WHY ROLL UP THE RUSSIAN SPY NETWORK NOW?

As a number of you have commented, DOJ announced the arrest of 10 alleged Russian spies yesterday (with one person, based in another country, remaining at large). The alleged spies are basically people living under false identities tasked to network with influential Americans to learn specific information.

One of the most interesting questions about the bust is the timing. It's clear from one of the complaints that the FBI has been tracking some of these alleged spooks for a decade. That suggests the government had been content, up to now, to simply track what Russia was tracking. But then, last week, they decided to roll up these alleged spies.

The timing and content of the two complaints adds to the interest of the question. The complaint describing the long-term surveillance, named Complaint 2 by DOJ, includes the following details from this year (showing the level of activity of the investigation with these longer-term suspects):

- A March 7 intercept from the Boston couple's townhouse
- A search from the female Boston defendant's safe deposit box conducted in April (one which implied there had been earlier searches of the box)
- Discussion of the male New Jersey defendant's travel to Russia in February to pick up a laptop (reflecting intercepts, physical

surveillance, and business records)
- Details describing the New Jersey defendant handing off the laptop he picked up in Moscow to the Seattle male defendant in early March
- January intercepts capturing discussions of Russian handlers encouraging the New Jersey female defendant to take a job tied to lobbying

In other words, at least from what appears in this complaint, none of the surveillance on these eight long-term alleged spies was all that recent.

The date on this complaint—named Complaint 2 but reflecting the decade of surveillance these defendants have been under—was Friday, June 25.

Then there's Complaint 1, which pertains to two additional defendants, Anna Chapman and Mikhail Semenko, and which is dated Sunday, June 27. The earliest dates in that complaint date back only to January 2010 (and June 2010 for Semenko), perhaps suggesting the FBI has had these two defendants under surveillance for a much shorter period of time. In addition, unlike the other complaint, this one does not provide details about the cover of the defendants (though there may be a number of reasons why this would be true).

Complaint 1 describes how FBI agents posed as Russian handlers and set up meetings with the two defendants on June 26—that is, the day **after** the complaint covering the eight other defendants was signed. In Semenko's case, the FBI agent asked the defendant to carry out a drop which—the complaint explains—he did.

In Chapman's case, the FBI agent asked her to hand off some money to another person purported

to be another member of the same Russian network. Rather than carry out the task, Chapman bought an international cell phone (trying, unsuccessfully, to cover her tracks), suggesting she called overseas for direction. She did not carry out the designated task. All of this suggests, of course, that by late on June 26 (that is, Saturday) the Russians presumably would have known someone pretending to be a Russian agent was onto Chapman.

The way these two complaints work together suggest DOJ decided on or before last Friday to roll up a spy network it had been tracking for a decade. Then, after having set that process into motion, it attempted to implicate two additional members of the network (Chapman and Semenko) in the following days. Doing so with Chapman probably alerted the Russians to FBI pursuit on Saturday.

After the Chapman call, FBI probably had to roll up the network. But the FBI had already made the decision to arrest the others. So why did DOJ decide to roll up this spy network now? Why not continue tracking what the Russians are tracking?

I can think of three potential reasons:

- To disrupt US-Russian relations
- Because the Russians had detected US (or third party) sabotage
- Because of other changes in DOJ personnel

Disrupting US-Russian relations

The Russians have already suggested that the arrest was timed to chill Russian-American relations following a great meeting between Obama and Medvedev.

> "We would like to note only that this type of release of information has

> happened more than once in the past, when our relations were on the rise," [a statement on the arrests from the Russian foreign ministry] said. "In any case, it deeply regrettable that all this is taking place on the background of the 'reset' in Russian-American relations declared by the United States administration itself."
>
> The arrests on Monday came after a period of warming in relations between the United States and Russia, with President Dmitri A. Medvedev making a visit to the United States this month, including to Silicon Valley in California, that was hailed here as a success. Mr. Medvedev met with President Obama, and the two seemed to have developed a personal bond.
>
> Some Russian politicians declared that the announcement of the arrests indicated that hostile elements in the United States government were bent on preventing relations from flourishing.

Obama, too is said to be miffed about the timing.

> After years of F.B.I. surveillance, investigators decided to make the arrests last weekend, just days after an upbeat visit to President Obama by the Russian president, Dmitri A. Medvedev, one administration official said. Mr. Obama was not happy about the timing, but investigators feared some of their targets might flee, the official said.

So if this explains the timing, then somehow the decision was made in spite of Obama's efforts to establish better relations with the Russians.

Russian detection of US (or third party) sabotage

There's also the possibility that the Russians had either detected the US surveillance or discovered sabotage of their communication network by the US or a third party.

Of particular interest, between the two complaints, there are references to three different problems with the laptops the Russians used to conduct secure WiFi communication.

Complaint 2 describes the Seattle defendants having trouble with their laptop communications.

> ZOTTOLI and MURPHY sat down together at a table where they stayed for approximately one hour and fifty minutes. During that time, law-enforcement agents stationed inside the Coffee Shop overheard MURPHY and ZOTTOLI discussing problems that the Seattle Conspirators were having with the computer equipment that they used for communicating with Center. In response to ZOTTOLI's description of these communication problems, MURPHY stated (in substance and in part), "this should help." MURPHY further responded (in substance and in part), "if this doesn't work we can meet again in six months," and also said "they don't understand what we got through over here."

Complaint 1 describes the FBI agent posing as a Russian handler discussing problems Chapman was having with her laptop.

> UC-1 asked, "So, tell me the notebooks? Are you still having a problem with the notebook? With the connection?" CHAPMAN replied, "Yes. I thought you were flying back so it is alright." UC-1 stated, "Do you want me … well [sic] can give it to consulate if you want them to look at it or you can wait and take it home yourself to Moscow." CHAPMAN stated, "It would be more convenient if I gave you it." Later, in the course of the

> meeting, CHAPMAN provided the laptop computer to UC-1 (hereafter the "Laptop"). Based on my training, experience, and participation in this investigation, I believe that the Laptop is the computer, which was beset by technical difficulties and which was used for laptop-to-laptop cover communications between CHAPMAN and Russian Government Official #1.

(Note, too, that one session when Russian Government Official #1 tried to establish laptop communication with Chapman, he noticed the FBI surveillance of him, and did not make the connection.)

Finally, Complaint 1 describes the FBI agent posing as a Russian handler telling Semenko he thought Semenko had problems with a transmission on June 5.

> UC-2 told Semenko that he wanted to discuss SEMENKO's attempted communication at the Restaurant on June 5, 2010. UC-2 told SEMENKO that UC-2 believed the communication attempt had not been successful, to which SEMENKO respondted, "I got mine." SEMENKO further explained that equipment he had been using for communication had automatically turned itself off at the end of the communications session, which SEMENKO stated was a sign that the communication was successful. SEMENKO further explained that, when he turned the equipment on again after it had shut down, he "saw the stuff [he] received," and also said that when the communication went through he was "like … totally happy."

And in the description of FBI surveillance of this, the complaint states that Semenko "was trying to utilize the private wireless network system," suggesting maybe the FBI knew that this

communication to have failed.

Now, there are a number of possible causes for this plethora of seemingly-problematic laptops. Maybe the Russian system is klugey, meaning the poor alleged spies sitting in their coffee houses have to try to finesse the connection each time. Maybe the US managed to sabotage the system (though they specify that their surveillance of this system used a commercially available program) which was causing problems with the WiFi communication. Maybe someone else has intercepted the system, and the US became aware that they weren't the only ones watching the alleged Russian spies.

Further note that complaint 1 makes it clear that Murphy purchased one laptop, traveled with it to Russian in February, and returned with a laptop of the same model but different serial number, to give it to Zottoli in March. And Chapman was about to travel with her purportedly problematic laptop to Russia in a few weeks. So whatever the issue with the laptops, the laptops were being dealt with directly in Russia, and they were about to get one of the laptops (Chapman's) seemingly having problems.

Changes in DOJ personnel

Finally, there's this curious detail of timing. The decision to roll up this network was obviously made on or before Friday, June 25.

As it happens, the DOJ also made a significant personnel announcement on Friday, naming the FBI's Special Agent in Charge in Philadelphia to to lead the NY Office.

> **Janice Fedarcyk** has been named assistant director in charge of the FBI's New York Division, FBI Director **Robert Mueller** announced Friday. Fedarcyk is the first woman to head the high-profile New York office.She replaces **Joseph Demarest**, who in May was named Assistant Director of the International Operations Division at FBI headquarters. Demarest was placed on temporary assignment to FBI headquarters

> while the Office of Professional Responsibility conducted an investigation into statements he made about a relationship he allegedly had with a subordinate in the New York office.
>
> Since 2007, Fedarcyk has headed the FBI's Philadelphia Division, which was recently involved with the indictment against American-born alleged extremist "Jihad Jane."
>
> Mueller said in a statement that Fedarcyk is well-prepared to lead the FBI's largest office.
>
> "Jan Fedarcyk brings both a strong national security and criminal investigative background from her current assignment as head of the Philadelphia Division and from her work at FBI Headquarters, where she managed terrorist financing investigations, served at the National Counterterrorism Center, and oversaw investigations of online exploitation of children," Mueller said.

This was a fairly sudden appointment.

Now I have no clue whether there's a connection between the timing of the arrests and the arrival of Fedarcyk in NY. But I find it notable that this decade-long, politically sensitive investigation got pulled just as the FBI office in charge of the investigation got a new boss.

Update: ApacheTrout offers another possibility:

> I'd like to add a 4th reason for consideration: that the quality of the information channeled by the alleged spy ring increased to the point where the FBI felt a significant security breach was about to occur. In other words, the FBI was okay with rinky dink info being sent to Russia all those years, but

> suddenly big time secrets were about to be stolen and sent to Russia, and that had to be stopped.

Update: One more point about timing. Look at the timing of the Saturday, June 26 meetings:

> Unspecified time: UC-2 calls Semenko on phone recorded pursuant to judicial order, arranges 7:30 PM meeting.
>
> 11:00 AM: UC-1 calls Chapman on consensually recorded call (not judicial order), tells her he has to meet her that day to give her something
>
> 12:30 PM: Chapman calls UC-1, call is recorded per judicial order. She told him it would be difficult to meet that day and asks whether they can meet the following day.
>
> 1:00 PM: Chapman calls UC-1 a third time, says she will come to NY and call UC-1 at 4:00 PM.
>
> 4:30 PM: Chapman and UC-1 meet. (UC-1 tells Chapman that it took him three hours to get to meeting place.)
>
> 6:00 PM: Chapman purchases international cell phone, ostensibly to alert others about contact.
>
> 7:30: UC-2 and Semenko meet.

That is, by the time UC-2 met, FBI already knew that Chapman had purchased her phone, if not made her call. Also note that they apparently did not have a warrant for the first call to Chapman, but they did for the call to Semenko, though given that those took place in different cities, can't necessarily conclude that the Semenko call preceded the Chapman one.