THE CELLEBRITE WARS: MOXIE'S STUNT AND FREDDIE'S PHONE

On April 21, the guy behind the Signal encrypted texting service, Moxie Marlinspike, wrote a post exposing vulnerabilities in the interface of Cellebrite, the cell phone extraction program that FBI relies on.

> Given the number of opportunities present, we found that it's possible to execute arbitrary code on a Cellebrite machine simply by including a specially formatted but otherwise innocuous file in any app on a device that is subsequently plugged into Cellebrite and scanned. There are virtually no limits on the code that can be executed.
>
> For example, by including a specially formatted but otherwise innocuous file in an app on a device that is then scanned by Cellebrite, it's possible to execute code that modifies not just the Cellebrite report being created in that scan, but also all previous and future generated Cellebrite reports from all previously scanned devices and all future scanned devices in any arbitrary way (inserting or removing text, email, photos, contacts, files, or any other data), with no detectable timestamp changes or checksum failures. This could even be done at random, and would seriously call the data integrity of Cellebrite's reports into question.

After telling Cellebrite to fuck off for integrating Signal exploitation into their offerings in about four different ways, Moxie announced that some Signal installs going forward would have such aesthetic sabotage built in in the future.

> In completely unrelated news, upcoming versions of Signal will be periodically fetching files to place in app storage. These files are never used for anything inside Signal and never interact with Signal software or data, but they look nice, and aesthetics are important in software. Files will only be returned for accounts that have been active installs for some time already, and only probabilistically in low percentages based on phone number sharding. We have a few different versions of files that we think are aesthetically pleasing, and will iterate through those slowly over time. There is no other significance to these files.

As a Signal user, I'm thrilled that Moxie is trying to make it harder for FBI to exploit my phone. As someone who'd like FBI to hold the January 6 insurrectionists accountable, this stunt couldn't have happened at a worse time, when the FBI was in the process of trying to exploit the devices of over 500 defendants in a violent assault on democracy.

Which brings us to Freddie Klein, the former Trump State Department official with family ties to Argentine fascists who was arrested for assault in conjunction with the insurrection.

Freddie wants his phone (and dash cam) back. Freddie was arrested on March 3 and his phone — which was plugged into his car charger when he was arrested — was exploited on March 12. Freddie's attorney Stanley Woodward first asked verbally for the phone, and on May 6,

prosecutors said they'd be happy to return Freddie's phone as soon as he stipulated that the exploitation of it happened via reliable methods.

> Thereafter, on May 6, 2021, the government advised that, "we would be happy to release Mr. Klein's phone as evidence in the case provided that Mr. Klein is willing to agree to the attached stipulation. This stipulation was subsequently revised following discussions with the Office of the Federal Public Defender for the District of Columbia, although that office has not approved or, to the undersigned's knowledge, accepted the stipulation as drafted. The stipulation provides, inter alia, that Mr. Klein agree that: "[t]he [digital] Images [of Mr. Klein's phone] are accurate duplicates of the Digital Media and were created using reliable methods" and "[t]he Images of the Digital Media and/or any other copies are 'admissible [into evidence] to the same extent as the original,' within the meaning of Federal Rule of Evidence 1003."

So now Freddie is moving formally to get it back, because his defense team wants the ability to inspect it forensically.

The government, however, maintains that absent that stipulation, they can't return the phone. Not only might they need it to introduce the evidence against Freddie, but it's possible the phone will have evidence implicating some of the other 500+ defendants, and the government wouldn't be able to call Freddie as a witness against them to attest to the accuracy of the Cellebrite report.

The government doesn't describe what evidence it thinks Freddie might have implicating others. But they note that some of the evidence they want to use at trial *against him* includes him

bragging about appearing in a video from the riot via a Signal text.

> After the filter team completed its review, the prosecution team began its review of the non-privileged and search warrant responsive contents of the defendant's phone via the Cellebrite extraction report and has identified relevant material that the United States intends to introduce as evidence at trial. The identified evidence thus far includes location information on January 6, 2021, as well as messages exchanged by the defendant via the Signal application ("app") regarding his presence at the U.S. Capitol.

The government then goes on to explain that some of the evidence they want to use is not available via other means (say, by serving a warrant on Facebook). They're talking about Signal, of course.

> It is also important to note that some of the evidence that has been discovered in the defendant's phone is not available to the government through other means. For example, the United States has identified text messages sent by the defendant through the Signal app, in which Klein identifies himself in a video at the Capitol. Notably, Signal is a "state-of-the-art end-to-end encryption" app that "keeps your conversations secure." See Why Use Signal, https://signal.org/en/ (last visited Jul 26, 2021). Signal advertises that even they cannot read messages or listen to calls, "and no one else can either." Id. As Signal itself says, "Signal doesn't have access to your messages; your chat list; your groups; your contacts; your stickers; your profile name or avatar; or even the GIFs you search for." See https://signal.org/bigbrother/centralcal

> ifornia-grand-jury/ (last visited Jul 26, 2021). Indeed, Signal has specifically asserted that "the broad set of personal information that is typically easy to retrieve in other apps simply doesn't exist on Signal's servers." Id. This includes address of the users, their correspondence, and the name associated with each account. Id. Indeed, according to Signal, the only information that it maintains is the timestamps for when each account was created and the date that each account last connected to the Signal service. Id. Thus, the messages sent by the defendant via the Signal app are *only* available to the government through the defendant's phone and the Cellebrite extraction of that phone.

To be clear: the government is generally making defendants stipulate to the accuracy of forensic reports before returning any devices (though I wonder if they have done so with Stewart Rhodes, who reportedly shared his phone and already got it back). For example, the government refused to return Vitali Gossjankowski's laptop, which has special software tied to his hearing impairment on it, without such a stipulation. So it's not *just* Freddie's use of Signal that has led them to refuse to return the phone.

Moreover, the concern about introducing evidence against others is real. A number of prosecutors' recent investigative moves (both specific arrests and the way they're wiring some plea deals to others) are best explained by the difficulty posed by a crime in which hundreds of the criminals, many of them misdemeanor defendants, have important evidence against others.

But this is the use case for which Moxie's stunt presented the real concern: someone whose phone has evidence needed to rebut his claims that the videos showing him violently attacking the Capitol aren't really him. And that's before any

special protections DOJ started taking after Moxie promised future sabotage in a tiny percentage of Signal installs.