GlobalResearch
Center for Research on Globalization

Invasive Cyber Technologies and Internet Privacy: Big Brother is only a "Ping" or Mouse Click Away

By Tom Burghardt
Global Research, October 11, 2010
Antifascist Calling... 10 October 2010

Region: USA
Theme: Intelligence

As they walked along the busy, yellow-lit tiers of offices, Anderton said: "You're acquainted with the theory of precrime, of course. I presume we can take that for granted."– Philip K. Dick, The Minority Report

What do Google, the CIA and a host of so-called "predictive behavior" start-ups have in common?

They're interested in you, or more specifically, whether your online interests–from Facebook to Twitter posts, and from Flickr photos to YouTube and blog entries–can be exploited by powerful computer algorithms and subsequently transformed into "actionable intelligence."

And whether the knowledge gleaned from an IP address is geared towards selling useless junk or entering a name into a law enforcement database matters not a whit. It's all "just data" and "buzz" goes the mantra, along what little is left of our privacy and our rights.

Increasingly, secret state agencies ranging from the CIA to the National Security Agency are pouring millions of dollars into data-mining firms which claim they have a handle on who you are or what you might do in the future.

And to top it off, the latest trend in weeding-out dissenters and nonconformists from the social landscape will soon be invading a workplace near you; in fact, it already has.

Welcome to the sinister world of "Precrime" where capitalist grifters, drug- and torture-tainted spy shops are all laboring mightily to stamp out every last vestige of free thought here in the heimat.

The CIA Enters the Frame

In July, security journalist Noah Shachtman revealed in Wired that "the investment arms of the CIA and Google are both backing a company that monitors the web in real time–and says it uses that information to predict the future."

Shachtman reported that the CIA's semi-private investment company, In-Q-Tel, and Google Ventures, the search giant's business division had partnered-up with a dodgy outfit called Recorded Future pouring, according to some estimates, $20 million dollars into the fledgling firm.

A blurb on In-Q-Tel's web site informs us that "Recorded Future extracts time and event information from the web. The company offers users new ways to analyze the past, present,

and the predicted future."

Who those ubiquitous though nameless "users" are or what they might do with that information once they "extract" it from the web is left unsaid. However, judging from the interest that a CIA-connected entity has expressed in funding the company, privacy will not figure prominently in the "new ways" such tools will be used.

Wired reported that the company, founded by former Swedish Army Ranger Christopher Ahlberg, "scours tens of thousands of websites, blogs and Twitter accounts to find the relationships between people, organizations, actions and incidents–both present and still-to-come."

"The cool thing is" Ahlberg said, "you can actually predict the curve, in many cases."

And as for the search giant's interest in "predicting the future" for the secret state, it wouldn't be the first time that Google Ventures sold equipment and expertise to America's shadow warriors.

While the firm may pride itself on the corporate slogan, "don't be evil," data is a valuable commodity. And where's there value, there's money to be made. Whether it comes in the form of "increasing share value" through the sale of private information to marketeers or state intelligence agencies eager to increase "situational awareness" of the "battlespace" is a matter of complete indifference to corporate bean counters.

After all, as Google CEO Eric Schmidt told CNBC last year, "if you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place."

But that standard, "only bad people have something to hide," is infinitely mutable and can be stretched–or manipulated as has so often been the case in the United States–to encompass everything from "Papist" conspiracies, "illegal" migrants, homosexuality, communism, drug use, or America's latest bête noire: the "Muslim threat."

Schmidt went on to say that "the reality is that search engines, including Google, do retain this information for some time. And we're all subject, in the U.S., to the Patriot Act, and it is possible that that information could be made available to the authorities."

In February, The Washington Post reported that "the world's largest Internet search company and the world's most powerful electronic surveillance organization are teaming up in the name of cybersecurity."

"The alliance" between Google and NSA "is being designed to allow the two organizations to share critical information without violating Google's policies or laws that protect the privacy of Americans' online communications," the Post alleged.

An anonymous source told the Post that "the deal does not mean the NSA will be viewing users' searches or e-mail accounts or that Google will be sharing proprietary data."

Really?

Last spring it was revealed that Google's Street View cars had been secretly vacuuming up terabytes of private wi-fi data for more than three years across Europe and the United States.

The Sunday Times reported that the firm had "been scooping up snippets of people's online activities broadcast over unprotected home and business wi-fi networks."

In July, The Washington Post's "Top Secret America" investigation disclosed that Google supplies mapping and search products to the U.S. secret state and that their employees, outsourced intelligence contractors for the Defense Department, may have filched their customers' wi-fi data as part of an NSA surveillance project.

And what about email and web searches? Last year, The New York Times revealed that NSA intercepts of "private telephone calls and e-mail messages of Americans are broader than previously acknowledged." In fact, a former NSA analyst described how he was trained-up fierce in 2005 "for a program in which the agency routinely examined large volumes of Americans' e-mail messages without court warrants."

That program, code-named PINWALE, and the NSA's meta-data-mining spy op STELLAR WIND, continue under Obama. Indeed, The Atlantic told us at the time that PINWALE "is actually an unclassified proprietary term used to refer to advanced data-mining software that the government uses."

But the seamless relationships amongst communications' giants such as Google and the secret state doesn't stop there.

Even before Google sought an assist from the National Security Agency to secure its networks after an alleged breech by China last year, in 2004 the firm had acquired Keyhole, Inc., an In-Q-Tel funded start-up that developed 3-D-spy-in-the-sky images; Keyhole became the backbone for what later evolved into Google Earth.

At the time of their initial investment, In-Q-Tel said that Keyhole's "strategic relationship … means that the Intelligence Community can now benefit from the massive scalability and high performance of the Keyhole enterprise solution."

In-Q-Tel's then-CEO, Gilman Louie, said that spy shop venture capitalists invested in the firm "because it offers government and commercial users a new capability to radically enhance critical decision making. Through its ability to stream very large geospatial datasets over the Internet and private networks, Keyhole has created an entirely new way to interact with earth imagery and feature data."

Or, as seen on a daily basis in the AfPak "theatre" deliver exciting new ways to kill people. Now that's innovation!

That was then, now the search giant and the CIA's investment arm are banking on products that will take privacy intrusions to a whole new level.

A promotional offering by the up-and-comers in the predictive behavior marketplace, Recorded Future–A White Paper on Temporal Analytics asserts that "unlike traditional search engines which focus on text retrieval and leaves the analysis to the user, we strive to provide tools which assist in identifying and understanding historical developments, and which can also help formulate hypotheses about and give clues to likely future events. We have decided on the term 'temporal analytics' to describe the time oriented analysis tasks supported by our systems."

Big in the hyperbole department, Recorded Future claims to have developed an "analytics engine, which goes beyond search, explicit link analysis and adds implicit link analysis, by looking at the 'invisible links' between documents that talk about the same, or related, entities and events. We do this by separating the documents and their content from what they talk about."

According to the would-be Big Brother enablers, "Recorded Future also analyzes the 'time and space dimension' of documents–references to when and where an event has taken place, or even when and where it will take place–since many documents actually refer to events expected to take place in the future."

Adding to the unadulterated creep factor, the technocratic grifters aver they're "adding more components, e.g. sentiment analyses, which determine what attitude an author has towards his/her topic, and how strong that attitude is–the affective state of the author."

Strongly oppose America's imperial project to steal other people's resources in Afghanistan and Iraq, or, crime of crimes, have the temerity to write or organize against it? Step right this way, Recorded Future has their eye on you and will sell that information to the highest bidder!

After all, as Mike Van Winkle, a California Anti-Terrorism Information Center shill infamously told the Oakland Tribune back in 2003 after Oakland cops wounded scores of peacenik longshoremen at an antiwar rally at the port: "You can make an easy kind of a link that, if you have a protest group protesting a war where the cause that's being fought against is international terrorism, you might have terrorism at that (protest). You can almost argue that a protest against that is a terrorist act."

And with Recorded Future's "sentiment analyses" such "links" will be even easier to fabricate.

Never mind that the prestigious National Academy of Science's National Research Council issued a scathing 2008 report, Protecting Individual Privacy in the Struggle Against Terrorists: A Framework for Assessment, that debunked the utility of data-ming and link analysis as effective counterterrorism tools.

"Far more problematic," the NRC informs us, "are automated data-mining techniques that search databases for unusual patterns of activity not already known to be associated with terrorists." Since "so little is known about what patterns indicate terrorist activity" the report avers, dodgy techniques such as link analysis "are likely to generate huge numbers of false leads."

As for Recorded Future's over-hyped "sentiment analyses," the NRC debunked, one might even say preemptively, the dodgy claims of our would-be precrime mavens. "The committee also examined behavioral surveillance techniques, which try to identify terrorists by observing behavior or measuring physiological states."

Their conclusion? "There is no scientific consensus on whether these techniques are ready for use at all in counterterrorism." Damningly, the NRC asserted that such techniques "have enormous potential for privacy violations because they will inevitably force targeted individuals to explain and justify their mental and emotional states."

Not that such inconvenient facts matter to Recorded Future or their paymasters in the so-

called intelligence community who after all, are in the driver's seat when the firm's knowledge products "make predictions about the future."

After all, as Ahlberg and his merry band of privacy invaders inform us: "Our mission is not to help our customers find documents, but to enable them to understand what is happening in the world."

The better to get a leg up on the competition or know who to target.

The "Real You"

Not to be outdone by black world spy agencies, their outsourced corporate partners or the futurist gurus who do their bidding, the high-tech publication Datamation, told us last month that the precrime concept "is coming very soon to the world of Human Resources (HR) and employee management."

Reporter Mike Elgan revealed that a "Santa Barbara, Calif., startup called Social Intelligence data-mines the social networks to help companies decide if they really want to hire you."

Elgan averred that while background checks have historically searched for evidence of criminal behavior on the part of prospective employees, "Social Intelligence is the first company that I'm aware of that systematically trolls social networks for evidence of bad character."

Similar to Recorded Future and dozens of other "predictive behavior" companies such as Attensity and Visible Technologies, Social Intelligence deploys "automation software that slogs through Facebook, Twitter, Flickr, YouTube, LinkedIn, blogs, and 'thousands of other sources,' the company develops a report on the 'real you'–not the carefully crafted you in your resume."

According to Datamation, "the company also offers a separate Social Intelligence Monitoring service to watch the personal activity of existing employees on an ongoing basis." Such intrusive monitoring transforms the "workplace" into a 24/7 Orwellian panopticon from which there is no hope of escape.

The service is sold as an exemplary means to "enforce company social media policies." However, since "criteria are company-defined, it's not clear whether it's possible to monitor personal activity." Fear not, it is.

Social Intelligence, according to Elgan, "provides reporting that deemphasizes specific actions and emphasizes character. It's less about 'what did the employee do' and more about 'what kind of person is this employee?'"

In other words, it's all about the future; specifically, the grim world order that fear-mongering corporations are rapidly bringing to fruition.

Datamation reports that "following the current trend lines," rooted in the flawed logic of information derived from data-mining and link analysis, "social networking spiders and predictive analytics engines will be working night and day scanning the Internet and using that data to predict what every employee is likely to do in the future. This capability will simply be baked right in to HR software suites."

As with other aspects of daily life in post-constitutional America, executive decisions, ranging from whether or not to hire or fire someone, cast them into a lawless gulag without trial, or even kill them solely on the say-so of our War-Criminal-in-Chief, are the new house rules.

Like our faux progressive president, some HR bureaucrat will act as judge, jury and executioner, making decisions that can–and have–wrecked lives.

Elgan tells us that unlike a criminal proceeding where you stand before the law accused of wrongdoing and get to face your accuser, "you can't legally be thrown in jail for bad character, poor judgment, or expectations of what you might do in the future. You have to actually break the law, and they have to prove it."

"Personnel actions aren't anything like this." You aren't afforded the means to "face your accuser." In fact, based on whether or not you sucked-up to the boss, pissed-off some corporate toady, or moved into the "suspect" category based on an algorithm, you don't have to actually violate comapny rules in order to be fired "and they don't have to prove it."

Datamation tells us, "if the social network scanning, predictive analytics software of the future decides that you are going to do something in future that's inconsistent with the company's interests, you're fired."

And, Elgan avers, now that "the tools are becoming monstrously sophisticated, efficient, powerful, far-reaching and invasive," the precrime "concept is coming to HR."

Big Brother is only a "ping" or mouse click away…

Articles by: Tom Burghardt
http://antifascist-calling.blogspot.com/