SWIFT: BIG BROTHER WITH A BOOZ ASSIST, ONLY WITHOUT THE PAPERWORK

As reporting on Edward Snowden reveal the scope of our spying on European friends, I've been thinking a lot about SWIFT.

SWIFT, you recall, is the database tracking international online money transfers. After 9/11, the US Government started helping itself to the data to track terrorist financing. But then in 2010 the servers moved entirely to the EU, and the EU forced the US to accede to certain protections: protections for EU citizens, a prohibition on bulk collection (and with it data mining), and two-pronged audit system.

Today, the CEO of SWIFT until 2007, Leonard Schrank, and the former Homeland Security Advisor, Juan Zarate, boast about the controls on SWIFT, suggesting it provides a model for data collection with oversight.

> Both the Treasury and Swift ensured that the constraints on the information retrieved and used by analysts were strictly enforced. Outside auditors hired by Swift confirmed the limited scope of use, and Swift's own representatives (called "scrutineers") had authority to stop access to the data at any time if there was a concern that the restrictions were being breached. These independent monitors worked on site at government agencies and had real-time access to the system. Every time an analyst queried the system, the scrutineer could immediately review the query. Each query had to have a reason attached to it that justified it as a counterterrorism matter. Over time, the

> scope of data requested and retained was reduced.
>
> This confirmed that the information was being used in the way we said it was — to save lives.
>
> [snip]
>
> The use of the data was legal, limited, targeted, overseen and audited. The program set a gold standard for how to protect the confidential data provided to the government. Treasury legally gained access to large amounts of Swift's financial-messaging data (which is the banking equivalent of telephone metadata) and eventually explained it to the public at home and abroad.
>
> It could remain a model for how to limit the government's use of mass amounts of data in a world where access to information is necessary to ensure our security while also protecting privacy and civil liberties.

This description should already raise concerns about the so-called gold standard for spying. When "scrutineers" cohabit with those they're supposed to be scrutinizing, it tends to encourage cooperation, not scrutiny.

And somehow, Schrank and Zarate neglect to mention that the vaunted audit process they describe was conducted by none other than Booz Allen Hamilton, the contractor that hired and let Edward Snowden abscond with the spying world's crown jewels. And, as ACLU noted in a report for the EU in 2006, even during Schrank's tenure, Booz was neck deep in aggressive surveillance.

But the real problem with highlighting SWIFT as a poster child of massive surveillance done right post-dates Schrank's tenure (though he must know about this), when the EU's independent audits for the first time revealed what went on

in SWIFT queries. Among other things: the actual requests were oral, and therefore couldn't be audited.

> The report revealed that the Americans have been submitting largely identical requests—but then supplementing them with oral requests.
>
> The oral requests, of course, make it impossible to audit the requests.
>
> > At the time of the inspection, Europol had received our requests for SWIFT data. Those four requests are almost identical in nature and request—in abstract terms—broad types of data, also involving EU Member States' data. Due to their abstract nature, proper verification of whether the requests are in line with the conditions of the Article 4(2) of the TFTP Agreement—on the basis of the available documentation—is impossible. The JSB considers it likely that the information in the requests could be more specific.
> >
> > Information provided orally—to certain Europol staff by the US Treasury Department, with the stipulation that no written notes are made—has had an impact upon each of Europol's decisions; however, the JSB does not know the content of that information. Therefore, where the requests lack the necessary written information to allow proper verification of compliance with Article 4(2) of the TFTP Agreement, it is impossible to check whether this deficiency is rectified by the orally provided information. [my

> > emphasis]

In addition, in spite of demands that the program include no bulk downloads, that's precisely what the US was doing.

> "We have given our trust to the other EU institutions, but our trust has been betrayed", said Sophia in't Veld (ALDE, NL), rapporteur on the EU-US Passenger Name Record (PNR) agreements. "This should be kept in mind when they want our approval for other agreements", she declared.
>
> "Somehow I am not surprised", said Simon Busuttil (EPP, MT), recalling that "at the time of the negotiations last year we were not satisfied with having Europol controlling it – we wanted additional safeguards". He added that "the agreement is not satisfactory", since it involves the transfer of bulk data, and insisted that "we need an EU TFTP".
>
> For Claude Moraes (S&D, UK), the US demands are "too general and too abstract". He also recalled that MEPs had insisted at the time that it must be specified how the US request would be made and that they needed to be "narrowly tailored". A written explanation should accompany each request, he added.
>
> This agreement is not in line with Member States' constitutional principles and with fundamental rights, argued Jan Philipp Albrecht (Greens/EFA, DE). He highlighted the problem of bulk data transfer, "which is exactly what we have criticised before". [my emphasis]

In other words, once an actual independent reviewer – not an embedded contractor like Booz

– reviewed the program, it became clear it was designed to be impossible to audit, even while engaging in precisely the bulk downloads the Europeans feared.

Not only is the experience of SWIFT one reason why the Europeans are so quick to object to the scale of US spying on them. But it is actually a poster child for surveillance done wrong.

Contrary to what its boosters want you to believe.