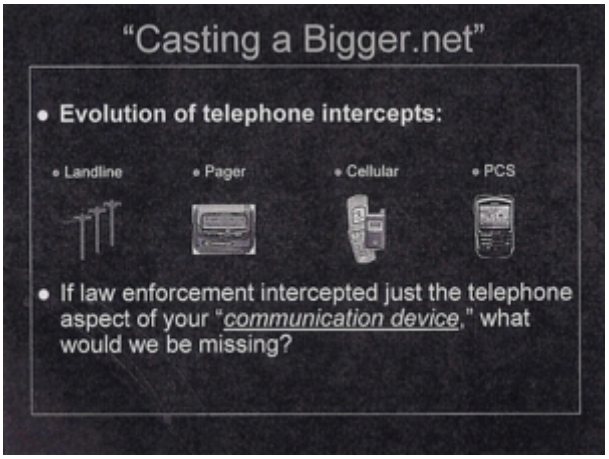
# FEDERAL PROSECUTORS ENCOURAGING LOCALITIES TO “CAST A BIGGER .NET”




Last month, Ars Tecnica reported on the Federal role in encouraging a data sharing agreement among a number of Virginia localities called the Hampton Roads Telephone Analysis Sharing Network.

The idea behind the program was to help localities do more sophisticated data analysis, both by (apparently) bringing the overall cost paid — both to telecoms, but also for shared licenses for the analytical software — down, but also by training and providing them with more sophisticated analytical tools. The article relied on a presentation liberated under open records act showing that this sharing was proposed by an investigative analyst in the Eastern District of VA US Attorney’s office.

One thing the presentation emphasized was how the latest version of the Lincoln Pen-Link software would permit the police departments to “cast a bigger .net” than earlier versions. It pointed to the advent of smart phones and asked,

> If law enforcement intercepted just the telephone aspect of your “communication device” what would we be missing?

The next slide answers that question: the cops

would be missing “Internet intercepts.” That is, in addition to telephone calls and text messages (plus some things no one uses anymore), it would be missing:

- VoIP
- Email
- Instant messaging
- Chats/forums/blogs
- File transfers/file sharing
- Video conferencing
- Web cam

Another slide boasts that Pen-Link 8 can conduct:

- Mobile intelligence
- GPS mapping
- Internet investigations
- Digital multimedia
- Live electronic surveillance
- Statistical and graphical analysis

I note this not just to raise concerns about the intrusive tools local cops are using to hunt drug dealers. But also to reiterate a point I made about USA Freedom Act.

We know, from documents like this and from Hemisphere, that federal law enforcement officials are using and encouraging localities to use CALEA equipment to obtain and analyze not just phone call metadata, but a whole slew of other things available via smart phones. Not just calls, but location and email and VOIP and phone cam information.

Call me crazy, but I think that suggests there is less than zero chance that they are also not also using these authorities under FISA to pursue terrorists and spies. And (as I’ll show later) because they claim (and FISC permits them to claim) the Fourth Amendment is weaker for national security investigations, they do it

with a much weaker standard of suspicion.

When the government adopts – and Congress ratifies – the notion of “connection chaining” via smart phones, there is a very very high likelihood this is the kind of analysis they are engaging in.