THE ALFA BANK DARK NET AT NOON

Before its John Doe nuisance lawsuits got shut down by Vladimir Putin's invasion of Ukraine, Alfa Bank made several claims that led me to chase down a minor — but potentially important — part of the Alfa Bank story.
Someone totally uninvolved in the Michael Sussman/Fusion/April Lorenzen effort played a role in making their efforts public in 2016: "Phil," the guy about whom I went to the FBI in 2017. As I told the FBI, I suspected he had played a role in the Guccifer 2.0 and Shadow Brokers operations.

This post will focus on what Alfa Bank got wrong. A follow-up post will look at why, if John Durham made the same error, it may matter for the Michael Sussmann case.

Someone exposes Tea Leaves' research via Krypt3ia

At issue is this post on the eponymously-named InfoSec blog Krypt3ia. As the post describes, someone tipped Krypt3ia off to a WordPress site and a purported i2p site (also called an "eepsite") that laid out a version of the claims that Michael Sussmann had shared with the FBI and the NYT in September 2016.

Those claims are at the heart of the false statement charge against Sussmann.

Along with the basic allegations about weird DNS look-ups between servers from Alfa Bank and Spectrum Health and a Trump marketing server, those sites also revealed that after the NYT called Alfa Bank for comment about the DNS anomaly in September 2016, the Trump DNS address changed. This is the digital equivalent of someone changing their phone number after

discovering they were being surveilled. The seeming response by Trump to the NYT call to Alfa for comment has always been regarded as the smoking gun showing human acknowledgement of the communications (a report from Alfa Bank attempted, unpersuasively, to contest that).

By connecting to a Russian-hosted proxy service, the Krypt3ia post about all this added an element of Russian mystery to the story. But that's it. The post offered no other new content.

The Krypt3ia post is more important for the function it played than its content. Krypt3ia's post served to make the contents of a publicly available but difficult to find i2p site — believed to be created by data scientist April Lorenzen, but written under the pseudonym Tea Leaves — accessible.

In response to tips from source(s) of his, Krypt3ia focused attention on a series of communications, none tied in his post to a then-identified person. First, someone alerted him to the WordPress site. That site spoke of Tea Leaves as a third person; there was never a pretense that it was Tea Leaves or Lorenzen. Krypt3ia learned of that WordPress site because someone approached Krypt3ia, purportedly asking for help finding an incomplete i2p address listed in the post.

> I caught wind of the site when someone asked me to look at an i2p address that they couldn't figure out and once I began to read the sites [sic] claims I thought this would be an interesting post.

That tip led Krypt3ia to find what was actually a proxy allowing access to a real i2p site — the one that injected an air of Russian mystery to the story.

> First off, the i2p address in the WordPress site is wrong from the start. Once I dug around I found that the real

> address was gdd.i2p.xyz which is actually a site hosted on a server in Moscow on Marosnet.

That led Krypt3ia to ask whether anyone at NYT wanted to verify the claim that Trump Organization seemingly took action after NYT called Alfa.

> I also have to wonder about this whole allegation that a NYT reporter asked about this.
>
> Say, any of you NYT's people out there care to respond?

Ask and you shall receive! Someone—as I lay out below, I have confirmed that this was "Phil"—put Krypt3ia in touch with a NYT reporter.

> First off, someone in my feed put me in touch with the NYT and a reporter has confirmed to me that what the site says about NYT reaching out and asking about the connections, then the connections going bye bye is in fact true.
>
> [snip]
>
> The biggest takeaway is that the NYT confirmed that they asked the question and shit happened. They are still looking into it.

In an update, someone purporting to be Tea Leaves responded to Krypt3ia via an untraceable Tutanota email account, and in response, Krypt3ia posed a bunch of questions, only to get no answer. That non-answer was a key reason why Krypt3ia later treated the allegations as a fraud — an opinion that Alfa Bank, at least, used to bolster their own claims of fraud.

As Krypt3ia mused in real time, it seemed that the entire point of the tips he was receiving was focusing attention on the allegations themselves. Except, if your goal was to release

a story that might swing an election, it was a really weird way of doing so.

> One does wonder though just who might be trying this tac to attempt to cause Donny trouble. It seems a half assed attempt at best or perhaps they were not finished with it yet.. But then why the tip off email to someone who then got in touch with me? Someone I spoke to about this alluded to maybe that was the plan, for me to blog about this from the start..
>
> [snip]
>
> I have to say it though, these guys are trying to get the word out but in a strange way. I mean this eepsite is now hosted in Czechoslovakia, staying with the Baltic flavor but why not broadcast this more openly? Why does the WordPress site have the wrong address to start and then the other eepsite disappears after a little poking and prodding?

There are at least four unattributed or unattributable communications that appeared in this post: an email to someone who, in turn, got in touch with Krypt3ia; a tip about the WordPress site (presumably from the person who got the email) and through it to the i2p gateway; the contact with the unnamed NYT reporter; and the email from someone claiming to be Tea Leaves via a service that made it impossible to prove it was the person who originally adopted that pseudonym.

Notably, this all happened between October 5, 2016 — before the Podesta drop and the DHS attribution of the DNC hack to Russia — and the days after it. Krypt3ia was checking out the i2p proxy on October 7, at 3:08PM ET — less than half an hour before DHS would release an unprecedented attribution statement, followed shortly by the Access Hollywood video, followed shortly by the first Podesta email drop.

Krypt3ia wrote his post the following day.

i2p sites aren't supposed to get noticed

To understand why using Krypt3ia to get noticed is so weird, you need to understand a little about i2p.

i2p is a network like Tor that provides obscurity and security. Even today, it's far less accessible than Tor (and was even more so in 2016). Krypt3ia could credibly access it, but I couldn't have. Reporter Eric Lichtblau or Fusion GPS' Laura Seago probably couldn't have either. Normally you need either a special browser or a gateway to to access an eepsite. Importantly, the public DNS routing information that was at the heart of the project that discovered the Alfa Bank anomalies doesn't exist for i2p. You can't just Google for a site.

If data scientist April Lorenzen put her research on an i2p site, as alleged, she may have done so to limit who noticed it and her role in it.

It didn't work out that way.

(Note, because the Durham investigation remains ongoing, I am not contacting her or her lawyers for comment or others who are obviously still the focus of Durham's investigation.)

Krypt3ia didn't link directly to her i2p site at first. He started by linking a gateway, which would be accessible to mere mortals who don't have an i2p browser or technical prowess. His second link may have been a different gateway — again, a link readily accessible to people without using special software. It was one of these links that got sent around by journalists and researchers.

That's what I mean about content versus function: Krypt3ia added no new content to this story. He did, however, make parts of it accessible to people — like reporters — who

would otherwise never have found it.

A comment purportedly from Lorenzen sent to Krypt3ia's site, playing on Tea Leaves' name, expressed (or feigned) surprise at finding what the email called a mirror (but which was a proxy).

> Thank you to https://krypt3ia .wordpress.com for pointing out a possible mirror of this (the original, what you are reading, http://gdd.i2p). We did not know about gdd.i2p.xyz until hearing about it from Krypt3ia. So we did a little research and see that i2p.xyz has been around for years and appears to mirror a lot of *.i2p sites. *i2p.xyz probably functions as an alternative for everybody that doesn't have the skills to reach an i2p site :)
>
> Next question, why would somebody first mirror — and then drop their mirror — of our http://gdd.i2p website. The following is just speculation: maybe normally i2p.xyz just mirrors everything but oops! Something hot — drop the mirror. I don't know. I didn't try to visit it. Mirrors of course could choose to alter content and measure who visits. We have no such opportunity to see who is visiting our real i2p site.

Whoever wrote the email, it emphasized how the proxy was different from the "real i2p site:" The proxy "functions as an alternative for everybody who that doesn't have the skills to reach an i2p site," but it also can "measure who visits" whereas a "real i2p site" cannot.

Whatever the story behind the Krypt3ia post, it had the effect of making it clear that researchers who believed they could find hackers by looking at public DNS data couldn't hide what they were doing, even on networks designed to be untrackable. It had the effect of making it clear their efforts to look for Russian hackers

in DNS data had been seen.

Alfa Bank alleges the Krypt3ia notice is part of an imagined conspiracy targeting the bank

It also appears to have convinced Alfa Bank that Krypt3ia was a key cog in the publication of this story. Their lawsuit claimed that,

> The scientists and researchers who obtained the nonpublic DNS data deliberately leaked portions of that data to other scientists and researchers and, ultimately, to the media.

Depositions in the Alfa Bank lawsuit make it clear that Alfa believed (presumably because of those characteristics about i2p) that Fusion GPS must have been behind the effort to alert Krypt3ia to the research site and, via his post, to alert the public.

In a February 10 bid to overcome privilege claims that Fusion GPS' Laura Seago had previously made, Alfa Bank lawyer Margaret Krawiec argued that Seago must have breached any privilege by sharing information from the publicly posted Tea Leaves information. Krawiec's logic was that someone internal to the privilege claims asserted by Perkins Coie must have told Seago where the i2p site was, because otherwise there would be no way she could find it.

> Krawiec: So, your honor, let me jump in there because one of the things that happened is that we were trying to understand how it was that Ms. Seago knew that this data had been published on the internet because it was published in an obscure place in the internet by

> this Tea Leaves that I told you about.
>
> And then what Fusion did was – so we asked about that. We said, "How did you know where to look for that data? Who told you?" Cut off, instruction not to answer, privileged. But guess what they did with those links of that data? They took that data that someone told them because no one would have known to find it where it was unless someone told them.
>
> And they wouldn't tell us who told them or how they found it, but then they took all those links – the supposed public source research – and disseminated it to seven or eight media outlets saying you have to check this out. This is big stuff.

Fusion's lawyer Joshua Levy countered that the link and the site itself were public.

> Levy: If you – if you take the example that Alfa-Bank's lawyer just presented to the Court, the link that someone at Fusion had circulated to a reporter, that link is a link to the internet. It's a publicly available link, right?
>
> The link – it's, it's like sending a New York Times article to a reporter at the Washington Post. Have you – have you seen this article? You should look at it. It's interesting. Here's a link. It happens to do with the subject matter which (indiscernible) is fascinated, [sic] but it's a publicly available link.
>
> Ms. Seago may have had communications internally at Fusion about that link. Those are privileged communications, but the link itself is available online for the Court, for me, for Ms. Krawiec. It's public. There's, there's nothing confidential about that link.

Alfa's lawyer responded by arguing that because an i2p site was so difficult to find, Seago's knowledge of its location must have come from privileged information, and because she subsequently shared a link to a gateway with journalists, she had waived privilege.

> Krawiec: Your Honor, I can tell you that where this link was when it was on the internet, you, myself, Mr. Levy, no one could have found that by doing a basic Google search. They were instructed where to find it in this obscure location.
>
> And all we were trying to understand is who instructed them because the person who posted it was Tea Leaves, the anonymous computer scientist who had this computer data.

Alfa's lawyer argued, not unreasonably, that because Tea Leaves' site could not have been discovered by a Google search, someone connected to Tea Leaves must have told Fusion where it was, and because Fusion, in turn, shared a link to it, any privilege around Fusion's discussions about Tea Leaves had therefore been breached.

Alfa's focus on how Tea Leaves' i2p site became public continued during a February 14 deposition of Peter Fritsch. In it, Alfa raised an email from Seago to Fritsch describing that Krypt3ia had become aware of Tea Leaves' work, in response to which questions Fritsch pled the Fifth. By the time Krypt3ia posted, it seems likely, Fusion already knew April Lorenzen was involved.

But in the Seago hearing, Fusion lawyer Joshua Levy stated clearly that, "Our client didn't move that specific communication –" pushing Tea Leaves' information (from the context, it's unclear to me whether this was a link directly to a gateway to Tea Leaves i2p site or one that involved Krypt3ia). Elsewhere Levy explained that Mark Hosenball had sent the link to Fusion

which, in turn, sent it out to other journalists.

Fusion's claims are consistent with them knowing of Lorenzen's work before the Krypt3ia post, but having nothing to do with the Krypt3ia post and/or public links directly to Lorenzen's site.

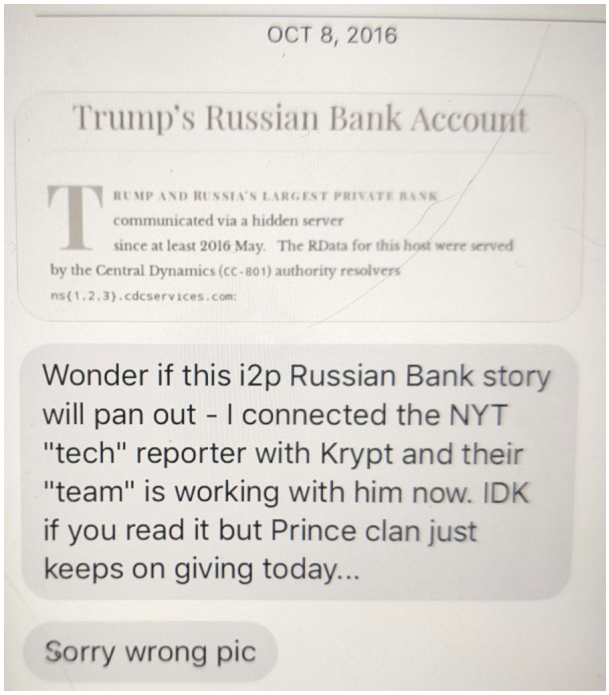
"Phil" hooked Krypt3ia up with the NYT

Alfa Bank seems to doubt Fusion's denials that they were behind all those levels of notice to Krypt3ia.

I have no idea who first alerted Krypt3ia to the WordPress site or the i2p site, and he says he doesn't remember who did. I do know who hooked him up with the NYT.

As I noted when I criticized this story in 2016, I was pitched the Alfa Bank story, like the NYT. But unlike the NYT, I was not pitched it by the people Durham is trying to put in jail like Sussmann, the researchers, or Fusion GPS. I was pitched it by the guy whom I've referred to by the pseudonym "Phil," the person I went to the FBI about in 2017. (This is a pseudonym and he has not been charged by DOJ.)

Not only did he pitch me on it, but he told me he was the one to have hooked Krypt3ia up with the NYT reporter.



The rest of our exchange is below…

The claim that Phil had introduced Krypt3ia to a NYT reporter was credible. At the time I knew of several NYT reporters he claimed to have ties to (at Phil's request, I had introduced him to one of them, and I've confirmed his contacts with others since). He also publicly interacted with Krypt3ia on Twitter.

But I had never checked whether Phil had really introduced the NYT to Krypt3ia until the Alfa Bank filing that blamed that tie on Fusion.

Nicole Perloth has confirmed it was Phil. As she described, Phil basically pushed Krypt3ia on her. "Nicole: Krypt is a person who can be an invaluable resource on this," specifically addressing Krypt3ia's expertise on the dark web, even while asking her to keep him (Phil) updated on when the story would be published.

When I asked Krypt3ia if it was possible that the same person alerted him to the i2p site as had connected him to a NYT journalist, he said he did not remember.

> Do you know if the person who connected you with the NYT reporter was the same was the one who pointed out the mirror? As per your post? Or don't you remember?

> Honestly don't remember. Did not take notes or anything, thought it all bullshit and some kind of game of disinformation.

Whether or not Phil had a role in first tipping Krypt3ia off to the i2p proxy, he had a role in making the NYT aware of a series of moving versions of that site, starting with the one in Russia.

Importantly, this is not the only attempt to broker these allegations that remains publicly unexplained. There's another unexplained package of these allegations — a "mediafire" package first posted on Reddit — raised in the Alfa suit that Fusion disclaimed credit for.

At least one person pushing this story was (as far as I know) completely unrelated to the efforts Durham and Alfa have focused on. Given that April Lorenzen used a pseudonym for her efforts, it would have been easy to hijack those efforts. So until April Lorenzen certifies that all the communications posted under the name "Tea Leaves" out there are hers (including the comment attached to a Tutanota email in Krypt3ia's post), neither should anyone assume she's responsible for all of them.

Alfa Bank believed that the public notice of the Tea Leaves i2p site was proof that Fusion, and only Fusion, was dealing these allegations. The opposite is the case.

To be sure: that might have mattered if Vladimir Putin's invasion hadn't killed the Alfa Bank lawsuit. But Phil's role in the Krypt3ia post doesn't much matter to the Sussmann indictment. Sussmann's alleged lie was on September 19, 2016, 16 days before the communications leading to the Krypt3ia post started. Nothing Phil did on October 8 and thereafter, it seems, could affect that alleged lie.

That said, Durham's sprawling single-count indictment does include allegations about Sussmann's outreach to the press that post-dates

Phil's involvement and may rely on it. Most notably, a paragraph describing that Sussmann emailed Lichtblau on October 10 encouraging him to send an opinion piece criticizing the NYT for its Trump coverage mentions that, "At or around that time, and according to public sources, [Lichtblau] was working on an article concerning the [Alfa Bank] allegations, but [Lichtblau's] editors at [NYT] had not yet authorized publication of the article." [my emphasis] Krypt3ia's comment, "the NYT confirmed that they asked the question and shit happened. They are still looking into it" — a comment that indirectly involved Phil — is one of those public sources.

At the time, Phil was pushing a NYT article more aggressively than what Durham describes Sussmann doing, and he played at least some role in the public sources that reported NYT was working on an article.

So Phil's involvement adds an important detail about how these claims were made public in the weeks leading up to the election, but none of that changes whether or not Sussmann lied to cover up Hillary and/or Rodney Joffe's role in all this.

Update: I've corrected the post to reflect that the original site, hosted in Russia, was a proxy, not a mirror. Thanks to @i2p at geti2p.net for the corrections starting in this exchange.

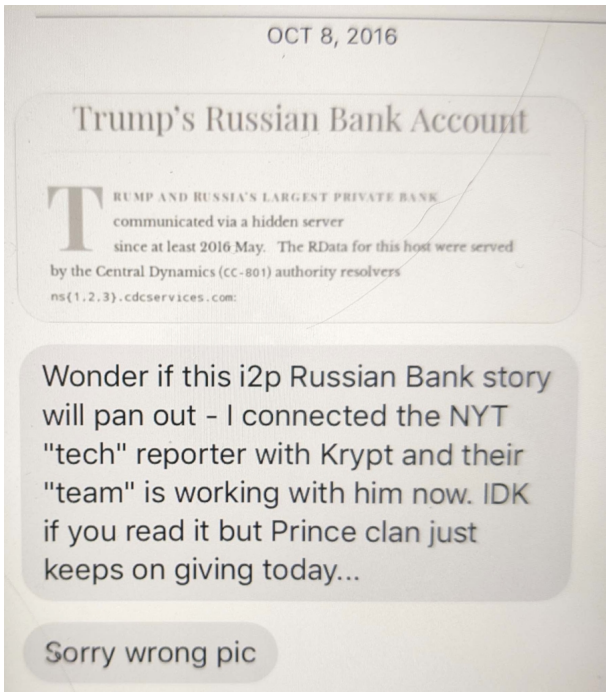
Texts

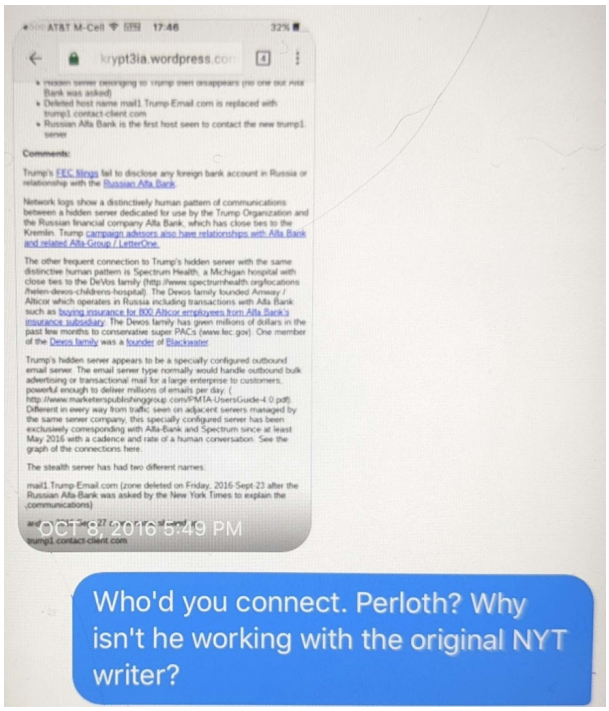
The following includes all the Signal texts included in the exchange regarding the Alfa Bank DNS anomalies.

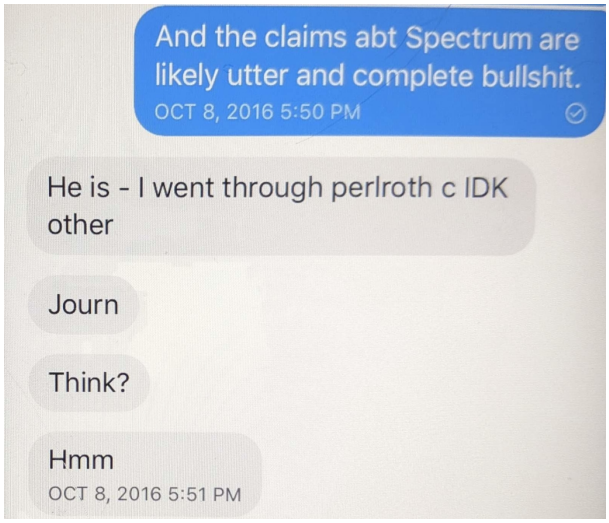
Two comments on these texts: I'm not sure what I meant in the text sent on October 9 at 10:51AM. I suspect I mistyped. I suspect I was trying to explain Betsy and Dick DeVos' traditional role in the Republican party — money — was less urgent to Trump in October 2016 than some kind

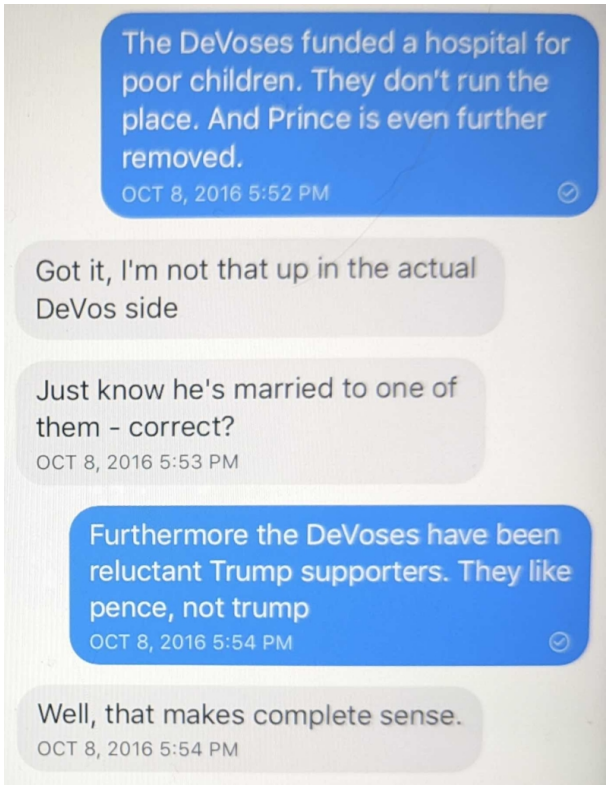
of credible Republican policy platform.

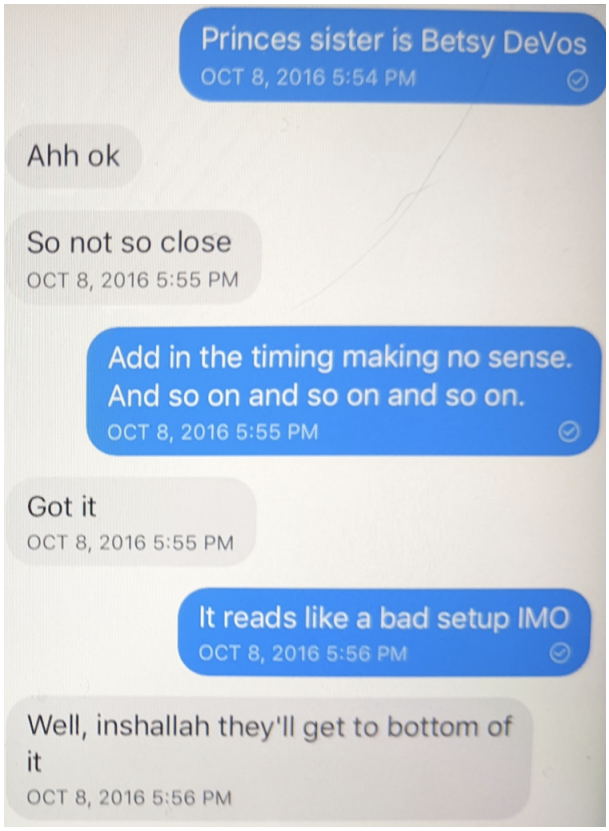
I stand by everything else I said in these texts, though admit my observation about the adversity between UAE and Russia turned out to be hilariously and epically wrong, *particularly* as it pertained to Prince.

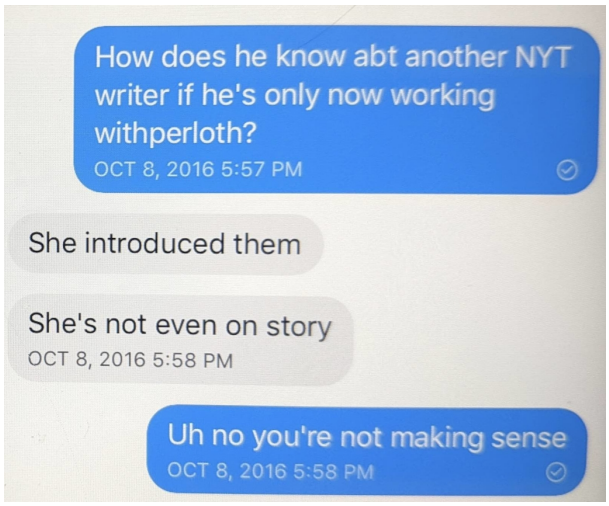


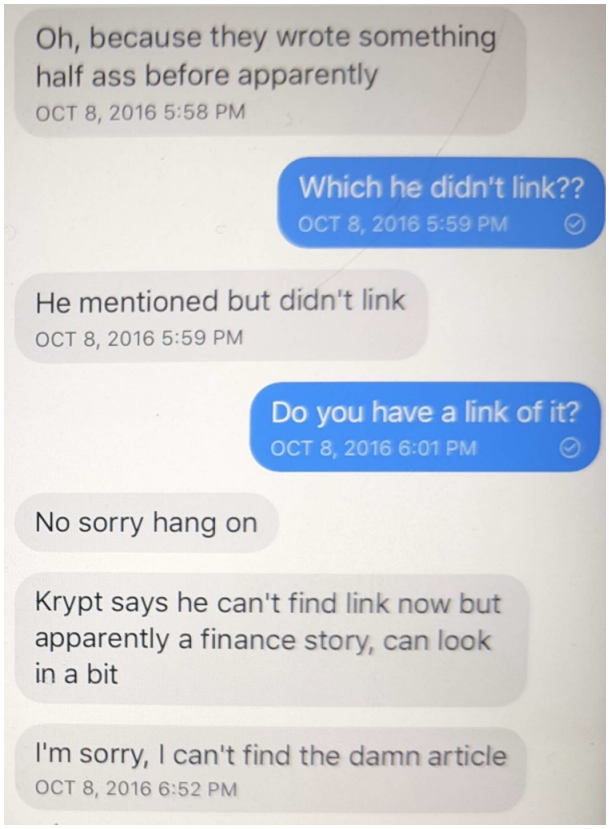


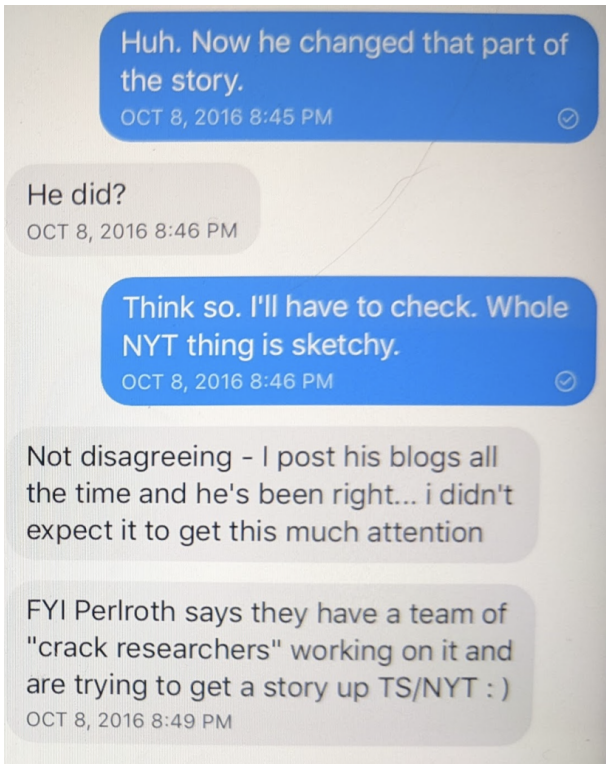

And the claims abt Spectrum are likely utter and complete bullshit.
OCT 8, 2016 5:50 PM
He is - I went through perlroth c IDK other
Journ
Think?
Hmm
OCT 8, 2016 5:51 PM

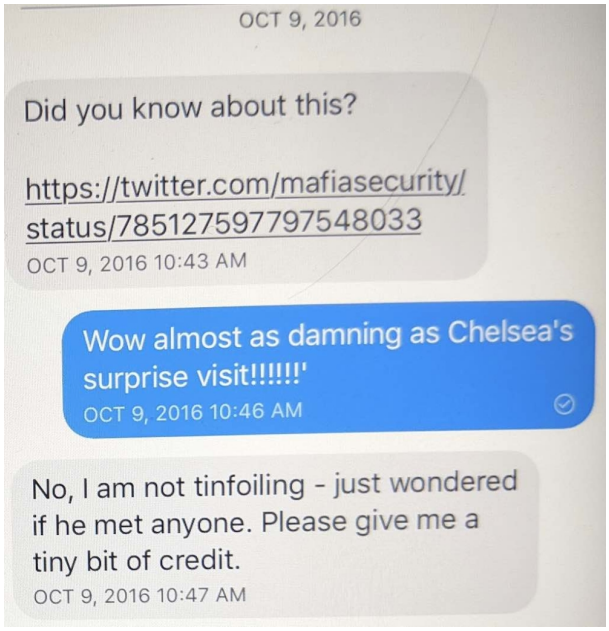

The DeVoses funded a hospital for poor children. They don't run the place. And Prince is even further removed.
OCT 8, 2016 5:52 PM
Got it, I'm not that up in the actual DeVos side
Just know he's married to one of them - correct?
OCT 8, 2016 5:53 PM
Furthermore the DeVoses have been reluctant Trump supporters. They like pence, not trump
OCT 8, 2016 5:54 PM
Well, that makes complete sense.
OCT 8, 2016 5:54 PM

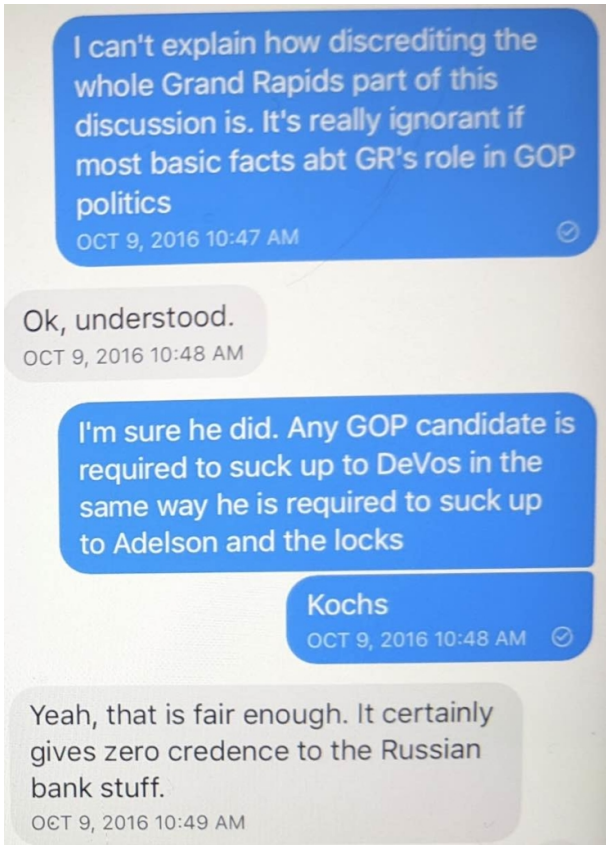

Princes sister is Betsy DeVos
OCT 8, 2016 5:54 PM
Ahh ok
So not so close
OCT 8, 2016 5:55 PM
Add in the timing making no sense. And so on and so on and so on.
OCT 8, 2016 5:55 PM
Got it
OCT 8, 2016 5:55 PM
It reads like a bad setup IMO
OCT 8, 2016 5:56 PM
Well, inshallah they'll get to bottom of it
OCT 8, 2016 5:56 PM

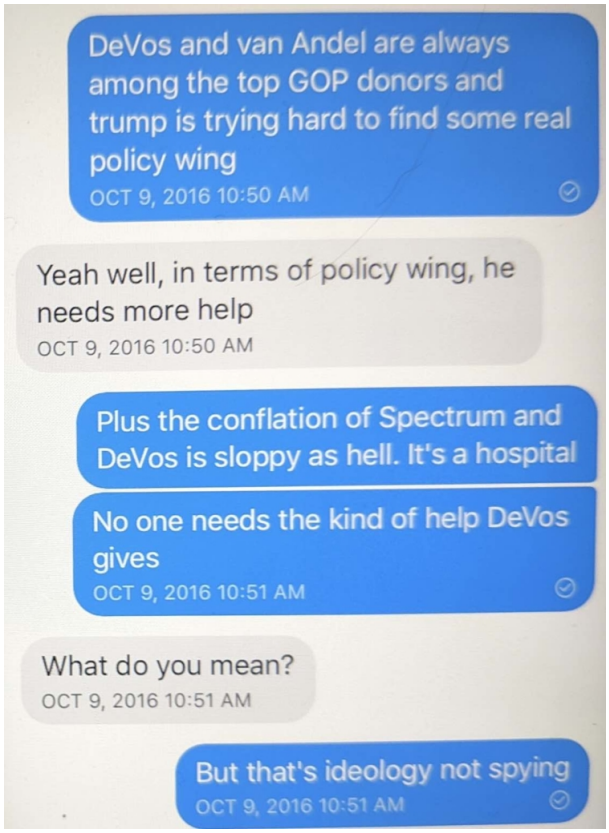

How does he know abt another NYT writer if he's only now working withperloth?
OCT 8, 2016 5:57 PM
She introduced them
She's not even on story
OCT 8, 2016 5:58 PM
Uh no you're not making sense
OCT 8, 2016 5:58 PM

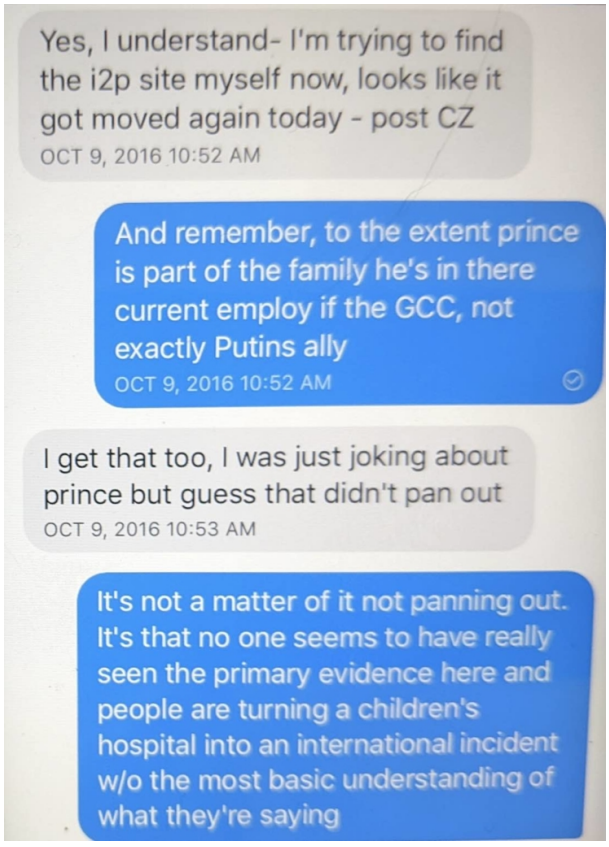

Oh, because they wrote something half ass before apparently
OCT 8, 2016 5:58 PM
Which he didn't link??
OCT 8, 2016 5:59 PM
He mentioned but didn't link
OCT 8, 2016 5:59 PM
Do you have a link of it?
OCT 8, 2016 6:01 PM
No sorry hang on
Krypt says he can't find link now but apparently a finance story, can look in a bit
I'm sorry, I can't find the damn article
OCT 8, 2016 6:52 PM

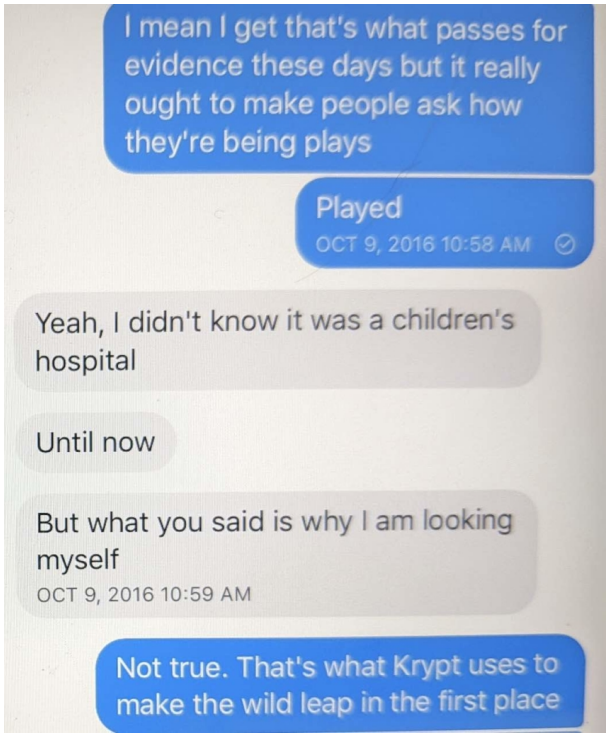

Huh. Now he changed that part of the story.
OCT 8, 2016 8:45 PM
He did?
OCT 8, 2016 8:46 PM
Think so. I'll have to check. Whole NYT thing is sketchy.
OCT 8, 2016 8:46 PM
Not disagreeing - I post his blogs all the time and he's been right... i didn't expect it to get this much attention
FYI Perlroth says they have a team of "crack researchers" working on it and are trying to get a story up TS/NYT :)
OCT 8, 2016 8:49 PM

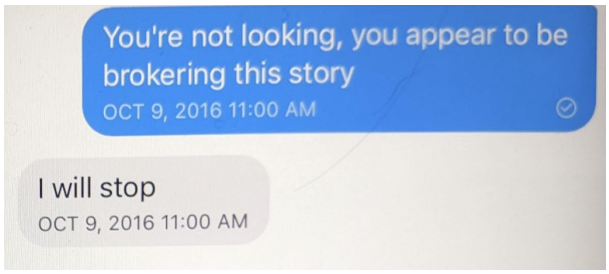

OCT 9, 2016
Did you know about this?
https://twitter.com/mafiasecurity/status/785127597797548033
OCT 9, 2016 10:43 AM
Wow almost as damning as Chelsea's surprise visit!!!!!!'
OCT 9, 2016 10:46 AM
No, I am not tinfoiling - just wondered if he met anyone. Please give me a tiny bit of credit.
OCT 9, 2016 10:47 AM


I can't explain how discrediting the whole Grand Rapids part of this discussion is. It's really ignorant if most basic facts abt GR's role in GOP politics
OCT 9, 2016 10:47 AM
Ok, understood.
OCT 9, 2016 10:48 AM
I'm sure he did. Any GOP candidate is required to suck up to DeVos in the same way he is required to suck up to Adelson and the locks
Kochs
OCT 9, 2016 10:48 AM
Yeah, that is fair enough. It certainly gives zero credence to the Russian bank stuff.
OCT 9, 2016 10:49 AM


DeVos and van Andel are always among the top GOP donors and trump is trying hard to find some real policy wing
OCT 9, 2016 10:50 AM
Yeah well, in terms of policy wing, he needs more help
OCT 9, 2016 10:50 AM
Plus the conflation of Spectrum and DeVos is sloppy as hell. It's a hospital
No one needs the kind of help DeVos gives
OCT 9, 2016 10:51 AM
What do you mean?
OCT 9, 2016 10:51 AM
But that's ideology not spying
OCT 9, 2016 10:51 AM


Yes, I understand- I'm trying to find the i2p site myself now, looks like it got moved again today - post CZ
OCT 9, 2016 10:52 AM
And remember, to the extent prince is part of the family he's in there current employ if the GCC, not exactly Putins ally
OCT 9, 2016 10:52 AM
I get that too, I was just joking about prince but guess that didn't pan out
OCT 9, 2016 10:53 AM
It's not a matter of it not panning out. It's that no one seems to have really seen the primary evidence here and people are turning a children's hospital into an international incident w/o the most basic understanding of what they're saying


I mean I get that's what passes for evidence these days but it really ought to make people ask how they're being plays
Played
OCT 9, 2016 10:58 AM
Yeah, I didn't know it was a children's hospital
Until now
But what you said is why I am looking myself
OCT 9, 2016 10:59 AM
Not true. That's what Krypt uses to make the wild leap in the first place


You're not looking, you appear to be brokering this story
OCT 9, 2016 11:00 AM
I will stop
OCT 9, 2016 11:00 AM