DOUBLE DIPPING AT SWIFT

Spiegel today reveals more details about NSA's "Follow the Money" program, in which it collects credit card information from select geographical regions. In addition, as TV Globo also revealed last week, they are conducting Tailored Access Operations against SWIFT, the international financial transfer messaging system.

> The NSA's Tracfin data bank also contained data from the Brussels-based Society for Worldwide Interbank Financial Telecommunication (SWIFT), a network used by thousands of banks to send transaction information securely. SWIFT was named as a "target," according to the documents, which also show that the NSA spied on the organization on several levels, involving, among others, the agency's "tailored access operations" division. One of the ways the agency accessed the data included reading "SWIFT printer traffic from numerous banks," the documents show.

Now, some caution about this claim is in order. Spiegel reports that NSA's financial records database has 180 million records, of which 84% are credit card transactions.

> The collected information then flows into the NSA's own financial databank, called "Tracfin," which in 2011 contained 180 million records. Some 84 percent of the data is from credit card transactions.

Even assuming the balance of the records in the database come from SWIFT, that's less than 29 million records (in 2011, so assume the number is larger now). In 2011, SWIFT was sending 17.5 million records a day. So whatever makes it into the actual database is just a small fraction of

international traffic.

But that almost certainly doesn't account for the bulk of the SWIFT information collected by the US government. Remember: in addition to stealing the data, Treasury also gets it via a now-public agreement. The former CEO of SWIFT Leonard Schrank and former Homeland Security Czar, Juan Zarate actually boasted in July, in response to the earliest Edward Snowden revelations, about how laudable Treasury's consensual access to the data was.

> 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.

Never mind that by the time they wrote this, an EU audit had showed the protections were illusory, in part because the details of actual queries were oral (and therefore the queries weren't auditable), in part because Treasury was getting bulk data. But there was a legitimate way to get data pertaining to the claimed primary threat at hand, terrorism. And now we know NSA also stole data.

Note, too, the timing. While Spiegel doesn't provide enough details about the exploitation of SWIFT for us to date it, the dates it does provide about this financial spying are 2010 and 2011. That was the period when the EU was trying to put sensible limits to Treasury's access of

SWIFT.

Back when the intelligence community first decided to go after SWIFT data, their first plan was to just steal it.

> Intelligence officials were so eager to use the Swift data that they discussed having the C.I.A. covertly gain access to the system, several officials involved in the talks said. But Treasury officials resisted, the officials said, and favored going to Swift directly.

12 years later, they apparently are stealing at least some of it. That probably means they wanted data for transactions that have nothing to do with the counterterrorism application first SWIFT and then the EU bought off on. So there's the legal access to counterterrorism data via Treasury, and the illegal access to (presumably) some other kind of data via NSA.

Indeed, though it may pertain to the credit card data, Spiegel reports that even the spooks are wary about the degree to which GCHQ and NSA collect data on people who aren't legitimate targets.

> But even intelligence agency employees are somewhat concerned about spying on the world finance system, according to one document from the UK's intelligence agency GCHQ concerning the legal perspectives on "financial data" and the agency's own cooperations with the NSA in this area. The collection, storage and sharing of politically sensitive data is a deep invasion of privacy, and involved "bulk data" full of "rich personal information," much of which "is not about our targets," the document says.

And these GCHQ spies aren't the only ones concerned about this spying. Eric Lichtblau's book described some of the worries about SWIFT

access.

> One reason people grew uncomfortable with the program was because “some foreign officials feared that the United States could turn the giant database against them.” (234) Others worried that the US might be “delving into corporate trade secrets of overseas companies.” (248) And when Alan Greenspan helped persuade SWIFT to continue offering US access to the database, he admitted how dangerous it was.
>
> > If the world’s financiers were to find out how their sensitive internal data was being used, he acknowledged, it could hurt the stability of the global banking systems. (246)

Sure, Alan Greenspan is a hack, but he normally underestimates the degree to which risks threaten the global financial system. And there’s a decent chance that NSA’s theft of this data goes beyond even that access — purportedly limited to counterterrorism — that got Greenspan so concerned.

Now if the rest of us can’t have privacy to conduct our private lives, I’m all in favor of making the banskters’ secrets public as well. Heh.

I recognize that that undermines a key assumption the banksters rely on: privacy. If NSA can steal whatever they want, they really do have the ability to undermine what few rules still govern the international gambling-masquerading-as-banking system.

But even having been warned about the risk stealing this data poses to the global financial system doesn’t appear to have stopped NSA.