputing efforts at their inception so they would be useful for both military and homeland security purposes. The question was, could this supercomputing network, which would become capable of storing terabytes of information, make intelligent sense of the digital trail that human beings leave behind?

Answering this question was of great interest to the intelligence community. Intelligence-gathering may have been their world, but the CIA and the NSA had come to realize that their future was to be profoundly shaped outside the government. It was at a time when military and intelligence budgets within the Clinton administration were in jeopardy, and the private sector had vast resources at their disposal. If the intelligence community wanted to conduct mass surveillance for national security purposes, it would require cooperation between the government and the emerging supercomputing companies.

To do this, they began reaching out to the scientists at American universities who were creating this supercomputing revolution. These scientists were developing ways to do what no single group of human beings sitting at work stations in the CIA and the NSA could ever hope to do: namely, gather huge amounts of data and make intelligent sense of it. There was already a long history of collaboration between America's best scientists and the intelligence community, from the creation of the atomic bomb and satellite technology to efforts to put a man on the moon.

In fact, the internet itself was created because of an intelligence effort. In the 1970s, the agency responsible for developing emerging technologies for military, intelligence, and national security purposes, DAPRA (Defense Advanced Research Projects Agency), linked four supercomputers to handle massive data transfers. It handed the operations off to the NSF (National Science Foundation) a decade or so later, which proliferated the network across thousands of universities and, eventually, the public, thus creating the architecture and scaffolding of the World Wide Web. It was not incidentally, created at CERN, despite the popular notion spread by the intelligence community.

Silicon Valley was no different. By the mid 1990s, the intelligence community was seeding funding to the most promising supercomputing efforts across academia, guiding the creation of efforts to make massive amounts of information useful for both the private sector as well as the intelligence community.

They funded these computer scientists through an unclassified, highly compartmentalized program that was managed for the CIA and the NSA by large military and intelligence contractors. It was called MDDS (Massive Digital Data Systems) project.

MDDS was introduced to several dozen leading computer scientists at Stanford, CalTech, MIT, Carnegie Mellon, Harvard, and others in a white paper that described what the CIA, NSA, DARPA, and other agencies hoped to achieve. The research would largely be funded and managed by unclassified science agencies like NSF, which would allow the architecture to be scaled up in the private sector if it managed to achieve what the intelligence community hoped for.

"Not only are activities becoming more complex, but changing demands require that the IC [Intelligence Community] process different types as well as larger volumes of data," the intelligence community said in its 1993 MDDS white paper (https://groups.google.com/forum/#!topic/mail.cypherpunks/4CDiW59hS88): "Consequently, the IC is taking a proactive role in stimulating research in the efficient management of massive databases and ensuring that IC requirements can be incorporated or adapted into commercial products. Because the challenges are not unique to any one agency, the Community Management Staff (CMS) has commissioned a Massive Digital Data Systems [MDDS] Working Group to address the needs and to identify and evaluate possible solutions."

Over the next few years, the program's stated aim was to provide more than a dozen grants of several million dollars each to advance this research concept. The grants were to be delivered largely through the NSF so that the most promising, successful efforts could be captured as intellectual property and form the basis of companies attracting investments from Silicon Valley. This type of public-to-private innovation system helped launch powerful science and technology companies like Qualcomm, Symantec, Netscape, and others, and funded the pivotal research in areas like Doppler radar and fiber optics, which are central to large companies like AccuWeather, Verizon, and AT&T today. Today, the NSF provides nearly 90% of all federal funding for university-based computer-science research.

The research arms of the CIA and NSA hoped that the best computer-science minds in academia could identify what they called "birds of a feather". Just as geese fly together in large V-shapes, or flocks of sparrows make sudden movements together in harmony, they predicted that like-minded groups of humans would move together online. The intelligence community named their first unclassified briefing for scientists the "birds of a feather" briefing, and the "Birds of a Feather Session on the Intelligence Community Initiative in Massive Digital Data Systems" took place at the Fairmont Hotel in San Jose, California (Silicon Valley) in the spring of 1995.

Their research aim was to track digital fingerprints inside the rapidly expanding global information network, which was then known as the World Wide Web. It was not as is popularly repeated, begun at CERN.

Could an entire world of digital information be organized so that the requests humans made inside such a network be tracked and sorted? Could their queries be linked and ranked in order of importance? Could "birds of a feather" be identified inside this sea of information so that communities and groups could be tracked in an organized way?

By working with emerging commercial-data companies, their intent was to track like-minded groups of people across the internet and identify them from the digital fingerprints they left behind, much like forensic scientists use fingerprint smudges to identify criminals. Just as "birds of a feather flock together," they predicted that potential terrorists would communicate with each other in this new global, connected world, and they could find them by identifying patterns in this massive amount of new information. Once these groups were identified, they could then follow their digital trails everywhere.

In 1995, one of the first and most promising MDDS grants went to a computer-science research team at Stanford University with a decade-long history of working with NSF and DARPA grants. The primary objective of this grant was "query optimization of very complex queries that are described using the 'query flocks' approach." A second grant, the NSF/DARPA grant most closely associated with Google's origin, was part of a coordinated effort to build a massive digital library using the internet as its backbone. Both grants funded research by two graduate students who were making rapid advances in web-page ranking, as well as tracking (and making sense of) user queries: future Google cofounders Sergey Brin and Larry Page.

The research by Brin and Page under these grants became the heart of Google: people using search functions to find precisely what they wanted inside a very large data set. The intelligence community however, saw a slightly different benefit in their research: Could the network be organized so efficiently that individual users could be uniquely identified and tracked?

This process is perfectly suited for the purposes of counter-terrorism and homeland security efforts: Human beings and like-minded groups who might pose a threat to national security and can be uniquely identified online before they do harm. This explains why the intelligence community found Brin's and Page's research efforts so appealing: prior to this time, the CIA largely used human intelligence efforts in the field to identify people and groups that might pose threats. The ability to track them virtually (in conjunction with efforts in the field) would change everything.

It was the beginning of what in just a few years' time would become Google. The two intelligence-community managers charged with leading the program met regularly with Brin as his research progressed, and he was an author on several research papers that resulted from this MDDS grant before he and Page left to form Google.

The grants allowed Brin and Page to do their work and contributed to their breakthroughs in web-page ranking and tracking user queries. Brin didn't work for the intelligence community, or for anyone else. Google had not yet been incorporated. He was just a Stanford researched taking advantage of the grant provided by the NSA and CIA through the unclassified MDDS program.

The MDDS research effort has never been part of Google's origin story, even though the principal investigator for the MDDS grant specifically named Google as directly resulting from their research: "It's core technology, which allows it to find pages far more accurately than other search engines, was partially supported by this grant," he wrote. In a published research paper that includes some to Brin's pivotal work, the authors reference the NSF grants that was created by the MDDS program.

Instead, every Google creation story only mentions just one federal grant: the NSF/DARPA "digital libraries" grant, which was designed to allow Stanford researchers to search the entire World Wide Web stored on the university's servers at the time. The development of the Google algorithms was carried on a variety of computers, mainly provided by the NSF-DARPA-NSA-funded Digital Library project at Stanford," Stanford's Infolab says of its origin, for example. NSF likewise only references the digital libraries grant, not the MDDS grant as well, in its own history of Google's origin. In the famous research paper, "The Anatomy of a Large-Scale Hypertextual Web Search Engine," which describes the creation of Google, Brin and Page thanked the NSF and DARPA for its digital library grant to Stanford. But the grant from the intelligence community's MDDS program, specifically designed for the breakthrough that Google was built upon, has faded into obscurity.

Google has said in the past that it was not funded or created by the CIA. For instance, when stories circulated in 2006 that Google had received funding from the intelligence community for years to assist in counter-terrorism efforts, the company told Wired magazine founder John Battelle, "The statements related to Google are completely untrue."

Did the CIA directly fund the work of Brin and Page, and therefore create Google? No. But were Brin and Page researching precisely what the NSA, the CIA, and the intelligence community hoped for, assisted by their grants? Absolutely.