OPSEC CONFUSION ON THE OATH KEEPER CONSPIRACY

I write a lot about the comms the Oath Keepers used to plan insurrection. There was the post about how they figured out, too late, not to plan an insurrection on Facebook; of the five counts of obstruction on the Oath Keeper indictment released Sunday, two pertain to Facebook. Then there was the post where I cataloged how many social media platforms were described in the last iteration of the indictment against them.

- A leadership list on Signal they appear to have obtained from either Watkins and/or Kelly Meggs
- Open channels on Zello, possibly separate ones for each large event
- Telephony chats and texts, including during January 6
- MeWe accounts
- Way too much blabbing on Facebook, followed by a foolish belief they could delete such content
- Parler for further blabbing
- Stripe for payment processing (possibly for dues)
- GoToMeeting for operational planning

The remaining three obstruction charges pertain to this social media activity, one — for Joshua James — specifically describing his attempt to

delete and burn the “[S]ignal comms about the op.”

Add hand-written ProtonMail attachments to the toolchest

It turns out I should have included ProtonMail in that list, because both the addresses to which Laura Steele sent her vetting application to join the Oath Keepers on January 3 were ProtonMail addresses, but the government only laid that out in their unsuccessful bid to keep her detained, in an attempt to use its encryption to ascribe to her that operational security.

> On the evening of January 3, 2021, Defendant Steele emailed a membership application and vetting form to the Oath Keepers of Florida.4 She copied Defendant Young on the email, and wrote: “My brother, Graydon Young told me to submit my application this route to expedite the process.” Under the section for “CPT Skill Sets (Community Preparedness Team) Experience or Interests,” she checked “Security.” Under “Skillsets,” she wrote: “I have 13 years of experience in Law Enforcement in North Carolina. I served as a K-9 Officer and a SWAT team member. I currently work Private Armed Security for [company name redacted]. I am licensed PPS through the North Carolina Private Protective Services.”
>
> Within 10 minutes, Defendant Steele sent another email, this one directly to Defendant Kelly Meggs’s email account at Proton Mail, again copying Defendant Young. She again attached her application and vetting form, and wrote: “My brother, Graydon Young told me to send the application to you so I can be

> verified for the Events this coming Tuesday and Wednesday."
>
> The following day (January 4), Defendant Steele sent the same materials to yet another Oath Keepers email address at Proton Mail. On her email, she copied co-defendants Kelly Meggs and Graydon Young.
>
> 4 The email recipient was actually a Florida Oath Keepers account at "protonmail.com." Proton Mail is housed overseas (in Switzerland) and offers end-to-end encryption. "Even the company hosting your emails has no way of reading them, so you can rest assured that they can't be read by third parties either." Mindaugas Jancis, ProtonMail review: have we found the most secure email provider in 2021?, CyberNews, Mar. 4, 2021, at https://cybernews.com/secure-email-providers/protonmail-review.

But Proton is not going to help if one side of a communication is on Gmail or some other email service on which FBI can serve a subpoena. Which may explain how the government obtained this email from the newly indicted Joseph Hackett in the latest superseding.

> 41. On December 19, 2020, HACKETT sent an email to YOUNG with a subject line "test." The body of the email stated: "I believe we only need to do this when important info is at hand like locations, identities, Ops planning." The email had a photo attached; the photo showed cursive handwriting on a lined notepad that stated: "Secure Comms Test. Good talk tonight guys! Rally Point in Northern Port Charlotte at Grays if transportation is possible. All proton mails. 7 May consider [a rally point] that won't burn anyone. Comms – work in progress. Messages in cursive to

> eliminate digital reads. Plans for recruitment and meetings."
>
> 7 Based on the investigation, "proton mails" appears to refer to the company "ProtonMail," which offers encrypted email services.

I've not seen anything that suggests the government has obtained Proton Mails from the Oath Keepers conducted entirely on the platform; that may have to wait until someone involved decides to cooperate. But I'm not sure how writing the most sensitive messages on what sounds like dead tree paper before sending it adds to the security.

DOJ's selective understanding of encryption

One of the more aggravating pieces of confusion in the new indictment, however, comes not from the alleged conspirators but from the government.

The last item in a list of Manner and Means employed in the conspiracy is the use of "secure and encrypted communications."

> Using secure and encrypted communications applications like Signal3 and Zello4 to develop plans and later communicate during the January 6 operation.

The first overt act describes Stewart Rhodes laying out what I am calling the "Antifa foil" on a GoToMeeting meeting.

> At a GoToMeeting5 held on November 9, 2020, PERSON ONE told those attending the meeting, "We're going to defend the president, the duly elected president, and we call on him to do what needs to

> be done to save our country. Because if you don't guys, you're going to be in a bloody, bloody civil war, and a bloody — you can call it an insurrection or you can call it a war or fight."

As a result, the following footnotes appear on the bottom of the same page.

> 3 Signal is an encrypted messaging service.
>
> 4 Zello is an application that emulates push-to-talk walkie-talkies over cellular telephone networks. Zello can be used on electronic communication devices, like cellular telephones and two-way radios.
>
> 5 GoToMeeting is an online meeting site that allows users to host conference calls and video conferences via the Internet in real time.

Start with Zello: It can be secure. But it wasn't, as used by the Oath Keepers, the day of the insurrection, because it was an open channel. Indeed, the reason we know about it is because journalist Micah Loewinger was following along in real time. Plus, anything saved onto a phone will be accessible once the phone is compromised, just like Signal will. (From the discovery letters shared with the Oath Keepers — the most recent of which is over a month old — the government appears to have initially relied on WNYC's published versions of the Zello chats. But this superseding indictment includes time stamps from Watkins' Zello exchanges, which suggests they've obtained a more reliable copy since then.

Signal, DOJ says, is encrypted. I have no problem with that. But they started compromising the Signal chats as soon as they exploited Jessica Watkins' phone. And the latest indictment seems to rely on the exploitation from another of the more involved participants —

it’s where the new details on the Quick Reaction Force come from (here’s my rough capture of the communications we’ve seen referenced to date).

What I find annoying is that, after treating Signal and Zello as super spooky applications, DOJ then treats GoToMeeting like a normal tool, just “an online meeting site that allows users to host conference calls and video conferences via the Internet in real time.”

But it is also end-to-end encrypted and has a number of other security features that are necessary for its use by mainstream businesses and health care providers. That said, it is centralized and probably responds eagerly to legal process, which is the distinction DOJ really intends by this. That is, it’s not *encryption* that makes the use of these apps a useful marker of a conspiracy, it’s decentralized security, security that the Oath Keepers didn’t use with Zello the day of the insurrection. Plus, for a conspiracy indictment, as opposed to other criminal charges, the use of G2M suggests a bureaucratization that should be more useful to prove the case.

In any case, with this fourth indictment, DOJ added content from G2M that was probably meant to be secure: Stewart Rhodes’ “Antifa foil” comments. An initial production of G2M had been provided to defendants by April 9, with a second attempt on April 23. So it may be that it has taken some time to reconstruct whatever full production they might receive from the various Oath Keeper accounts.

The money is the metadata

That said, it is amusing seeing the conspirators try to add a layer of security to the already secure ProtonMail while they’re laying a trail of travel plans that knots them all up into a network. Here are just some of the fleshed out details from the indictment:

> 79. On January 4, 2021, HARRELSON and DOLAN departed Florida together in a vehicle rented by DOLAN and traveled to the Washington, D.C., metropolitan area.
>
> [snip]
>
> 82. On January 4, 2021, PERSON TEN checked into the Hilton Garden Inn in Vienna, Virginia. The room was reserved and paid for using a credit card in PERSON ONE's name.
>
> [snip]
>
> 85. On January 5, 2021, PERSON ONE and MINUTA separately traveled to the Washington, D.C., metropolitan area and checked into the Hilton Garden Inn in Vienna, Virginia.
>
> [snip]
>
> 90. KELLY MEGGS paid for two rooms, each for two people, at the Comfort Inn Ballston from January 5-6, 2021. The rooms were reserved under the name of PERSON THREE.
>
> 90. KELLY MEGGS paid for two rooms, each for two people, at the Comfort Inn Ballston from January 5-6, 2021. The rooms were reserved under the name of PERSON THREE.
>
> 91. KELLY MEGGS also booked two rooms at the Hilton Garden Inn in Washington, D.C., from January 5-7, 2021. KELLY MEGGS paid for both of the rooms, using two different credit cards.
>
> [snip]
>
> 93. HACKETT paid for a room at the Hilton Garden Inn in Washington, D.C., from January 5-7, 2021. The room was booked in the name of PERSON SIXTEEN.
>
> [snip]
>
> 95. MINUTA, using his personal email

> address and his personal home address, reserved three rooms at the Mayflower Hotel in Washington, D.C., under the names of MINUTA, JAMES, and PERSON TWENTY. A debit card associated with PERSON FIFTEEN was used to pay for the room reserved under MINUTA's name. A credit card associated with JAMES was used to pay for the room reserved under JAMES's name.

Kelly Meggs, by paying for what appears to be the QRF room and another for Person 3 to tend the weapons, would tie the Floridians staying in the DC Hilton Garden with a group coming from at least three states at the Ballston Comfort Inn (and that's before you consider the surveillance footage that shows others dropping off weapons). Minuta, by reserving three rooms at the Mayflower, would tie Joshua James, Person Twenty, and Person Fifteen to the group, including Minuta, staying at the Vienna Hilton Garden, which includes Rhodes and Person Ten. And there's at least one known payment — from some unidentified person to James' wife — that doesn't show up here.

Post 9/11, it's hard to hide hotel travel, especially retroactively, after engaging in a terrorist attack, but it doesn't help that the Oath Keepers didn't compartment their network at all. So all the encrypted messaging and meeting apps in the world could not hide that this was a network that spanned (thus far, but I'm holding out hope they'll roll out the first Mississippi defendants any day!) at least seven states.

Update: I've taken out a reference to the Ohioans walking Isaacs back to a hotel in DC. They did separate early but it was not to take him back. Thanks to Benny Bryant for the correction.