“TOO MUCH TRANSPARENCY DEFEATS THE VERY PURPOSE OF DEMOCRACY”

In truly bizarre testimony he will deliver to the House Intelligence Committee next week, Paul Rosenzweig argues that “too much transparency defeats the very purpose of democracy.” He does so, however, in a piece arguing that the government needs what amounts to be almost full transparency on all its citizens.

The first section of Rosenzweig analysis talks about the power of big data. It doesn’t provide any actual evidence that big data works, mind you. On the contrary, he points to one failure of big data.

> When we speak of the new form of “dataveillance,” we are not speaking of the comparatively simple matching algorithms that cross check when a person’s name is submitted for review¾when, for example, they apply for a job. Even that exercise is a challenge for any government, as the failure to list Abdulmutallab in advance of the 2009 Christmas bombing attempt demonstrates.[11] The process contains uncertainties of data accuracy and fidelity, analysis and registration, transmission and propagation, and review, correction, and revision. Yet, even with those complexities, the process uses relatively simple technologically—the implementation is what poses a challenge.
>
> By contrast, other systems of data analysis are far more technologically sophisticated. They are, in the end, an

> attempt to sift through large quantities of personal information to identify subjects when their identities are not already known. In the commercial context, these individuals are called "potential customers." In the cyber conflict context, they might be called "Anonymous" or "Russian patriotic hackers." In the terrorism context, they are often called "clean skins" because there is no known derogatory information connected to their names or identities. In this latter context, the individuals are dangerous because nothing is known of their predilections. For precisely this reason, this form of data analysis is sometimes called "knowledge discovery," as the intention is to discover something previously unknown about an individual. [my emphasis]

Nevertheless, having not provided evidence big data works, he concludes that "There can be little doubt that data analysis of this sort can prove to be of great value."

The reference to Abdulmutallab is curious. At the beginning of his testimony he repeats the reference.

> In considering this new capability we can't have it both ways. We can't with one breath condemn government access to vast quantities of data about individuals, as a return of "Big Brother"[4] and at the same time criticize the government for its failure to "connect the dots" (as we did, for example, during the Christmas 2009 bomb plot attempted by Umar Farouk Abdulmutallab.

This formulation — and the example of Abdulmutallab even more so — is utterly crazy. Having big data is not the same thing as analyzing it correctly. Criticism that the

Intelligence Community failed to connect the dots — with the UndieBomb attack, but even with 9/11 — assumes they had the dots but failed to analyze them or act on that analysis (as the IC did fail, in both cases). Indeed, having big data may actually be an impediment to analyzing it, because it drowns you. And while Rosenzweig suggests the only big data failure with Abdulmutallab involved not placing him on a watch list, that's false. The NSA had wiretaps on Anwar al-Awlaki which, according to the government, collected information tying Abdulmutallab to an attack.

Yet they didn't respond to it.

And you know what? We measly citizens don't know why they didn't respond to it — though we do know that the FBI agents who were analyzing the Awlaki data were … you guessed it! Overwhelmed.

Before anyone involved in government claims that big data helps — rather than hinders — they should have to explain why a full-time tap on Anwar al-Awlaki didn't find the guy who was texting him about a terrorist attack. Particularly in the absence of any other compelling evidence big data works (and the Administration's claims of 54 "terrorist events stopped" barely makes a claim to justify Section 702 collection and certainly doesn't justify Section 215), then logical conclusion is that it in fact does the opposite.

Having made the unsubstantiated claim that giving the government full transparency on citizens and others provides a benefit, Rosenzweig then dismisses any privacy concerns by redefining it.

Part of that involves claiming — reports of the collection of address books notwithstanding — that so long as we don't get identified it doesn't matter.

> The anonymity that one has in respect of these transactions is not terribly different from "real-world anonymity." Consider, as an example, the act of

> driving a car. It is done in public, but one is generally not subject to routine identification and scrutiny.

He then proposes we not limit what can be seen, but instead ensure that nothing unjustified can happen to you based on the discovery of something about you.

> In other words, the veil of anonymity previously protected by our "practical obscurity" that is now so readily pierced by technology must be protected by rules that limit when the piercing may happen as a means of protecting privacy and preventing governmental abuse. To put it more precisely, the key to this conception of privacy is that privacy's principal virtue is a limitation on consequence. If there are no unjustified consequences (i.e., consequences that are the product of abuse or error or the application of an unwise policy) then, under this vision, there is no effect on a cognizable liberty/privacy interest. In other words, if nobody is there to hear the tree, or identify the actor, it really does not make a sound.

If nothing bad in real life happens to you because of this transparency the government should have on citizens, Rosenzweig argues, nothing has happened.

For the moment, I'll just bracket the many examples where stuff happens in secret — being put on a no fly list, having your neighbor recruited as an informant using data the NSA found, having your computer invaded based on equations of Anonymous with hacker — that still have effects. On those, no one can now assess whether something bad has happened unjustly, because no one will ever see it. And I'll bracket all the things everyone has ever written about how living in a Panopticon changes

behavior and with it community.

Here's how Rosenzweig justifies setting up a (what he fancies to be anonymous but isn't, really) Panopticon while denying citizens the same right to see; here's how he supports his "too much transparency" comment.

> Finally, let me close this statement of principles by noting that none of this is to diminish the significance of the transparency and oversight, generally. Transparency is a fundamental and vital aspect of democracy. Those who advance transparency concerns often, rightly, have recourse to the wisdom of James Madison, who observed that democracy without information is "but prologue to a farce or a tragedy."[13]
>
> Yet Madison understood that transparency was not a supreme value that trumped all other concerns. He also participated in the U.S. Constitutional Convention of 1787, the secrecy of whose proceedings was the key to its success. While governments may hide behind closed doors, U.S. democracy was also born behind them. It is not enough, then, to reflexively call for more transparency in all circumstances. The right amount is debatable, even for those, like Madison, who understand its utility.
>
> What we need is to develop an heuristic for assessing the proper balance between opacity and transparency. To do so we must ask, why do we seek transparency in the first instance? Not for its own sake. Without need, transparency is little more than voyeurism. Rather, its ground is oversight—it enables us to limit and review the exercise of authority.

Man, that series of sentences … "without need, transparency is little more than voyeurism" …

"why do we seek transparency for its own sake" are pretty ironic in testimony defending the NSA's collection of records of every phone-based relationship in the US, of having access to 75% of the Internet traffic in the US, and of tapping 35 world leaders just because it could.

But first, Madison.

Because Madison participated in a series of secret meetings the results of which and eventually the details of which were subsequently made public to the entire world, Rosenzweig suggests Madison might support a system where citizens never got to learn how close to all their data the government collects and how it uses it.

Then he argues the only purpose of transparency — the thing separating it from voyeurism — is "oversight," which he describes as limit[ing] and review[ing] the exercise of authority.

If he thought this through, he might realize that even if that's the only legitimate purpose for transparency, it'd still require some oversight over the Executive and the Legislature that, in his delegated model of oversight simply would not and could not (and does not) exist. One thing we're learning about the dragnet, for example, is that a good deal of collection on US persons goes on under Executive Order 12333 that gets almost no Congressional review at all. And that's just the most concrete way we're learning how inadequate the oversight practiced by the Intelligence Committees is.

But that's not the only purpose of transparency.

One other purpose of transparency — arguably, the purpose of democracy — is to exercise some rationality to assess the best policies. The idea is that if you debate policies and only then decide on them, you end up with more effective policies overall. It doesn't always work out that way, but the idea, in any case, is that policies subjected to debate end up being smarter than policies thought up in secret.

It's about having the most effective government.

So in addition to making sure no one breaks the law (Rosenzweig seems unconcerned that NSA has been caught breaking the law and violating court orders repeatedly), transparency — democracy — is supposed to raise the chances of us following better policies.

I presume Rosenzweig figures the debate that goes on within the NSA and within the National Security Counsel adequate to the task of picking the best policies (and the Constitution certainly envisions the Executive having a great deal of that debate take place internally, though surely not on programs as monumental as this).

But here's the thing: the public evidence — whether it be missing the Abdulmutallab texts on an attack, the thin claims of 54 terrorist events, or Keith Alexander's reports that the US has been plundered like a colony via cyberattacks under his watch — it's actually not clear this approach is all that effective. In fact, there's at least reason to believe some parts of the approach in place are ineffective.

That's why we need more transparency. Not to be voyeurs on a bunch of analysts at NSA (really?). But to see if there's a better way to do this.

Ultimately, though, Rosenzweig defeats himself. He's right that we need to find "the proper balance between opacity and transparency" (though he might step back and reconsider what the "very purpose of democracy" is before he chooses that balance). But it is utterly illogical to suggest the balance be set for almost complete transparency when the government looks at citizens — records of all their phone-based relationships and access to 75% of the Internet data — but then argue that delegated transparency (but with almost no transparency on the delegated part) is adequate for citizens looking back at their government.

Related: Homeland Security Czar Lisa Monaco endorses the idea that just because we can

collect it doesn’t mean we should. Michael Hayden learns surveillance isn’t actually all that fun. And Keith Alexander says we should get rid of journalism.