KEITH GARTENLAUB CHALLENGES THE DESTROYED FISA WALL

Keith Gartenlaub is appealing his conviction on possession of child porn to the Supreme Court, based on a FISA challenge. And while any petition for cert before SCOTUS faces long odds, I believe this one is interestingly situated in that its challenge to the plain view doctrine, in conjunction with the use of FISA evidence in a prosecution having nothing to do with national security, may present a way for SCOTUS to reconsider the wall between national security investigations and criminal prosecutions.

As a reminder, the FBI decided to investigate Gartenlaub (at a time when they were making other bone-headed investigative decisions involving Chinese-Americans) because he had access to files the Chinese government was seeking and a naturalized Chinese-American wife.

FBI switched back and forth from criminal to FISA access at least once (and probably twice), and in the process did a physical search of three Gartenlaub hard drives using the more expansive search regime available under FISA, only to then repeat the same search to obtain the same evidence of child porn to use for prosecution.

The government never presented evidence the child porn had been accessed since 2005, and Gartenlaub presented an alternate explanation for how it had gotten on his computer. In fact, the record suggests the FBI didn't want to prosecute Gartenlaub for child porn; they wanted to flip him, so he would spy on his well-connected in-laws. It didn't happen and now, even after his release from prison, he's trying to challenge the genesis of his prosecution from that FISA search.

The reason why the case is interesting is because the FBI was seeking something very

specific: materials relating to Boeing's C-17 program. A criminal forensic search for such materials, conducted under a Rule 41 warrant, would start by turning off the forensic search for items — most notably, videos — that would not return the suspected evidence of crime (which would be engineering documents).

Because of typical games the FBI plays with forensics, this was not established in the District court. But the appeal points to the government's claims that under FISA they don't have to use such forensic narrowing. It goes on to establish that they did not use such forensic narrowing tools, and, not having done that, found no evidence to support the FISA allegations but instead finding evidence that led to the child porn charges.

> In its Opposition Brief before the Ninth Circuit, the government acknowledges that there were no limitations to its secret search of Gartenlaub's hard drives, saying in a header: "The Government Was Permitted to Search Every File on Defendant's Computers . . . ."17 And nothing in the record indicates that the government used any standard forensic techniques routinely used to particularize computer searches like: date limitations; targeted key word searches; image recognition scans; taint teams, or other routine, well established techniques to limit a digital search to its target and screen out privileged, confidential, and irrelevant information.
>
> Despite its unlimited search, the FBI found no evidence that Gartenlaub had provided C-17 data to China, or otherwise acted as a spy for China. But the FBI did allegedly find, among the tens of thousands of files on the hard drives, a handful of files containing child pornography. Dropping its fantasy that Gartenlaub was a Chinese spy, the

> FBI turned to the theory he collected child pornography.

The appeal then argues that using FISA to get to criminal evidence is an end run around criminal procedure, in part because Gartenlaub had no way to challenge the criminal warrant after the evidence had already been found via FISA warrant.

> Gartenlaub's case demonstrates how easy it is to bypass the Constitution's criminal procedure guarantees by getting a secret FISA search warrant and using it to prosecute regular crimes. And it is impossible for a criminal defendant to challenge a secret FISA warrant because the defendant cannot access any of the information underlying the FISA warrant due to its secrecy. This thwarts a criminal defendant's Due Process right to test the government's case in adversarial proceedings. For these reasons alone the Court should grant certiorari to clarify the use of non-responsive FISA evidence in regular criminal proceedings.

Ultimately, one of Gartenlaub's requests for cert (and most his requests parallel this closely) argues that the government should not be permitted to use FISA warrants unless it submits those FISA warrants for court review.

> Gartenlaub's case is an example of how the government can abuse a national security investigation under FISA to prosecute unrelated non-national security crimes. Because of this risk, the government should not be permitted to use secret national security warrants to prosecute regular crimes if it won't submit those warrants and supporting materials to investigation and the adversarial process the criminal procedure amendments require. This Court

> should grant certiorari to analyze and clarify the scope of the 1978 FISA's encroachment upon the fundamental, centuries old, criminal procedure protections of the Fourth, Fifth, and Sixth Amendments.

On its face, it's a fairly modest request. And, as the appeal notes, a fairly modest one, given that there is only one other case where FISA is known to be used in a pure criminal case. The appeal distinguishes this case from the past one, *Isa*, in a way that appeals directly to the Court's recent narrowing of digitally-based searches.

> The 27 year old FISA case of United States v. Isa appears to be one of the few instances where a prosecutor used the non-responsive fruits of a FISA search for an unrelated regular criminal prosecution.70 Isa upheld the use of a FISA surveillance recording, in a state prosecution, of the surveillance target's murder of his 16-year-old daughter.71 During the course of the surveillance the murder occurred and was incidentally recorded. Unlike Gartenlaub's case, the evidence was not obtained via the methodical rummaging over the course of months through the target's computers.

In other words, on its face, it presents a case where there is no question of standing, where the reach of the questions presented may seem narrow, and on topics that fit nicely with recent court decisions recognizing the greater invasiveness of digital searches.

Except the impact of putting FISA review on the table for a purely criminal case (the appeal raises the Carter Page example) would have significant, probably overdue impact on the complete elimination of the wall between intelligence and criminal investigations after

9/11.

None of that says it will work, of course. But it’s a neat formulation that, if it did, might finally push FISA back towards being closer to what it was first envisioned as.