Secure Messaging? More Like Secure Mess

Gennie Gebhart
Associate Director of Research

Erica Portnoy
Staff Technologist

People come to secure messaging for different reasons.

And developers have to balance conflicting priorities.

Security
Usability
Accessibility
Growth


LINE

There is **no single secure messenger** to rule them all.

Outline

- User personas
- Mapping features onto concerns
- Policy choices
- Questions to leave with

Outline

- **User personas**
- Mapping features onto concerns
- Policy choices
- Questions to leave with

Journalist

Motivation: protect sources; avoid getting scooped

Technical proficiency: has institutional resources available for support

Bandwidth: doesn't have time to manage their own IT

Priorities: physical compromise, cannot risk "misfires"

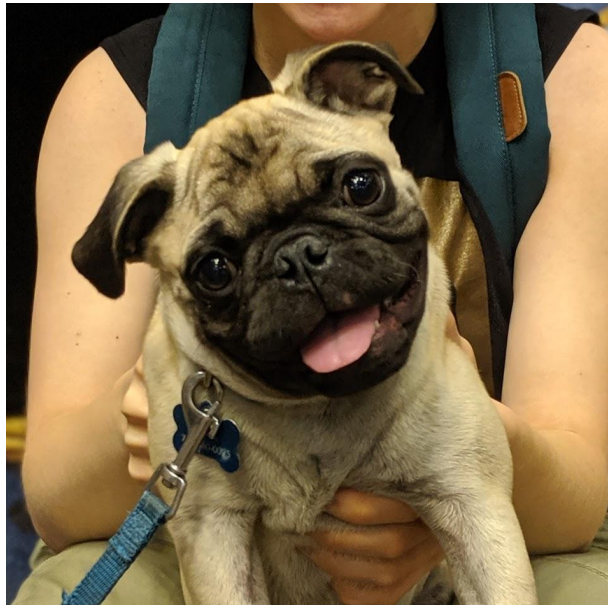
Therapy Client

Motivation: communicate with therapist; worried about rumors of WhatsApp contacts showing up in Facebook friend recommendations

Technical proficiency: average

Bandwidth: can take a little time to set things up, but doesn't have time for repeated tasks

Priority: phone number privacy



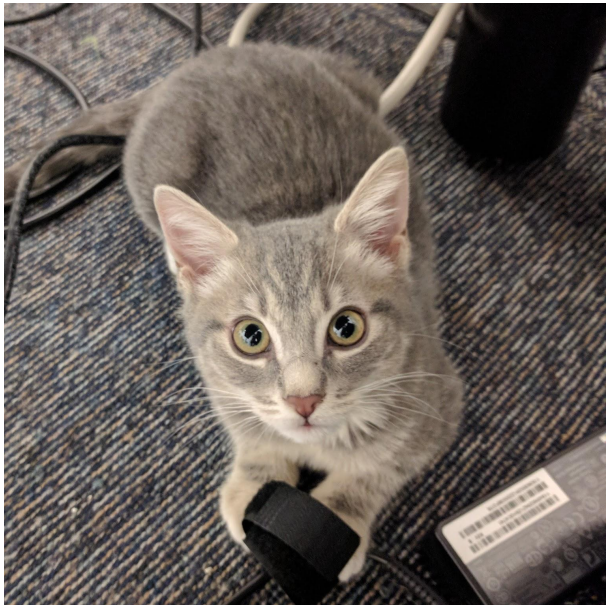
Open source maintainer

Motivation: wants to attend hacker conferences professionally; wants to be protect phone number

Technical proficiency: professional

Bandwidth: can spend some time and effort setting things up

Priorities: physical compromise, phone number privacy



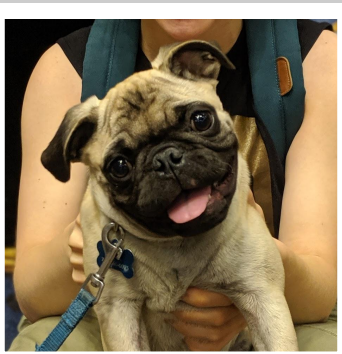

user testing

Outline

- User personas
- **Mapping features onto concerns**
- Policy choices
- Questions to leave with

Physical compromise

Journalist



Therapy Client

Open Source Maintainer

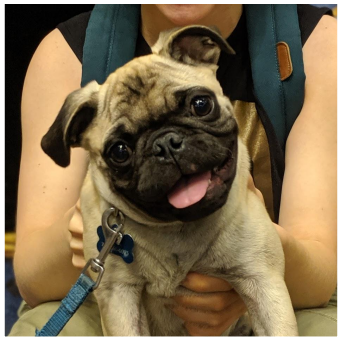
EFF

Physical compromise

↓

Message ephemerality

Journalist



Therapy Client

Open Source Maintainer

Phone number privacy

Journalist

Therapy Client

Open Source Maintainer

EFF

Phone number privacy

↓

Aliases or usernames

Journalist

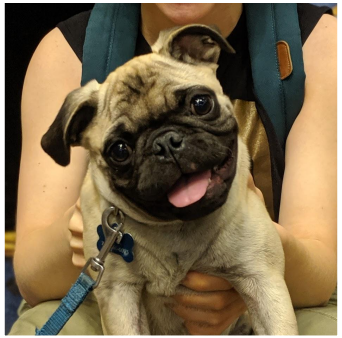
Therapy Client

Open Source Maintainer

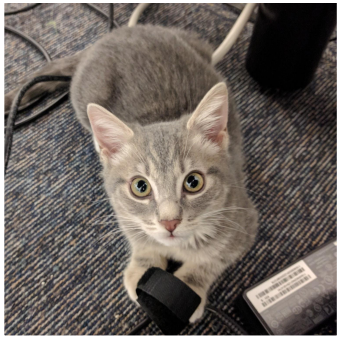
EFF

Cannot risk “misfires”

Journalist



Therapy Client



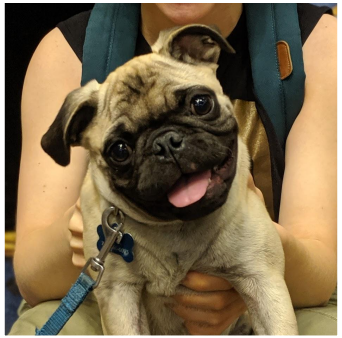
Open Source Maintainer

Cannot risk “misfires”

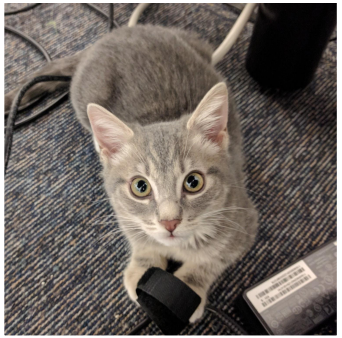
↓

Key verification and single-mode

Journalist



Therapy Client



Open Source Maintainer

Outline

- User personas
- Mapping features onto concerns
- **Policy choices**
- Questions to leave with

Crypto is the **easy part**.

secure messaging (n): no one but you and your intended recipients can read your messages or otherwise analyze their contents to infer what you are talking about

secure messaging (n): no one but you and your intended recipients can read your messages or otherwise analyze their contents to infer what you are talking about

secure messaging (n): no one but you and your intended recipients can read your messages o otherwise analyze their conte hat you are talking abo

law enforcement “ghosts”

secure messaging (n): no one but you and your intended recipients can read your messages or otherwise analyze their contents to infer what you are talking about

secure messaging (n): no one but you and your intended recipients can read your messages or otherwise analyze their contents to infer what you are

unencrypted backups

secure messaging (n): no one but you and your intended recipients can read your messages or otherwise analyze their contents to infer what you are talking about

client-side scanning

sec *g* (n): no one but you ended recipients can read your messages or otherwise analyze their contents to infer what you are talking about

Outline

- User personas
- Mapping features onto concerns
- Policy choices
- **Questions to leave with**

Don’t ask, “What new secure messenger should I build from scratch?”

Instead, ask, “**How can I help improve the ones that already exist?**”

Don’t ask, “What is the perfect combination of features?”

Instead, ask, “**What is the right combination for particular use cases?**”

Don’t just ask, “Who is this tool meant for?”

Also ask, “Who uses it, and **how do those imagined and real groups overlap?**”

Thank you

Erica Portnoy
erica@eff.org
@ohemorange

Gennie Gebhart
gennie@eff.org
@jenuhhveev

EFF

- User personas
- Mapping features onto concerns
  - Message ephemerality
  - Phone number privacy
  - Key verification and single-mode
- Policy choices
  - Law enforcement “ghost”
  - Unencrypted backups
  - Client-side scanning
- Questions to leave with