DZHOKHAR TSARNAEV'S YAHOO WARRANT

The government has started unsealing a bunch of previously sealed documents from the Boston Marathon investigation. In this post I wanted to comment on a motion to suppress the evidence from a Yahoo, Google, and computer search.

There are two interesting details in it. The FBI got a warrant for both Tsarnaev brothers' Yahoo email on April 19, 2013, while Dzhokhar was still bleeding out in a boat in Watertown. The warrant basically got everything connected with the account, and then permitted the government to search both the contents and metadata for a list of things:

> 1. All communications between or among Tamerian [sic] Tsarnaev and Dzhokhar Tsarnaev;
>
> 2. All communications pertaining to the Boston Marathon, explosives, bombs, the making of improvised explosive devices, firearms, and potential people and places against which to use firearms, explosives or other destructive devices.;
>
> 3. The identity of the person or persons who have owned or operated the J.tsarnaev@yahoo.com and Tamerlan~tsarnaev@yahoo.com e-mail accounts or any associated e-mail accounts;
>
> 4. The data described in paragraphs II(A)(3)-(5), above [i.e., the contents of all electronic data files, whether word-processing, spreadsheet, image, video, or any other content, calendar data, and lists of friends, buddies, contacts, or other subscribers].
>
> 6. [sic] The existence and identity of any co-conspirators;

> 7. The travel or whereabouts of the person or persons who have owned or operated the J.tsarnaev@yahoo.com and Tamerlan_tsarnaev@yahoo.com e-mail accounts or any associated email accounts;
>
> 8. The identity, location, and ownership of any computers used to access these e-mail accounts;
>
> 9. Other e-mail or Internet accounts providing Internet access or remote data storage or e-commerce accounts;
>
> 10.The existence or location of physical media storing electronic data, such as hard drives, CD- or DVD-ROMs, or thumb drives; and
>
> 11.The existence or location of paper print-outs of any data from any of the above.

The motion went on to explain that item 4, above, included the following:

> 3. The contents of all electronic data files, whether word-processing, spreadsheet, image, video, or any other content;
>
> 4. The contents of all calendar data;
>
> 5. Lists of friends, buddies, contacts, or other subscribers.

I'm interested in this because the full list — including whatever other items were included in item 4 and whatever was originally numbered 5 — probably resembles what the government would get from Yahoo under PRISM, and therefore answers questions I raised in this post about how the government requests under PRISM to Yahoo expanded between August 2007 and January 2008. The calendar and buddy lists are unsurprising (indeed, we know NSA used to steal that stuff in the clear). But I'm also interested in how many

of the initial list address hardware, which suggests one thing they're likely getting under PRISM is mapping of such hardware. Also note the location-data of both the person using the account and the hardware associated with its use.

The other interesting detail is that the government didn't go after Dzhokhar's other Internet accounts until July 3, 2013, after he'd already been indicted.

> On July 3, 2013, after the grand jury had returned its indictment against Mr. Tsarnaev, the government sought search warrants for multiple providers, including Google, Facebook, YouTube, Twitter, Instagram, and Skype.

The motion doesn't say whether or not the government had already obtained the call detail records from these accounts, which it could have gotten with an administrative subpoena. It also doesn't include Vkontakte (which would have required an MLAT process), which both brothers used.

I'm most interested in this, however, because it means the government didn't go after Skype until over two months into the investigation. Remember: Dzhokhar had relied entirely on Skype for his "calling" for several weeks leading up to the attack, between the time his iPhone got shut down and the time he got a burner for use in the attack. So I find the delay of interest.

Of course, these Internet communications platforms are all things we believe the government dragnets the metadata of overseas. I assume they got call detail records using an Administrative subpoena, but technically it's the kind of thing they might not have needed to do.

Update: Nick Weaver pulled the warrant itself. Here's the section on connection logs.

> User connection logs for any connections

> to or from these and any associated e-mail accounts, including:
>
> a. Connection time and date;
>
> b. Disconnect time and date;
>
> c. The IP address that was used when the user connected to the service;
>
> d. Source and destination of any e-mail messages sent from or received by the account, and the date, time, and length of the message; and
>
> e. Any address to which e-mail was or is to be forwarded from the account or e-mail address.

Update: Here's a list of what has been released so far. Fox says they'll update as things get unsealed here.

- Motion to suppress fruits of searches at Norfolk Street and University of Massachusetts (Filed 05/07/14)
- Motion to suppress statements (Filed 05/07/14)
- Motion to suppress fruits of searches: Electronically stored information, including email communications and data contained in the Sony Vaio laptop computer (Filed 05/12/14)
- Letter from Carmen M. Ortiz, U.S. Attorney, District of Massachusetts (Written July 22, 2014)
- Government's opposition to

defendant’s renewed motion for hearing to address “leaks” (Filed 08/08/14)

- Motion to compel the government to comply with its expert disclosure obligations, and to suspend defendant’s expert disclosure deadline (Filed 07/25/14)
- Government’s opposition to defendant’s motion to compel compliance and suspend defendant’s expert disclosure deadline (Filed 08/08/14)
- United States of America v. Dzhokhar Tsarnaev (Order: August 18, 2014)
- Motion to compel discovery (Filed: 10/10/14)
- Sealed motion to seal motion to admit testimony by Sister Helean Prejean (May 8, 2015)
- Government’s reply to defendant’s opposition to its motion in limine to exclude the testimony of Sister Helen Prejean (May 9, 2015)
- Government’s opposition to defendant’s motion to compel compliance and suspend defendant’s expert disclosure deadline
- State Police Crime

Processing – Mercedes ML350 (April 28,2013)

- State Police Crime Scene evidence examination / latent print development (April 20, 2013)
- State Police firearms identification report (April 24, 2013)
- State Police bullet analysis
- State Police gunshot primer residue analysis (Oct. 30, 2013)
- FBI Laboratory report of items recovered at Boylston Street Scene 1 and Cambridge Apartment (April 21, 2014)
- State Police Firearms identification report (Aug. 22,2013)