CENTER FOR DEMOCRACY AND TECHNOLOGY'S JAMES DEMPSEY ON "THE WALL," THEN AND NOW

Remember "the wall" that used to separate intelligence from criminal investigations and was used as an excuse for intelligence agencies not sharing intelligence they were permitted to share before 9/11?

It was demolished in 2001 — when the PATRIOT Act explicitly permitted what had been permitted before, sharing of intelligence information with the FBI — and 2002 — when the FISA Court of Review overruled presiding FISA Judge Royce Lamberth's efforts to sustain some Fourth Amendment protections in criminal investigations using minimization procedures.

Nevertheless, the specter of a wall that didn't prevent the Intelligence Committee from discovering 9/11 rising again is one of the things lying behind PCLOB's weak recommendations on back door searches in its report on Section 702.

Of particular note, that's what the Center for Democracy and Technology's James Dempsey cites in his squishy middle ground recommendation on back door searches.

> *It is imperative not to re-erect the wall limiting discovery and use of information vital to the national security*, and nothing in the Board's recommendations would do so. The constitutionality of the Section 702 program is based on the premise that there are limits on the retention, use and dissemination of the communications of U.S. persons collected under the program. The proper mix of limitations

> that would keep the program within constitutional bounds and acceptable to the American public may vary from agency to agency and under different circumstances. The discussion of queries and uses at the FBI in this Report is based on our understanding of current practices associated with the FBI's receipt and use of Section 702 data. The evolution of those practices may merit a different balancing. For now, *the use or dissemination of Section 702 data by the FBI for non-national security matters is apparently largely, if not entirely, hypothetical*. The possibility, however, should be addressed before the question arises in a moment of perceived urgency. Any number of possible structures would provide heightened protection of U.S. persons consistent with the imperative to discover and use critical national security information already in the hands of the government.546
>
> 546 *See* Presidential Policy Directive – Signals Intelligence Activities, Policy Directive 28, 2014 WL 187435, § 2, (Jan. 17, 2014) (*limiting the use of signals intelligence collected in bulk to certain enumerated purposes*), *available at* http://www.whitehouse.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities. [my emphasis]

Dempsey situates his comments in the context of the "wall." He then suggests there are two possible uses of back door searches: "national security matters," and non-national security matters, with the latter being entirely hypothetical, according to what the FBI self-reported to PCLOB.

Thus, he's mostly thinking in terms of "possible structures [that] would provide heightened protection of US. persons," to stave off future

problems. He points to President Obama's PPD-28 as one possibility as a model.

But PPD-28 is laughably inapt! Not only does the passage in question address "bulk collection," which according to the definition Obama uses and PCLOB has adopted has nothing to do with Section 702. "[T]he Board does not regard Section 702 as a 'bulk' collection program," PCLOB wrote at multiple points in its report.

More troubling, the passage in PPD-28 Dempsey cites permits bulk collection for the following uses:

> (1) espionage and other threats and activities directed by foreign powers or their intelligence services against the United States and its interests;
>
> (2) threats to the United States and its interests from terrorism;
>
> (3) threats to the United States and its interests from the development, possession, proliferation, or use of weapons of mass destruction;
>
> (4) cybersecurity threats;
>
> (5) threats to U.S. or allied Armed Forces or other U.S or allied personnel;
>
> (6) transnational criminal threats, including illicit finance and sanctions evasion related to the other purposes named in this section;

Ultimately, this represents — or should — an expansion of permissible use of Section 702 data, because its discussion of terrorism and cybersecurity do not distinguish between those with an international nexus and those without. And the discussion of transnational crime might subject any petty drug dealer selling dope from Mexico to foreign intelligence treatment.

That this is what passes for the mushy middle on PCLOB is especially curious given that Dempsey

was one of the first PCLOB member to express concern about back door searches. He did so in November's Section 215 hearing, and even suggested limiting back door searches to foreign intelligence purposes (which is not the standard for FBI, in any case) was inadequate. Nevertheless, in last week's report, he backed only very weak protections for back door searches, and did so within the context of national security versus non-national security, and not intelligence versus crime.

Now, I don't mean to pick on Dempsey exclusively — I'll have a few more posts on this issue. And to be clear, Dempsey does not represent CDT at PCLOB; he's there in his private capacity.

But I raised his affiliation with CDT because in that capacity, Dempsey was part of an amicus brief, along with representatives from ACLU, Center for National Security Studies, EPIC, and EFF, submitted in the In Re Sealed Case in 2002, in which the FISA Court of Review reversed Lamberth and permitted prosecutor involvement in FISA warrants. That brief strongly rebuts the kind of argument he adopted in last week's PCLOB report.

Here's what that brief had to say about the distinction between national security and non-national security and intelligence and crime in 2002:

> The Fourth Amendment applies to all criminal investigations, not merely those that are concerned with minor crimes. The government's assertion, of course, is not simply that espionage and terrorism crimes are especially serious ones, but that these crimes are special in a constitutional sense. Gov't Br. at 73-74. The government does not attempt to locate any support for this audacious assertion in the text of the Fourth Amendment (where there is, in any event, no support to be found); rather it relies on the fact that the prosecution of these crimes serves the ultimate

> purpose of protecting national security. Gov't Br. at 74. *Notwithstanding the government's assertion to the contrary, however, Fourth Amendment requirements do not turn on a criminal investigation's ultimate purpose*.
>
> [snip]
>
> The Supreme Court's "special needs" cases clearly reaffirm that any search whose primary or exclusive purpose is criminal investigation may proceed only on the basis of probable cause. *This basic constitutional protection is not suspended for investigations of crimes that are particularly serious, or for investigations whose ultimate purpose is to protect against threats to national security. Any investigation whose primary or exclusive purpose is to collect evidence of criminal conduct must adhere to the ordinary requirements of the Fourth Amendment*.
>
> The government's theory that FISA is available even for investigations that are purely criminal is profoundly troubling in itself, but it is made more so by the government's failure consistently to specify the crimes that in its view are constitutionally "special," let alone point to a constitutional or even statutory basis for such a specification. While the government refers to espionage and international terrorism as crimes that are entitled to special constitutional status, see, e.g., Govt. Br. at 38, *it repeatedly asserts the arrant principle that FISA is available to purely criminal investigations so long as the government believes that the prosecution of the crime will protect national security*. See, e.g., Govt. Br. at 37 ("[i]t is enough that the government intends to "protect" national security

> from foreign threats"); Govt. Br. at 38-39 n.13 (legislative history does "not undermine the idea that FISA may used [sic] to obtain evidence for a prosecution designed to protect national security"). The suggestion appears to be that the government could bypass the ordinary requirements of the Fourth Amendment not just in espionage and international terrorism investigations — a disturbing proposition on its own — but that the government could bypass the Fourth Amendment in any criminal investigation, however minor the crime being investigated, so long as the government believes that the prosecution is designed to protect national security from foreign threats.
>
> *The notion that a search or surveillance may be justified simply because the government invokes the rubric of "national security" flies in the face of the most basic principles of American constitutional democracy*. The government's theory would effectively allow the executive branch unilaterally to suspend the ordinary requirements of the Fourth Amendment simply by claiming that a prosecution is designed to address a threat to national security. This Court should not sanction the government's attempt to exploit the rubric of "national security" as a means of avoiding the basic Constitutional requirement that the government stay clear of constitutionally protected areas until it has probable cause to believe that a crime has been committed. [my emphasis]

In 2002, Dempsey (and CDT and several other NGOs) argued aggressively against precisely the argument Dempsey apparently now makes, that there are crimes that qualify as threats

to national security first and therefore for which the Fourth Amendment becomes special. Indeed, by pointing to PD-28, Dempsey may even be embracing an expansion of this national security category from what he argued against 12 years ago, to include cybersecurity and transnational crime (presumably including drugs).

Moreover, Dempsey should know — because he signed onto a brief that was appalled by the claim 12 years ago — that the government uses a breathtakingly broad interpretation of how garden variety crimes might be shoe-horned into that national security definition. So long as the government believes prosecution of a crime will protect national security — and in the oral argument in this case, Ted Olson actually argued that *not* prosecuting rape to coerce an informant might also count as national security use of a FISA wiretap — then it doesn't count as a criminal purpose.

Meaning FBI's assurances to PCLOB that using Section 702 data for criminal purposes are hypothetical rest on a definition of national security that has already swallowed the meaning of criminal.

And, of course, Dempsey signed onto that argument combatting his current position in the context of traditional FISA, not Section 702 collection that never requires probable cause on the front end.

It may just be a testament to the 12 year epidemic of Stockholm Syndrome we have suffered since Dempsey signed onto this brief. It may be that Dempsey is, in part, accounting for the In Re Sealed Case decision as precedent (though PCLOB goes beyond both that and FISCR's decision in Yahoo's challenge of Protect America Act surveillance). It may be that some interim events — I'll look at one in a follow-up post — have imperceptibly changed our notions of crime and national security. It may just be that Elisebeth Collins Cook and Rachel Brand were that persuasive (or Dempsey's desire to prevent

another partisan split on PCLOB that strong) that explains his change of position.

Whatever the explanation, James Dempsey signed onto a brief in 2002 that compelling argues his position last week was dangerously wrong.