Ethics and Privacy in user research

You won’t believe what happens next!

18F

Based on https://handbook.18f.gov/research-guidelines/#managing-personally-identifiable-information-pii

PII, or personally identifiable information, is any data (or combination of data) that can identify an individual.

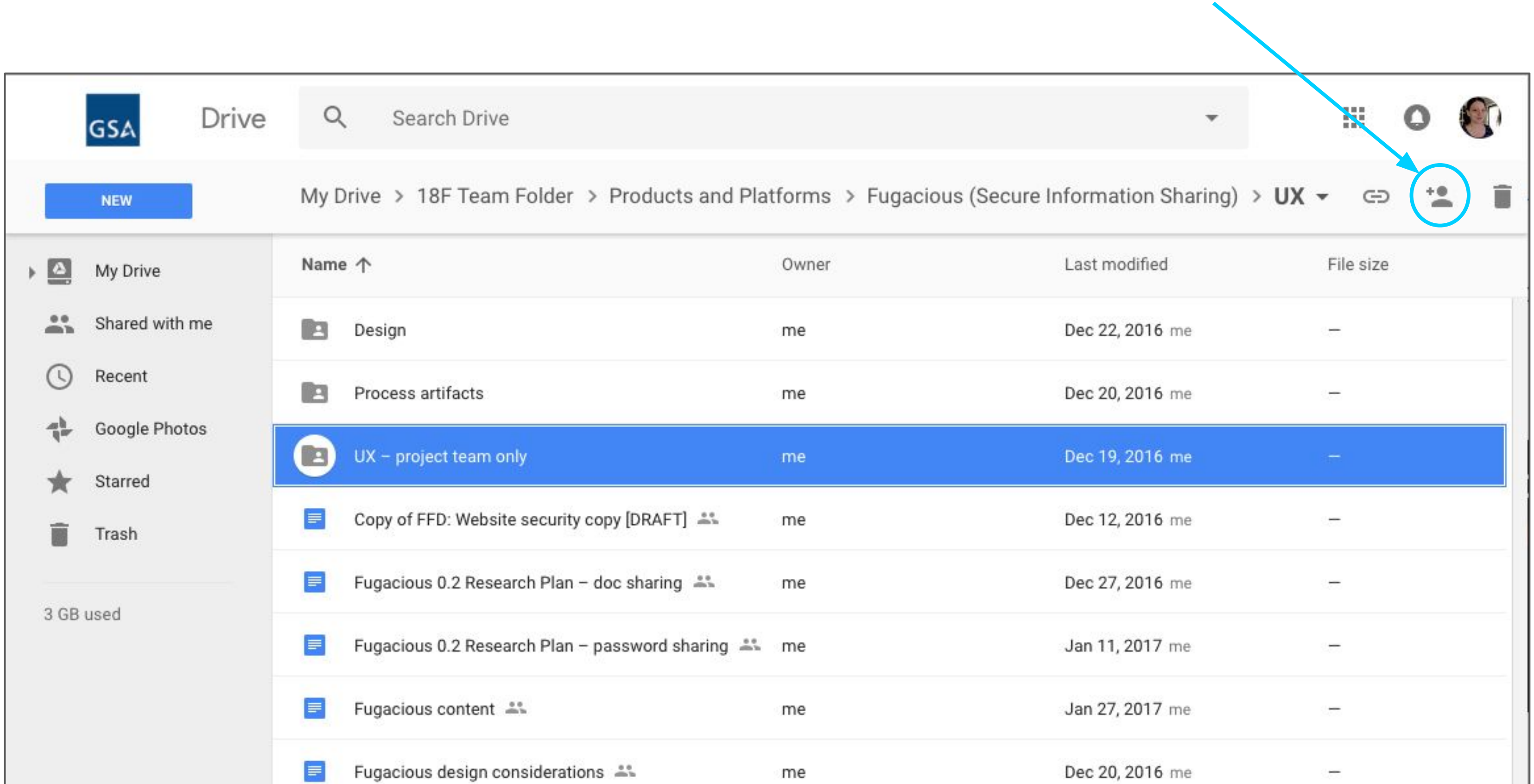
PII can be name, name+agency, email, home address, voice recording, or a photo of a person’s face.

It kind of depends.

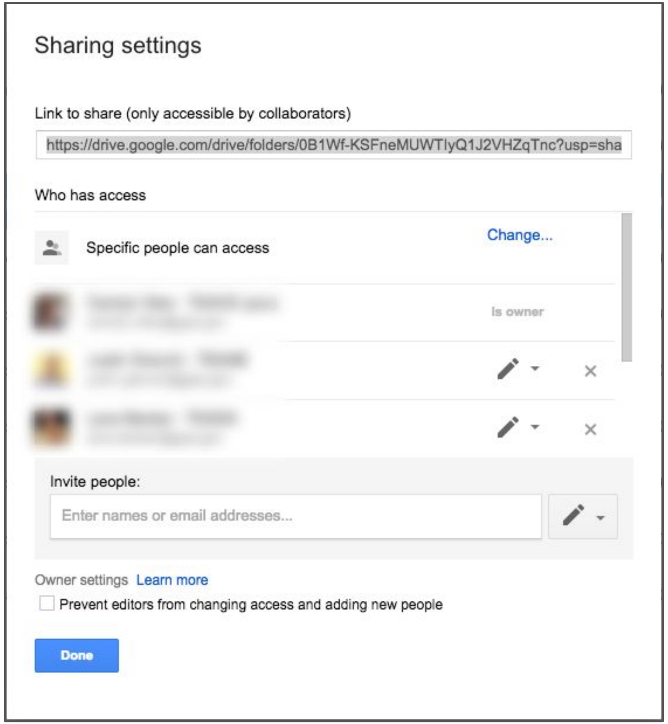
Doing user interviews means handling PII. Here's how to be smart about it.

Tip 1:
Find an approved place to store PII. At the GSA, we store PII in Google Drive. Be sure to edit the privacy settings so only the core research team has access.

Lock down any folders containing raw interview notes or PII.



This means fussing with Google Drive’s sharing settings a bit.



Be sure to **REMOVE** sharing permissions to GSA, 18F, PIF, and anyone else not on the core project team, which tend to be added by default if your file is in the 18F project folder.

Tip 2:
Create an interview roster with research participants contact info (if you need it) and assign each person a code.

It’ll look something like this.

Code	Name	Role	Contact method	Most recent contact
A01	Andrey Bolkonsky	Patriarch of the Bolkonsky family	@andreyB on Slack	
A02	Marya Bolkonsky	Daughter	marya.bolkonsky@warandpeace.gov	emailed on 3/22/2017
A03	Pierre Bezuhov	protagonist	@pibuz	
A04	Ilya Rostov	Patriarch of the Rostov family	ilya.rostov@warandpeace.gov	

Note: the names above are characters from Tolstoy’s *War and Peace.* You didn’t think I’d reveal real PII in a presentation about protecting PII, did you?

Keep this roster and signed consent forms in a *separate* place from the raw interview notes, and destroy the roster after the project is over.

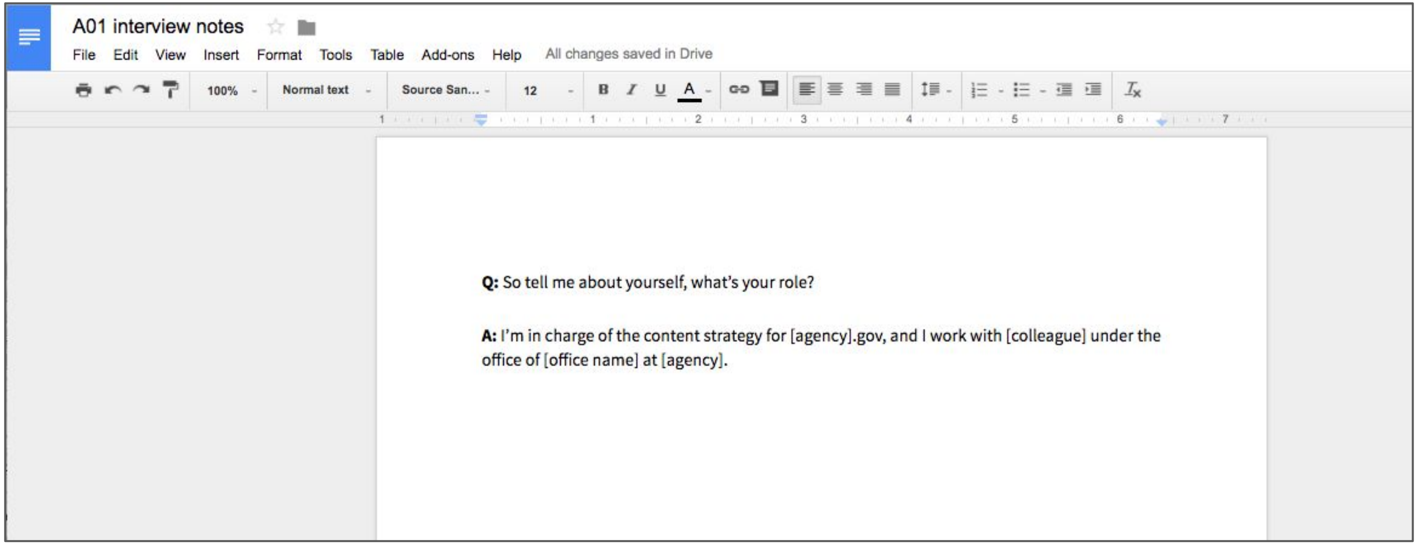
Identify your interview notes with the code from the roster, *not* the person’s name.

PARTICIPANT CODE
(although you can also
omit this)

You can also identify notes with the time and date of the interview.

Tip 3:
Don’t write out a person’s name, agency, projects, or other PII when you’re taking notes. If you happen to record PII during the session, be sure to sanitize the notes afterward.

That way even if someone finds the notes, they’re less likely to be able to tie it back to the participant.



Tip 4:
Ensure all participants understand how their information is stored and shared.

Tip 5:

Ensure all participants understand who is in the room and how we'll use the information we collect.

In an informed consent form we explain how we use a person’s information and what steps we take to protect it.

This acts kind of like an agreement between you and the research participant, so be sure you know what you’re promising and then hold up your end of the bargain.

Tip 7:
Don’t write participants’ names or other PII in Slack, Trello, or any other system not approved for handling PII. 🙊

Tip 8:

Give participants an opportunity to ask questions before starting. Make sure they understand what we’re doing and feel comfortable starting the session.

Those are the basics!

Have a question that’s not answered here?
Head on over to #research and we’ll totally geek out with you.

18F