Mind Your Tweets: The CIA Social Networking Surveillance System

From Wikileaks

October 24, 2009

By Tom Burghardt *(Global Research)*[1] (http://www.globalresearch.ca/index.php?context=va&aid=15827)

That social networking sites and applications such as Facebook, Twitter and their competitors can facilitate communication and information sharing amongst diverse groups and individuals is by now a cliché.

It should come as no surprise then, that the secret state and the capitalist grifters whom they serve, have zeroed-in on the explosive growth of these technologies. One can be certain however, securocrats aren't tweeting their restaurant preferences or finalizing plans for after work drinks.

No, researchers on both sides of the Atlantic are busy as proverbial bees building a "total information" surveillance system, one that will, so they hope, provide police and security agencies with what they euphemistically call "actionable intelligence."

Build the Perfect Panopticon, Win Fabulous Prizes!

In this context, the whistleblowing web site Wikileaks published a remarkable document October 4 by the INDECT Consortium, the Intelligence Information System Supporting Observation, Searching and Detection for Security of Citizens in Urban Environment.

Hardly a catchy acronym, but simply put INDECT is working to put a human face on the billions of emails, text messages, tweets and blog posts that transit cyberspace every day; perhaps your face.

According to Wikileaks, INDECT's "Work package 4" is designed "to comb web blogs, chat sites, news reports, and social-networking sites in order to build up automatic dossiers on individuals, organizations and their relationships." Ponder that phrase again: "automatic dossiers."

This isn't the first time that European academics have applied their "knowledge skill sets" to keep the public "safe"--from a meaningful exercise of free speech and the right to assemble, that is.

Last year The Guardian reported that Bath University researchers' Cityware project covertly tracked "tens of thousands of Britons" through the installation of Bluetooth scanners that capture "radio signals transmitted from devices such as mobile phones, laptops and digital cameras, and using the data to follow unwitting targets without their permission."

One privacy advocate, Simon Davies, the director of Privacy International, told The Guardian: "This technology could well become the CCTV of the mobile industry. It would not take much adjustment to make this system a ubiquitous surveillance infrastructure over which we have no control."

Which of course, is precisely the point.

As researchers scramble for a windfall of cash from governments eager to fund these dubious projects, European police and security agencies aren't far behind their FBI and NSA colleagues in the spy game.

The online privacy advocates, Quintessenz, published a series of leaked documents in 2008 that described the network monitoring and data mining suites designed by Nokia Siemens, Ericsson and Verint.

The Nokia Siemens Intelligence Platform dubbed "intelligence in a box," integrate tasks generally done by separate security teams and pools the data from sources such as telephone or mobile calls, email and internet activity, bank transactions, insurance records and the like. Call it data mining on steroids.

Ironically enough however, Siemens, the giant German electronics firm was caught up in a global bribery scandal that cost the company some $1.6 billion in fines. Last year, The New York Times described "a web of secret bank accounts and shadowy consultants," and a culture of "entrenched corruption ... at a sprawling, sophisticated corporation that externally embraced the nostrums of a transparent global marketplace built on legitimate transactions."

According to the Times, "at Siemens, bribery was just a line item." Which just goes to show, powering the secret state means never having to say you're sorry!

Social Network Spying, a Growth Industry Fueled by Capitalist Grifters

The trend by security agencies and their corporate partners to spy on their citizens has accelerated greatly in the West since the 9/11 terrorist attacks.

This multi-billion industry in general, has been a boon for the largest American and European defense corporations. Among the top ten companies listed by Washington Technology in their annual ranking of the "Top 100" prime government contractors, all ten--from Lockheed Martin to Booz Allen Hamilton--earned a combined total of $68 billion in 2008 from defense and related homeland security work for the secret state.

And like Siemens, all ten corporations figure prominently on the Project on Government Oversight's Federal Contractor Misconduct Database (FCMD), which tracks "contract fraud, environmental, ethics, and labor violations." Talk about a rigged game!

Designing everything from nuclear missile components to eavesdropping equipment for various government agencies in the United States and abroad, including some of the most repressive regimes on the planet, these firms have moved into manufacturing the hardware and related computer software for social networking surveillance in a big way.

Wired revealed in April that the FBI is routinely monitoring cell phone calls and internet activity during criminal and counterterrorism investigations. The publication posted a series of internal documents that described the Wi-Fi and computer hacking capabilities of the Bureau's Cryptographic and Electronic Analysis Unit (CEAU).

New Scientist reported back in 2006 that the National Security Agency "is funding research into the mass harvesting of the information that people post about themselves on social networks."

And just this week in an exclusive report published by the British high-tech publication, The Register, it was revealed that "the government has outsourced parts of its biggest ever mass surveillance project to the disaster-prone IT services giant formerly known as EDS."

That work is being conducted under the auspices of the Government Communications Headquarters (GCHQ), the British state's equivalent of America's National Security Agency.

Investigative journalist Chris Williams disclosed that the American computer giant HP, which purchased EDS for some $13.9 billion last year, is "designing and installing the massive computing resources that will be needed to analyse details of who contacts whom, when where and how."

Work at GCHQ in Cheltenham is being carried out under "a secret project called Mastering the Internet." In May, a Home Office document surfaced that "ostensibly sought views on whether ISPs should be forced to gather terabytes of data from their networks on the government's behalf."

The Register reported earlier this year that telecommunications behemoth Detica and U.S. defense giant Lockheed Martin were providing GCHQ with data mining software "which searches bulk data, such as communications records, for patterns ... to identify suspects." (For further details see: Antifascist Calling, "Spying in the UK: GCHQ Awards Lockheed Martin £200m Contract, Promises to 'Master the Internet'," May 7, 2009)

It seems however, that INDECT researchers like their GCHQ/NSA kissin' cousins in Britain and the United States, are burrowing ever-deeper into the nuts-and-bolts of electronic social networking and may be on the verge of an Orwellian surveillance "breakthrough."

As New Scientist sagely predicted, the secret state most certainly plans to "harness advances in internet technology--specifically the forthcoming 'semantic web' championed by the web standards organisation W3C--to combine data from social networking websites with details such as banking, retail and property records, allowing the NSA to build extensive, all-embracing personal profiles of individuals."

Profiling Internet Dissent

Pretty alarming, but the devil as they say is in the details and INDECT's release of their "Work package 4" file makes for a very interesting read. And with a title, "XML Data Corpus: Report on methodology for collection, cleaning and unified representation of large textual data from various sources: news reports, weblogs, chat," rest assured one must plow through much in the way of geeky gibberish and tech-speak to get to the heartless heart of the matter.

INDECT itself is a rather interesting amalgamation of spooks, cops and academics.

According to their web site, INDECT partners include: the University of Science and Technology, AGH, Poland; Gdansk University of Technology; InnoTech DATA GmbH & Co., Germany; IP Grenoble (Ensimag), France; MSWiA, the General Headquarters of Police, attached to the Ministry of the Interior, Poland; Moviquity, Spain; Products and Systems of Information Technology, PSI, Germany; the Police Service of Northern Ireland, PSNI, United Kingdom (hardly slouches when it comes to stitching-up Republicans and other leftist agitators!); Poznan University of Technology; Universidad Carlos III de Madrid; Technical University of Sofia, Bulgaria; University of Wuppertal, Germany; University of York, Great Britain; Technical University of Ostrava, Czech Republic; Technical University of Kosice, Slovakia; X-Art Pro Division G.m.b.H, Austria; and finally, the Fachhochschule Technikum, also in Austria.

I don't know about you, but I find it rather ironic that the European Union, ostensible guardians of democracy and human rights, have turned for assistance in their surveillance projects to police and spy outfits from the former Soviet bloc, who after all know a thing or two when it comes to monitoring their citizens.

Right up front, York University's Suresh Manadhar, Ionnis Klapaftis and Shailesh Pandey, the principle authors of the INDECT report, make their intentions clear.

Since "security" as the authors argue, "is becoming a weak point of energy and communications infrastructures, commercial stores, conference centers, airports and sites with high person traffic in general," they aver that "access control and rapid response to potential dangers are properties that every security system for such environments should have."

Does INDECT propose building a just and prosperous global society, thus lessening the potential that terrorist killers or other miscreants will exploit a "target rich environment" that may prove deadly for innocent workers who, after all, were the principle victims of the 2004 and 2007 terrorist outrages in Madrid and London? Hardly.

As with their colleagues across the pond, INDECT is hunting for the ever-elusive technological quick-fix, a high-tech magic bullet. One, I might add, that will deliver neither safety nor security but rather, will constrict the democratic space where social justice movements flourish while furthering the reach of unaccountable security agencies.

The document "describes the first deliverable of the work package which gives an overview about the main methodology and description of the XML data corpus schema and describes the methodology for collection, cleaning and unified representation of large textual data from various sources: news reports, weblogs, chat, etc."

The first order of business "is the study and critical review of the annotation schemes employed so far for the development and evaluation of methods for entity resolution, co-reference resolution and entity attributes identification."

In other words, how do present technologic capabilities provide police, security agencies and capitalist grifters with the ability to identify who might be speaking to whom and for what purpose. INDECT proposes to introduce "a new annotation scheme that builds upon the strengths of the current-state-of-the-art," one that "should be extensible and modifiable to the requirements of the project."

Asserting that "an XML data corpus [can be] extracted from forums and social networks related to specific threats (e.g. hooliganism, terrorism, vandalism, etc.)," the authors claim they will provide "different entity types according to the requirements of the project. The grouping of all references to an entity together. The relationships between different entities" and finally, "the events in which entities participate."

Why stop there? Why not list the ubiquitous "other" areas of concern to INDECT's secret state partners? While "hooliganism, terrorism, vandalism, etc.," may be the ostensible purpose of their "entity attributes identification" project, surely INDECT is well aware that such schemes are just as easily applicable to local citizen groups, socialist and anarchist organizations, or to the innumerable environmental, human rights or consumer campaigners who challenge the dominant free market paradigm of their corporate sponsors.

The authors however, couldn't be bothered by the sinister applications that may be spawned by their research; indeed, they seem quite proud of it.

"The main achievements of this work" they aver, "allows the identification of several types of entities, groups the same references into one class, while at the same time allows the identification of relationships and events."

Indeed, the "inclusion of a multi-layered ontology ensures the consistency of the annotation" and will facilitate in the (near) future, "the use of inference mechanisms such as transitivity to allow the development of search engines that go beyond simple keyword search."

Quite an accomplishment! An enterprising security service or capitalist marketing specialist need only sift through veritable mountains of data available from commercial databases, or mobile calls, tweets, blog posts and internet searches to instantaneously identity "key agitators," to borrow the FBI's very 20th century description of political dissidents; individuals who could be detained or "neutralized" should sterner methods be required.

Indeed, a surveillance scheme such as the one INDECT is building could greatly facilitate--and simplify--the already formidable U.S. "Main Core" database that "reportedly collects and stores--without warrants or court orders--the names and detailed data of Americans considered to be threats to national security," as investigative journalists Tim Shorrock and Christopher Ketchum revealed in two disturbing reports last year.

The scale of "datasets/annotation schemes" exploited by INDECT is truly breathtaking and include: "Automatic Content Extraction" gleaned from "a variety of sources, such as news, broadcast conversations" that identify "relations between entities, and the events in which these participate."

We next discover what is euphemistically called the "Knowledge Base Population (KBP)," an annotation scheme that "focuses on the identification of entity types of Person (PER), Organization (ORG), and Geo-Political Entity (GPE), Location (LOC), Facility (FAC), Geographical/Social/Political (GPE), Vehicle (VEH) and Weapon (WEA)."

How is this accomplished? Why through an exploitation of open source materials of course!

INDECT researchers readily aver that "a snapshot of Wikipedia infoboxes is used as the original knowledge source. The document collection consists of newswire articles on the order of 1 million. The reference knowledge base includes hundreds of thousands of entities based on articles from an October 2008 dump of English Wikipedia. The annotation scheme in KBP focuses on the identification of entity types of Person (PER), Organization (ORG), and Geo-Political Entity (GPE)."

For what purpose? Mum's the word as far as INDECT is concerned.

Nothing escapes this panoptic eye. Even popular culture and leisure activities fall under the glare of security agencies and their academic partners in the latest iteration of this truly monstrous privacy-killing scheme. Using the movie rental firm Netflix as a model, INDECT cites the firm's "100 million ratings from 480 thousand randomly-chosen, anonymous Netflix customers" as "well-suited" to the INDECT surveillance model.

In conclusion, EU surveillance architects propose a "new annotation & knowledge representation scheme" that "is extensible," one that "allows the addition of new entities, relations, and events, while at the same time avoids duplication and ensures integrity."

Deploying an ontological methodology that exploits currently available data from open source, driftnet surveillance of news, broadcasts, blog entries and search results, and linkages obtained through a perusal of mobile phone records, credit card purchases, medical records, travel itineraries, etc., INDECT claims that in the near future their research will allow "a search engine to go beyond simple keyword queries by exploiting the semantic information and relations within the ontology."

And once the scheme is perfected, "the use of expressive logics ... becomes an enabler for detecting entity relations on the web." Or transform it into an "always-on" spy you carry in your pocket or whenever you switch on your computer.

This is how our minders propose to keep us "safe."

CIA Gets In on the Fun

Not to be outdone, the CIA has entered the lucrative market of social networking surveillance in a big way.

In an exclusive published by Wired, we learn that the CIA's investment arm, In-Q-Tel, "want to read your blog posts, keep track of your Twitter updates--even check out your book reviews on Amazon."

Investigative journalist Noah Shachtman reveals that In-Q-Tel "is putting cash into Visible Technologies, a software firm that specializes in monitoring social media. It's part of a larger movement within the spy services to get better at using "open source intelligence"--information that's publicly available, but often hidden in the flood of TV shows, newspaper articles, blog posts, online videos and radio reports generated every day." Wired reported:

- Visible crawls over half a million web 2.0 sites a day, scraping more than a million posts and conversations taking place on blogs, online forums, Flickr, YouTube, Twitter and Amazon. (It doesn't touch closed social networks, like Facebook, at the moment.) Customers get customized, real-time feeds of what's being said on these sites, based on a series of keywords. (Noah Shachtman, Exclusive: U.S. Spies Buy Stake in Firm that Monitors Blogs, Tweets," Wired, October 19, 2009)

Although In-Q-Tel spokesperson Donald Tighe told Wired that it wants Visible to monitor foreign social media and give American spooks an "early-warning detection on how issues are playing internationally," Shachtman points out that "such a tool can also be pointed inward, at domestic bloggers or tweeters."

According to Wired, the firm already keeps tabs on 2.0 web sites "for Dell, AT&T and Verizon." And as an added attraction, "Visible is tracking animal-right activists' online campaigns" against meat processing giant Hormel.

Shachtman reports that "Visible has been trying for nearly a year to break into the government field." And why wouldn't they, considering that the heimat security and even spookier black world of the U.S. "intelligence community," is a veritable cash-cow for enterprising corporations eager to do the state's bidding.

In 2008 Wired reports, Visible "teamed-up" with the Washington, DC-based consulting firm "Concepts & Strategies, which has handled media monitoring and translation services for U.S. Strategic Command and the Joint Chiefs of Staff, among others."

According to a blurb on the firm's web site they are in hot-pursuit of "social media engagement specialists" with Defense Department experience and "a high proficiency in Arabic, Farsi, French, Urdu or Russian." Wired reports that Concepts & Strategies "is also looking for an 'information system security engineer' who already has a 'Top Secret SCI [Sensitive Compartmentalized Information] with NSA Full Scope Polygraph' security clearance."

In such an environment, nothing escapes the secret state's lens. Shachtman reveals that the Office of the Director of National Intelligence (ODNI) "maintains an Open Source Center, which combs publicly available information, including web 2.0 sites."

In 2007, the Center's director, Doug Naquin, "told an audience of intelligence professionals" that "'we're looking now at YouTube, which carries some unique and honest-to-goodness intelligence.... We have groups looking at what they call 'citizens media': people taking pictures with their cell phones and posting them on the internet. Then there's social media, phenomena like MySpace and blogs'."

But as Steven Aftergood, who maintains the Secrecy News web site for the Federation of American Scientists told Wired, "even if information is openly gathered by intelligence agencies it would still be problematic if it were used for unauthorized domestic investigations or operations. Intelligence agencies or employees might be tempted to use the tools at their disposal to compile information on political figures, critics, journalists or others, and to exploit such information for political advantage. That is not permissible even if all of the information in question is technically 'open source'."

But as we have seen across the decades, from COINTELPRO to Operation CHAOS, and from Pentagon media manipulation during the run-up to the Iraq war through driftnet warrantless wiretapping of Americans' electronic communications, the secret state is a law unto itself, a self-perpetuating bureaucracy that thrives on duplicity, fear and cold, hard cash.

As published in Global Research. Thanks to Tom Burghardt and Global Research for covering this material. Copyright remains with the aforementioned.

Source documents:

- EU social network spy system brief, INDECT Work Package 4, 2009

Retrieved from "https://secure.wikileaks.org/wiki/Mind_Your_Tweets:_The_CIA_Social_Networking_Surveillance_System"

Categories: Analyses | European Union | 2009 | 2009-10 | United States | Government (bureaucracy)