THE DISCOVERY REFRIGERATOR: WHEN JOSHUA SCHULTE SOCIAL ENGINEERED HIS CELLMATE'S BROTHER

In advance of some other things, I want to look at the time that Joshua Schulte, who was convicted last week on nine counts related to stealing and leaking CIA files to WikiLeaks, social engineered the brother of his cellmate.

One of the charges on which the jury found Schulte guilty was sending WaPo reporter Shane Harris a warrant affidavit from the investigation into him, along with Schulte's own narrative purportedly debunking the allegations made in the warrant. The jury found that Schulte's description of two hundred people who might have access to the DevLAN backups and the network setup that would allow them that access was National Defense Information. Effectively, prosecutors argued and the jury agreed, Schulte was revealing CIA's organizational structure and numbers of classified employees to a journalist. It's a picayune Espionage count that because it likely won't be treated as the same leak as the charge for sending CIA's hacking tools, could add years to Schulte's sentence.

Schulte sent the warrant affidavits along with a dangle, a promise to tell Harris some dirt about Russian oligarchs' ties to Marc Kasowitz and Rudy Giuliani.

> We have decided to share with you an initial exposé (depending on how the first one goes with you we will share up to nine more) involving Russian oligarchs, business ties and wire transfers involving hundreds of millions of dollars to Donald Trump's closest advisers and law firms, including

> Giuliani and Mark Kasowitz firms. Trump's self-reported best friend plays a starting role.

In cross-examination of FBI Agent Evan Schlessinger, Schulte suggested, credibly, that this dangle came from his cellmate, Omar Amanat.

> Q. Well, you remember the ProtonMail email that referenced Marc Kasowitz, right?
>
> A. Yes.
>
> Q. OK. And there's no relation between me and Marc Kasowitz, right?
>
> A. No. You're — not that I'm aware of.
>
> Q. OK. Let's talk about the cell search at the MCC. Now, in the cell search at the MCC, did you know what cell I was in?
>
> A. Yes.
>
> Q. And just real quick, you did know that there was a relationship between Mr. Amanat and Marc Kasowitz, right?
>
> A. I know it was a — it's connected to Mr. Amanat. I don't know exactly how.
>
> Q. OK.
>
> A. Or how it relates to Mr. Amanat.

Of course, Schulte wasn't charged for leaking information about Trump's once and future lawyers. He was charged for sharing information about the CIA that — even if Amanat were the one who sent the email to Harris — would still mean Schulte shared it with Amanat, someone else who wasn't cleared to receive it.

Plus, the record now shows that Schulte had been working with Omar Amanat and his brother, Irfan, to get these documents out.

An FBI interview of Schulte's cousin, Shane

Presnall, conducted just days before his first trial on January 13, 2020 but only released in April, explains that the Amanats were participating in the effort to publicize Schulte's case starting as soon as Schulte and Amanat ended up in a cell together in December 2017. In fact, Presnall handed off Schulte's warrants (it's not clear whether this includes Schulte's response, which is where the classified information was) to Amanat's brother, Irfan, by leaving them in the fridge at the apartment he had shared with Schulte. (At the time, Irfan had been charged in the same fraud as Omar, but he was still out on pretrial release; since these events in 2018, both Omar and Irfan have been sentenced, served their time, and released.)

> JS's idea to get to press was to get court documents to get more attention to his case. JS told SP he was trying to create public outrage. When arrested in December 2017, another inmate in MCC, named Omar Amanat, told JS that Omar had media comments [sic] and that JS should send documents out and Omar will get them out. SP expressed skepticism about having a stranger do this. Then Omar's cousin (Iffy) reaches out to SP via WhatsApp and says they have media contacts and can get documents out. When moving everything out of the apartment, SP put the documents in the bottom of the fridge in his apartment and informed Iffy where the where the documents would be. Iffy came and got the documents at JS's apartment. Iffy confirmed to SP that Iffy got the documents. Iffy had the key because SP handed it to him.

Presnall was also communicating with reporters via Signal and a ProtonMail account, JohnGalt. But after he handed off the documents, he never heard from Irfan again.

But Schulte and the Amanats continued to work closely to get the documents out.

Just days before the ProtonMail dangle with the warrants was sent to Harris on September 24, the Samsung phone primarily used by Schulte texted Irfan on Signal. [This is a version of the Signal report, GX 822-1 as submitted in the first trial, but in which I replaced phone numbers with names and eliminated extraneous data; the righthand-most column shows who sent a particular text, the second-from-right is who received it.]

Schulte claimed to be Omar. He said that J — Schulte — needed "screen shots of Romania hack and Moscow."

Hey bro	2018-09-22T19:57:49	outgoing	Irfan	Samsung
It's your Lil bro from J cell	2018-09-22T19:58:24	outgoing	Irfan	Samsung
Hey	2018-09-22T20:01:54	incoming	Samsung	Irfan
Hey	2018-09-22T20:02:06	outgoing	Irfan	Samsung
Confused got 2 messages from u	2018-09-22T20:02:22	incoming	Samsung	Irfan
Did you just call	2018-09-22T20:02:39	incoming	Samsung	Irfan
J needs screen shots of Romania hack and Moscow	2018-09-22T20:02:53	outgoing	Irfan	Samsung
On Yahoo.	2018-09-22T20:02:56	outgoing	Irfan	Samsung
I didn't call	2018-09-22T20:02:59	outgoing	Irfan	Samsung
On purpose	2018-09-22T20:03:08	outgoing	Irfan	Samsung
Ok got a call from your other phone	2018-09-22T20:03:31	incoming	Samsung	Irfan
Ok sending. Was just reviewing	2018-09-22T20:03:41	incoming	Samsung	Irfan
Probably by mistake	2018-09-22T20:03:46	outgoing	Irfan	Samsung

Irfan was understandably confused because, at the same time as someone claiming to be his brother was texting from the Samsung, someone else was calling him on what must be the iPhone that Omar primarily used.

Nevertheless, Irfan sent the files and only then did Schulte tell Omar's brother he had pretended to be Omar to get Irfan to send files he had been trying to get from his cellmate.

Romania andd abu moscow	2018-09-22T20:22:31	outgoing	Irfan	Samsung
?	2018-09-22T20:22:41	outgoing	Irfan	Samsung
hmm	2018-09-22T20:23:12	incoming	Samsung	Irfan
resending all	2018-09-22T20:23:16	incoming	Samsung	Irfan
File Transfer: /data/user/0/org.thoughtcrime.securesms/app_parts/part931762616.mms	2018-09-22T20:23:36	incoming	Samsung	Irfan
File Transfer: /data/user/0/org.thoughtcrime.securesms/app_parts/part-1577809699.mms	2018-09-22T20:24:09	incoming	Samsung	Irfan
File Transfer: /data/user/0/org.thoughtcrime.securesms/app_parts/part-1094684893.mms	2018-09-22T20:24:14	incoming	Samsung	Irfan
File Transfer: /data/user/0/org.thoughtcrime.securesms/app_parts/part430820762.mms	2018-09-22T20:24:40	incoming	Samsung	Irfan
review and let me know	2018-09-22T20:25:12	incoming	Samsung	Irfan
got it?	2018-09-22T20:48:33	incoming	Samsung	Irfan
Yes ty	2018-09-22T22:12:08	outgoing	Irfan	Samsung
The write-ups for epoch time and the Yahoo declaration included several GX exhibits? Did you get those online or do you have a copy of all the GX exhibits?	2018-09-22T22:26:42	outgoing	Irfan	Samsung
have copy of most GX. which ones needed	2018-09-22T22:27:03	incoming	Samsung	Irfan
send me write up I'll check	2018-09-22T22:27:13	incoming	Samsung	Irfan
The ones in the reference for the expert report: GX 3553, 3549, 3550, 3551, 3552, 3579A, 3579B,	2018-09-22T22:29:57	outgoing	Irfan	Samsung
File Transfer: /data/user/0/org.thoughtcrime.securesms/app_parts/part1993391788.mms	2018-09-22T22:34:19	incoming	Samsung	Irfan
File Transfer: /data/user/0/org.thoughtcrime.securesms/app_parts/part-1345819090.mms	2018-09-22T22:34:31	incoming	Samsung	Irfan
File Transfer: /data/user/0/org.thoughtcrime.securesms/app_parts/part-338756291.mms	2018-09-22T22:34:35	incoming	Samsung	Irfan
File Transfer: /data/user/0/org.thoughtcrime.securesms/app_parts/part1730408322.mms	2018-09-22T22:34:44	incoming	Samsung	Irfan
File Transfer: /data/user/0/org.thoughtcrime.securesms/app_parts/part-2057752853.mms	2018-09-22T22:34:48	incoming	Samsung	Irfan
File Transfer: /data/user/0/org.thoughtcrime.securesms/app_parts/part1298981091.mms	2018-09-22T22:34:52	incoming	Samsung	Irfan
File Transfer: /data/user/0/org.thoughtcrime.securesms/app_parts/part244243140.mms	2018-09-22T22:34:56	incoming	Samsung	Irfan
OMG you're the best	2018-09-22T22:35:16	outgoing	Irfan	Samsung
lol you're the guide	2018-09-22T22:35:37	incoming	Samsung	Irfan
I've been trying to get O to get those for me for weeks rofl	2018-09-22T22:35:43	outgoing	Irfan	Samsung
This is J	2018-09-22T22:35:53	outgoing	Irfan	Samsung
[emoji:FACE WITH ROLLING EYES]	2018-09-22T22:36:06	outgoing	Irfan	Samsung
haha don't you know O is great but he has a fragmented brain for docs :)	2018-09-22T22:36:08	incoming	Samsung	Irfan
I call him master airhead	2018-09-22T22:36:31	outgoing	Irfan	Samsung

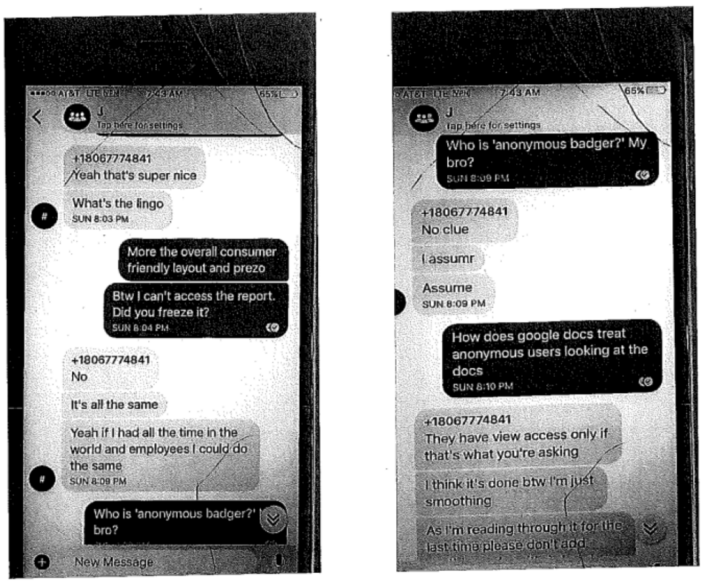
Irfan and Schulte had a good laugh together

about “master airhead” Omar, and then they got back to work on the documents they were working on.

Over the next two days Irfan and Schulte chatted away as they worked on various files, at several points, switching to group chat. At one point, Omar asked who “anonymous badger” is. “My bro?”

Who is 'anonymous badger? My bro?	2018-09-24T00:09:29	incoming	Group	
No clue	2018-09-24T00:09:37	outgoing	Group	Samsung
I assumr	2018-09-24T00:09:40	outgoing	Group	Samsung
Assume	2018-09-24T00:09:43	outgoing	Group	Samsung
How does google docs treat anonymous users looking at the docs	2018-09-24T00:10:06	incoming	Group	

Here’s a picture of Omar’s side of that conversation, working on the Google doc via his iPhone while Schulte and Irfan worked from other locations, from one of the 2018 warrant affidavits tied to this part of the investigation.



On September 26, Schulte texted Irfan to say that Omar broke a screen (perhaps an exacerbation of the crack seen above) but that everything was still a go.

Hey O's screen broke... But we're all good here... Still on for tomorrow	2018-09-25T23:59:00	outgoing
oh hey ok good thanks for letting me know was worried!	2018-09-25T23:59:35	incoming

That’s the day when jailhouse informant Carlos Betances narced them out to the guard before they could do … something … in the law library.

> Q. Mr. Betances, did there come a time when you learned of an effort to take the Samsung somewhere else in the jail?

A. Yes.

Q. And what did you learn about that?

A. That they were going to pay this friend of mine, Flaco, 200 bucks to take it down to the library that day.

Q. And who wanted to pay to bring the phone to the library?

MR. SCHULTE: Objection. Hearsay.

THE COURT: How did you learn about that information?

THE WITNESS: Because Flaco told me.

[snip]

BY MR. LOCKARD: Q. Mr. Betances, did you observe anything about Mr. Schulte's or Omar's behavior around that time?

A. Yes. They were very wary. They wanted to go down to the library then, and – so once I realized that they wanted to go down there, I threw this little piece of paper at the guard who was right there, and letting him know that something was going to happen in the library, that he could – he should –

THE INTERPRETER: Interpreter correction. A. – that he should conduct a search or everybody should go down and figure out what was about to happen. So that is what happened. When Josh and Omar came up, they said something had happened, that there was a search, there had been a search in the library, but they never found out that I was the one who had prevented that from happening.

Q. And did you hear Mr. Schulte or Omar discuss why they wanted the phone in the library?

MR. SCHULTE: Objection.

THE COURT: Overruled.

> A. They wanted to send something very important. I don't know what it was, but it was important. They had spent a week, a long time with the phones. They would give me the phone back very late at night with a very low charge.

Over the course of the next few days, as one after another of the detainees in on the contraband phone gig got caught and put into the SHU, it seemed that Omar came to rely on the Samsung (the first of the contraband phones was seized on September 26) to send Irfan gloomy texts. What appears to be Omar asks Irfan to call Carlos' son to let the son know they'd put $500 in his father's commissary fund, something that Betances testified to at the second trial, claiming he newly remembered just last month being offered a $5,000 bribe through the air conditioning pipes to stay quiet.

So as the brothers allegedly discussed arranging paying off the guy who narced them out, they also discussed what Harris has received. "How much to carlo," Irfan asked about the payment. "Washpo has em," Omar discussed the documents.

Ok can u send $500 to 3477864211	2018-09-29T01:15:07	outgoing	Irfan	Samsung
Good meeting with Mark he was shocked	2018-09-29T01:15:11	incoming	Samsung	Irfan
Ok	2018-09-29T01:15:13	incoming	Samsung	Irfan
Will send	2018-09-29T01:15:20	incoming	Samsung	Irfan
Did he read artickes	2018-09-29T01:15:20	outgoing	Irfan	Samsung
How much to carlo	2018-09-29T01:15:24	incoming	Samsung	Irfan
Washpo has em. Except for day at MCC. They don't have that one. Just Russia	2018-09-29T01:15:37	outgoing	Irfan	Samsung
Yes I have him at Redvertro	2018-09-29T01:15:41	incoming	Samsung	Irfan
And tech	2018-09-29T01:15:46	incoming	Samsung	Irfan
And tech report	2018-09-29T01:15:48	outgoing	Irfan	Samsung
And entire story	2018-09-29T01:15:52	incoming	Samsung	Irfan
Yes he got both	2018-09-29T01:15:54	incoming	Samsung	Irfan
Oh ok	2018-09-29T01:16:07	outgoing	Irfan	Samsung
What does he think	2018-09-29T01:16:12	outgoing	Irfan	Samsung
Will follow up with him	2018-09-29T01:16:16	incoming	Samsung	Irfan
Shocked but not surprised it's the world today	2018-09-29T01:16:28	incoming	Samsung	Irfan

The very last Signal text sent on the phone, on a day when Schulte was definitely in SHU but Omar was not yet, was a text from Omar to Harris, asking if they could shift to a different ProtonMail address, psalms100@protonmail.com.

Hi Shane, the anon email is down since Sunday evening Can you resend your questions to psalms100@protonmail.com. thanks	2018-10-02T21:54:50	outgoing	Harris	Samsung

It's a point Schulte made at trial: When that last text was sent, he was in SHU. He couldn't have sent it.

According to Agent Schlessinger, there was no

activity on the ProtonMail account Schulte had described in his notebook setting up on August 21, Annon1204, after Schulte was put in SHU. While Schulte pointed to a follow-up, on Annon1204, on September 26 that he suggested must have come from Omar, the switch to a different ProtonMail account after Schulte was moved overnight on October 1 is consistent with Omar not having the password for Annon1204, and so moving the ongoing conversation with Harris to another ProtonMail account, psalms100.

The entire (resumed) conversation with Shane Harris started with Schulte pretending to be Anonymous, partly in an effort to get Harris to send documents that Schulte's family had already been warned, by the FBI, not to release publicly. Along the way, Schulte pretended to be Omar and then Omar pretended to be Schulte pretending to be Anonymous.

It was a grand scheme across contraband cell phones and Google docs to send out a bunch of documents. One of which, the jury has now issued their verdict, constituted a very costly crime.