# WHAT'S THE RELATIONSHIP DATABASE ABOUT?

Atrios asks what the whole dragnet is about.

> It's actually a serious question. Maybe it's just a full employment program for spooks. Maybe they just do it because they can. But the only "real" point to such an extensive surveillance system is to abuse that surveillance (the surveillance itself is already an abuse of course).
>
> At best it's a colossal fucking waste of money. At worst?

I actually think there are understandable answers for much of this.

Since Michael Hayden took over the NSA, contractors have assumed an increasingly dominant role in the agency, meaning you've got a former DIRNSA at Booz Allen Hamilton pitching future Booz VPs on solutions to keep the country safe that just happen to make them fabulously profitable and don't happen to foreground privacy. As Thomas Drake showed, we're pursuing the biggest and most privacy invasive solutions because contractors are embedded with the agency.

I think there's the One Percent approach we got from Dick Cheney, that endorses maximal solutions to hunt terrorists even while avoiding any real accountability (both for past failures and to review efficacy) because of secrecy. We're slowly beginning to wean ourselves from this Cheney hangover, but it is taking time (and boosters for his approach are well-funded and publicized).

And, at the same time, criminals and other countries have attacked our weak network security underbelly, targeting the companies

that have the most political sway, DOD contractors and, increasingly, financial companies, which is setting off panic that is somewhat divorced from the average American's security. The accountability for cybersecurity is measured in entirely different ways than it is for terrorism (otherwise Keith Alexander, who claims the country is being plundered like a colony, would have been fired years ago). In particular, there is no punishment or even assessment of past rash decisions like StuxNet. But here, as with terrorism, the notion of cost-benefit assessment doesn't exist. And this panicked effort to prevent attacks even while clinging to offensive cyberweapons increasingly drives the overaggressive collection, even though no one wants to admit that.

Meanwhile, I think we grab everything we can overseas out of hubris we got while we were the uncontested world power, and only accelerated now that we're losing that uncontested position. If we're going to sustain power through coercion — and we developed a nasty habit of doing so, especially under Bush — then we need to know enough to coerce successfully. So we collect. Everything. Even if doing so makes us stupider and more reliant on coercion.

So I can explain a lot of it without resorting to bad faith, even while much of that explanation underscores just how counterproductive it all is.

But then there's the phone dragnet, the database recording all US phone-based relationships in the US for the last 5 years. In spite of extensive discussion of ways to do this without creating a database of every phone based relationship (and the House Intelligence Committee's willingness to shorten the retention period to 3 years), Keith Alexander and James Clapper insist we cannot change the way we do this. This, in spite of the almost complete lack of any evidence the database (and its predecessor) has been useful over the last 12 years.

Indeed, in an op-ed, Adam Schiff suggests (given his reference to having urged changes privately before he did publicly, which he did in the first HPSCI hearing after the Snowden leaks) he has been making this point for some time.

> As for the effectiveness of the program, the evidence that it has made us safer is limited. The Obama administration cites about a dozen cases in which the database was consulted in an investigation. Although many of the details of these cases remain classified, evidence that the metadata program was an integral part of the success of each of these investigations — or even most of them — is far from clear. Instead, it appears that the utility of the metadata program has been conflated with the success of other collection efforts.
>
> Finally, on the third test of whether the program has been structured to minimize unnecessary intrusion on our privacy, the NSA program plainly fails. Rather than a narrowly tailored effort that reduces the potential for abuse or violations of privacy, the bulk collection regime is vast, touching billions of phone calls made in the United States over the last five years.
>
> This is all the more troubling because there are other less intrusive ways to structure the program. I have urged the administration — privately at first, then publicly — to reconfigure the NSA effort so that the call records remain with the telephone companies that already hold them for business purposes. Under this model, the government could meet its national security needs by asking the companies to run a number once it had been connected to a suspected terrorist plot. The government would neither collect nor retain the

> phone records.
>
> At the Tuesday hearing, NSA Director Keith Alexander acknowledged that such a restructuring is technically feasible provided the phone companies maintain the data long enough and in an accessible format. Such a system might be less efficient for the NSA, but it could nonetheless provide quick and timely results. And Americans have the right to expect that intelligence-gathering programs are judged on more than efficiency alone. After all, if efficiency were the only priority, there would be no need for a 4th Amendment.

Keith Alexander's shout out to terrorist supporter Peter King for his vocal support of the NSA in the hearing the other day made me realize that the sole known person caught primarily because of the Section 215 data, Basaaly Moalin, did far less than King did in the 1980s supporting Irish terrorists, and did it (according to a 2009 FBI assessment) for the same reasons — to raise his leadership profile in his tribe. The database simply hasn't netted any serious threat.

And while I seem to be the only one gravely concerned that the NSA suggested it might use the relationship database to target informants, rather than actual terrorist associates, that does seem to be part of the explanation: "investigative leads" (as Clapper justified the program) are far more useful when they come complete with means to coerce even more useful investigative leads, no matter how unethical that might be.

But ultimately, even that application can't explain the need for a relationship database encapsulating the entire country.

There seems to be little that justifies that relationship database than the desire to have it, in case, for such time as the government

plans to unleash the nuclear bomb of reading every relationship in the country.