GlobalResearch
Center for Research on Globalization

“Obese Intelligence”: The NSA Search Engine. “Over 850 Billion Records about Phone Calls, Emails, Cellphone Locations, and Internet Chats”

By Dr. Binoy Kampmark
Global Research, August 27, 2014

Region: USA
Theme: Intelligence, Police State & Civil Rights

The Intercept was already getting the intelligence community excited with its revelations that the National Security Agency had decided to mimic inspector Google. Through creating a search engine in the manner of those pro-transparency pioneers, the intelligence community was turning the tables on the very idea of searchable information. Why keep it the operating preserve of the public? The search engine has, as it stands, over 850 billion records about phone calls, emails, cellphone locations, and internet chats.[1]

The revelations have a few implications, the most obvious one confirming the seamless transition between intelligence work on the one hand, and the policing function on the other. The distinction between intelligence communities whose interests are targeting matters foreign to the polity; and those who maintain order within the boundaries of a state in a protective capacity, prove meaningless in this form. The use of ICREACH makes it clear that the Drug Enforcement Administration and the Federal Bureau of Investigation are regular clients and users of the system.

A 2010[2] memorandum from the Chief of Liaison Support Group at the CIA titled “CIA colleagues enthusiastically welcome NSA training” speaks with praise about those “NSA-ers embedded in CIA’s workspaces”. Indeed, it speaks very highly of the “information sharing” ethos of the NSA within the Intelligence Community, channelling Google’s operating rationale within more secret spaces. Furthermore, in 2010, the relevant data base provided the NSA “and second Party telephony metadata events to over 1000 analysts across 23 US Intelligence Community agencies.”

Those keen on squirreling information into such a data base are no doubt thrilled by the prospects that it can be made available to the “appropriate” sources. ICREACH has become one of the largest, if not largest system for the internal processing and sharing of surveillance records within the United States. It is not, according to *The Intercept*, connected with the NSA database that stores data on Americans’ phone calls pursuant to s. 215 of the Patriot Act.

The difference between the two accumulated pools of data is one of scope: ICREACH is mammoth in reach, and positively defiant in its push against the law; the database gathered under s. 215 guidelines is minute in comparison, confined to the dangerously pertinent idea of combating terrorism and like threats. ICREACH exists outside the system of court orders, being a creature of Executive Order 12333. The document, instituted by President Ronald Reagan in 1981, was intended to add robustness to the intelligence gathering capabilities of

the US intelligence community.

John Tye[3], formally of the US State Department, has wrestled with the way EO 12333 is used. He accepts its premise that it is primarily "to target foreigners abroad, and collection happens outside the US." However, "My complaint is not that they're using it to target Americans, my complaint is that the volume of incidental collection on US persons is unconstitutional."

The idea of restraining intelligence gathering to pertinent, specific targeting has gotten increasingly old fashioned in the information banquet of the modern NSA community. Farming modern metadata provides a diet positively rich in carbohydrates, a deficient diet when it comes to nutrition, but excessive when it comes to those fats a lean intelligence, and policing service, should avoid.

The true fat stripping agent here is the law, with its targeted formulae that keeps intelligence agencies focused and relevant in their activities. The most humble analyst will use the law as a tool for gathering, and analysing good data. The slothful gatherer will prefer the short cuts, including the magical search term that avoids as much as it captures. Bugger the law and type in the search term.

The progenitor of this system was retired NSA director Gen. Keith Alexander. In a 2006 letter to John Negroponte, then Director of National Intelligence, Alexander outlined his ideas of a search tool that would "allow unprecedented volumes of communications metadata to be shared and analysed". To what end? Prizing open a "vast, rich source of information". Superbly dim in a sense – information is not knowledge; and knowledge is not, on its own accord, information. The glaring point here is that the higher ups in the intelligence community have gotten the wrong end of the stick.

In 2007, ICREACH was launched, its purpose being to deliver "the first-ever wholesale sharing communications database within the US Intelligence Community." It became, as spokesman from the US Office of the Director of National Intelligence Jeffrey Anchukaitis suggested, part of a fundamental "pillar of the post-9/11 intelligence community" – the principle of sharing information between. Authorities, irrespective of legal distraction or distinction, could obtain data that would otherwise be "stove-piped in any single office or agency."

The problems of such data-sharing processes is the mechanical presumption that they take place in a legal vacuum. On the one hand, members of the intelligence community are becoming the lounge lizards of bureaucracy. They hug metadata the way a viewer of cable channel television surfs the package of channels. Nothing is actually processed. What matters is having the package to begin with.

The other consequence is dangerous – such sharing practices distribute sensitive material of citizens, both American and non-American, in a manner that mocks any legal restraint. According to Brian Owsley, who presided as federal magistrate judge between 2005 and 2013, "there shouldn't be this buddy-buddy system back-and-forth." Time, it would seem, to burn the fat off the obese operator that is the modern US intelligence community.

Dr. Binoy Kampmark was a Commonwealth Scholar at Selwyn College, Cambridge. He lectures at RMIT University, Melbourne. Email: bkampmark@gmail.com

Notes

[1] https://firstlook.org/theintercept/article/2014/08/25/icreach-nsa-cia-secret-google-crisscross-proton/

[2] https://firstlook.org/theintercept/document/2014/08/25/cia-colleagues-enthusiastically-welcome-nsa-training

[3] http://arstechnica.com/tech-policy/2014/08/meet-john-tye-the-kinder-gentler-and-by-the-book-whistleblower/

Articles by: Dr. Binoy Kampmark