THE KELIHOS PEN REGISTER: CODIFYING AN EXPANSIVE DEFINITION OF DRAS?

As I noted in yesterday's post on the arrest of Pyotr Levashov, the government used a Rule 41 warrant ("in an abundance of caution," they explained in the application) to authorize the redirection of infected computers to the FBI sinkhole. As that was the first public use of the newly expanded authority, I expect there to be a lot of commentary about its use.

I'm just as interested in the Pen Register/Trap and Trace application accompanying the warrant, however. It authorizes the sinkhole to obtain the IP and routing address for infected computers, so the government can inform ISPs of the infection. I'm interested in it for the way it transcribes phone technology onto packet headers.

> 9. In the traditional telephone context, pen registers captured the destination phone numbers of outgoing calls, while trap and trace devices captured the phone numbers of incoming calls. Similar principles apply to electronic communications, as described below.
>
> 10. The Internet is a global network of computers and other devices. Devices directly connected to the Internet are identified by a unique Internet Protocol (*IP')address. This number is used to route information between devices. Generally, when one device requests information from a second device, the requesting device specifies its own IP address so that the responding device knows where to send its response.
>
> 11. On the Internet, data transferred between devices is not sent as a

continuous stream, but rather it is split into discrete packets. Generally, a single communication is sent as a series of data packets. When the packets reach their destination, the receiving device reassembles them into the complete communication. Each packet has two parts: a header with routing and control information, and a payload, which generally contains the content of the transmitted communication.

12. The packet header contains non-content dialing, routing, addressing and signaling information, including IP addresses and port numbers. Both the IP address of the requesting device (the source IP address) and the IP address of the receiving device (the destination IP address) are included in specific fields within the packet header, as are source and destination port numbers. On the Internet, IP addresses and port numbers function much like telephone numbers and area codes often both are necessary to route a communication. Sometimes these port numbers identify the type of service that is connected with a communication, such as email or web-browsing, *but often they identify a specific device on a private network*. In either case, port numbers are used to route data packets either to a specific device or a specific process running on a device. Thus, in both cases, port numbers are used by computers to route data packets to their final destinations.

13. The headers of data packets also contain other dialing, routing, addressing and signaling information. This information includes the transport protocol used (there are several different protocols that govern how data is transferred over networks); the flow label (for the most recent version of

> the Internet Protocol suite, called IPv6, the flow label helps control the path and order of transmission of packets); and the packet size. [my emphasis]

I'm sure the FBI has used similar PRTTs hundreds of times, including (perhaps especially) in the FISA context. But I'm not aware of one that has been made public. Moreover, the application of the PRTT is different here than in many contexts, because the sinkhole, not an ISP, will be obtaining the data requested.

I raise that because the PRTT asks for information — such as the use of a port number to ID a device running on a private network — that might be considered content to an ISP. If such an order were presented to an ISP, then, the request would arguably go beyond what a user had voluntarily shared with a third party, and therefore what should be available using a PRTT. (This paper from Matt Blaze and others from last year explains this in detail, though the paper notes that port numbers are specifically permitted by DOJ's Electronic Surveillance Manual.) The data is necessary to the intent here, because FBI is trying to ID which devices have been infected. But it's not clear the legal case is sound.

Yet the application describes it as dialing, routing, addressing, and signaling information (the DRAS definition at the base of PRTT law) without an explanation of this technical distinction, and without a discussion of what it means that the FBI sinkhole, and not an ISP, is collecting the data.

I suspect one reason the government has made all the materials associated with Levashov public is to codify their use. And that's true as much for this use of the PRTT as it is for the Rule 41 warrant.