

FISA AND THE SPACE-TIME CONTINUUM

I'm going to do a series of FISA posts on both the Keith Gartenlaub case (he was convicted on child porn charges after the FBI found old images on his computers during a FISA search) and the reported Paul Manafort FISA orders.

But first I want to explain FISA and the space-time continuum.

The space part is easy: the FISA Amendments Act slightly changed the geographical rules on what authority the government could use to target various kinds of people. It legalized the government's practice of collecting on foreigners from facilities in the United States under Section 702. And it also required a judge's approval for any spying on Americans overseas. While FAA envisioned two kinds of authorities for spying overseas – 703 (collection in the US on an American overseas, as in calling up Google for someone's email box) and 704/705(b) (collection overseas on an American overseas, which is using all methods covered by E.O. 12333, including hacking them and collecting off switches), in practice just the latter authority is used. Effectively, then, the change just codified the domestic collection on foreigners, while requiring a court order for the same E.O. 12333 collection that had already been going on.

The time part is trickier.

The short version is that FISA imposes some restrictions on whether you can collect data at rest to obtain data from outside the period of a FISA order. Thus, if you're not supposed to collect on someone when they're in the US (whether that person is a US person or a foreigner), there are classified restrictions about whether you can collect stored data from that period.

None of these rules are (as far as I'm aware)

public, but there are rules for all the various laws. In other words, you're not supposed to be able to collect Gmail on a foreigner while they're in the US, but you're also not supposed to be able to cheat and just get the same Gmail as soon as they leave the country.

This is even more complex for Americans. Domestically, there are two kinds of collection: 1805, which is the collection of data in motion – an old fashioned wiretap, and 1824, which is called a “physical search” order. The government likes to hide the fact that the collection of data at rest is accomplished with an 1824 physical search order, not 1805. So an 1824 order might be used to search a closet, or it might be used to image someone's hard drive. Most often, 1805 and 1824 get combined, but not always (the FISC released a breakdown for these last year).

Of course (as the Gartenlaub case will show), if you image someone's hard drive, you're going to get data from well before the time they've been under a FISA order, quite possibly even from before you've owned your computer.

Then there's travel overseas. If an American on whom there's already an 1805 and/or 1824 order travels overseas, the Attorney General can automatically approve a 705(b) order for him (effectively replicating the old EO 12333 authority). But that collection is only supposed to cover the period when the person is overseas, and only for the period when they've had a FISA order against them. Using the kind of hacking they use overseas is going to get data in motion and stored communications and a whole lot more, meaning they may well get stuff sitting on the computer someone brings with them (yet another reason to bring travel laptops and phones overseas). And apparently, they only turn off an implant when a FISA order expires; they don't entirely remove the implant. In addition, given the bulk collection the NSA conducts overseas, it would be child's play (and from descriptions of violations, appears to have included) going

back and accessing data that was collected in motion that had in the interim been sitting in NSA's coffers.

Effectively, once someone leaves the country the NSA has access to time machines to collect data from the past, though there are supposed to be limits on doing this.

The FISA problems last year arose, first and foremost, from NSA collecting on Americans overseas outside the window of the orders covering them, which was a persistent problem that the NSA just never got around to fixing. That's bad enough. But when you consider a 705(b) order only covers the period when an American normally targeted domestically is overseas, collecting outside the span of the order means you're probably also using foreign collection to collect (including by hacking) in the US.

Which is all a way of saying that discussions of FISA almost always focus on the geographical limitations: Is someone inside the US or outside? Foreigner or American?

But because of the differing rules on data in motion and data at rest – and because of the truly awesome methods used as soon as someone goes overseas – there are actually a lot of ways that NSA can get around the legal limitations based on space by playing with the limitations on time.

Again, there are rules (which are not public) that are supposed to prevent this kind of thing from going on. But it does seem to be a problem NSA has long struggled with, even at the times it appeared to be operating in good faith rather than manipulating the space-time continuum to get what they want where they can get it.