Sara Brown
LFI – week 17
10/14/18

Protecting Your Privacy With Messaging Apps

Did you know that your texts might not be private?
Depending on what app you use to text, your messages or metadata (information about your messages, like the phone numbers of the people you text) might be easily seen by people other than the recipient. This can include service providers, people with access to your phone (like a spouse or parent), malicious individuals, or governments.

What should I consider?
There is no one best messaging app – what's best for you will depend on your circumstances. Some questions to ask yourself are:

- Why do I want a secure messenger?
- What features are important to me?
- Is there someone specific who I want to keep from seeing your messages? Who or what is that (government, parents, significant other, service providers etc.)?
- What messaging apps do my friends and contacts use?
- Do I want to avoid giving our my phone number to people with whom I would like to exchange messages?
- Does the messaging app have access to my photos, camera, contact list, or other information/tools on my device?
- Are my messages encrypted? (Encryption is a way to hide the contents of messages from unauthorized eyes. It uses mathematical formulas to make messages unreadable to anyone who doesn't have the "keys" to unlock them.)

Ready to make your texting more secure?
You can use the table on the back of this sheet to compare some of the most popular messaging apps.

App/Service	Encrypted?	Other info
Facebook Messenger	In transit only. Facebook can read your messages.	-Links your mobile device to your Facebook account and phone number -Recipients have your Facebook name instead of your phone number (*note*: check your privacy settings within Facebook to make sure your phone number isn't publicly visible)
Google Hangouts	In transit only. Google can read your messages.	-Links your mobile device to your Google account -Recipients have your Google username instead of your phone number
iMessage	Yes – if recipient also has iMessage	-Gives Apple access to phone number and contact list -If backed up to iCloud, at risk for hacking
Signal	Yes – end-to-end	-Gives Open Whisper Systems access to phone number and contacts -Can only use if recipient also has Signal on their device
SMS/text message	No	-Other info varies widely depending on device, carrier, and more
Snapchat	No	-Gives Snapchat access to phone number and contacts -Messages and photos "expire" (disappear from your and the recipient's device) after a set amount of time -Can only use if recipient also has Snapchat on their device
Whatsapp	Yes – end-to-end	-Owned by Facebook, so gives Facebook access to phone number and contacts -Can only use if recipient also has Whatsapp on their device

NOTE: This comparison is not comprehensive because there is more information, and there are more messaging apps, than can be captured in a single table. Also, apps are updated frequently, so you should always research the latest version before deciding what is right for you. **Consider this a starting point.**

For more information/sources for this handout:

Secure Messaging? More Like a Secure Mess (Electronic Frontier Foundation) - https://www.eff.org/deeplinks/2018/03/secure-messaging-more-secure-mess
Surveillance Self-Defense: Communicating With Others (Electronic Frontier Foundation) - https://ssd.eff.org/en/module/communicating-others
Choosing Tool: Chat Apps (My And My Shadow): https://myshadow.org/ckeditor_assets/attachments/171/choosingtools_chatapps.pdf