Signal Guidelines

We recommend Signal as the standard for secure, end to end encrypted messaging. We've seen a demonstrated commitment to minimizing the amount of data they are in any way able to access. A 2016 subpoena response included the only information that Signal had stored – the date of account creation and of last access, viewable here: 2016-10-04-eastern-virginia-subpoena-response While there are occasional panicky news articles about "Signal being compromised" in every instance that we have seen, the compromise has been of a user's device and not of Signal encryption. From Cellebrite reports on J20 defendant devices, we have seen that even if a phone is unencrypted, the Signal localized encrypted storage on Androids effectively protects data when enabled. That said, here are some things to be aware of in your use of Signal.

- For anyone using or about to use Signal, we strongly recommend reading through Texting Tips for the Brave to get an initial understanding of what good Signal behavior and security practice looks like. Understand the rules of different ways and times that you're using this tool and keep yourself and those around you safe.
- The desktop client is less vetted and there are concerns about how different operating systems, in particular Windows and iOS handle the notifications and store information. When a number has been deregistered, Signal desktop still attempts to sink with cached notifications, so be sure and remove your Signal desktop and disconnect from your number before deregistering.
- One current issue – group names are searchable, which is great! But those group names still show up when they have been left and deleted, so employ caution in how you name your groups and understand that if you have a group called "do these crimes" that name is something that could be accessed later and used against you.
- Turn on a passcode lock to Signal! Set a timeout period that makes sense so that if you haven't used it in a while, it will be harder to get into.
- Good practices:
  - Use the contact verification! It's there for a reason and most of us don't use it nearly enough.
  - Remove yourself from old threads, then delete them.
  - On active threads with disappearing messages, it is a good practice to periodically delete the non-disappearing elements like who was added/left the group and any sent messages lingering past the window.
  - Be cautious and get consent before adding someone to a group. Institute vouching procedures and waiting periods for new people on sensitive threads. Make sure you understand the vouch security level – "hard vouches" vs. "soft vouches" and everything in between.
  - Groups cannot have people removed, people can only leave them. If you're deregistering your number, remove yourself from all groups first.
- Right now, deregistered numbers can be added to groups, so be sure the person you're adding is on Signal still and block old numbers within the app when someone changes their number
- Answers to some question we've seen about Signal:
  - Disappearing message times start from when the message is opened/read. If your "disappearing in five minutes" message isn't opened for a week, it won't disappear until a week and five minutes.