Interview checklist

January 9, 2018

Part 1: Beginning

1. Introduce ourselves and our institution, thank the interviewee for their time.
2. Explain what our project is about and how interviewee's participation helps.
3. Mention that it will take 30-60 minutes and that we can stop any time.
4. Present consent form and explain confidentiality and anonymity.
5. Ask for signature and for permission to record.
6. Ask if interviewee has any questions before we begin.
7. Start recording if interviewee gave permission.

Part 2: Introductory questions

- Ask some warm-up questions.
- Get demographic information.
    - Gender
    - Age range (18-25, 26-35, 36-45, 46-55, 56-65, >65)
    - Occupation
    - Country of residence
    - Level of education (no degree, high school degree, BSc/BA/..., MSc/MA/PhD/...)
- How much time do you spend on the Internet each day?
- How many devices do you use to go online?
- What would you define as "sensitive" information in your daily online activity?
- Who do you think tracks you when you're online?
- Why do you think these entities track you?

Part 3: The Tor network

- Tell me more about how you first found out about Tor.
- Do you remember why you started using Tor?
- Tell me more about the first few times you used Tor
    - What did you notice about the browser?
    - How well did it allow you to accomplish your tasks?
- How often do you use Tor?
- What do you think Tor does for you when you browse the Internet?
    - What do you think the advantages of using Tor are?
    - What do you think the disadvantages of using Tor are?

    - Who or what are you trying to protect yourself against when using Tor?
    - What do you think the limits of using Tor are?
- What kinds of communications do you use Tor for?
- Would you consider any of these communications “sensitive”?
- Tell me about any communications you would not wish to conduct over Tor?
    - Why is this the case?
- What features would you expect from an anonymous browser such as Tor?
- Do you feel safer when browsing over Tor as opposed to when you are not using it?
- Do you think anyone can unmask your identity when you use Tor?
    - Why/why not?
    - What about The Tor Project?
    - What about law enforcement?
    - What about your Internet Service Provider?
    - What about the website you’re visiting? Can they identify you?
- Assume you use Tor to go to bbc.com. What information about you do you think is protected by Tor? What information about you do you think is **not** protected by Tor?
- Could you draw a diagram for us that illustrates how you think Tor works?
    - [*Suggest that there are actors who interact (cf. email) but don’t prime them with a diagram. Encourage them to vocalize thought processes.*]

Part 4: Onion services

- Do you know what an onion service is?
- Tell us in your own words what an onion service means to you.
- Could you draw a diagram for us that illustrates how you think onion services work?
- Have you used onion services in the last three months?
- Why do you use onion services?
- Tell me more about any issues you have had while browsing onion services.
    - Why have you had these issues?
- How do you keep track of onion services?
- How do you learn about new onion services?
- How do you usually go to onion services? Over bookmarks/links/Google/…?
- The domain format of onion services is unusual.
    - Have you had any issues related to the onion services domain format?
    - Can you tell me more about these issues?
    - Why did they arise?
    - How do you manage these issues?
- Tell me more about how you verify the authenticity/legitimacy of onion services.
    - How do you know that you are going to the right website?
    - How do you know the website you are on is the one you wanted to get to?
- Assume you go to the onion site of bbc.com. What information about you do you think is protected by Tor? What information about you do you think is **not** protected by Tor?

- Do you feel safer when going to an onion site than when going to the corresponding web site?
- Phishing attacks often involve an attacker registering domains that look similar to the victim domains. Do you have any thoughts on how phishing would work for onion services?
- Some onion services use “vanity” domains. How do you think that changes how you handle these domains?
    - [*Show them facebookcorewwwi.onion and protonirockerxow.onion.*]
    - Would it make it easier to memorize the domains?
    - Would it make it easier to recognize the domains?
- How do you feel about the current availability of onion services?
    - Are there websites you would like an onion service version of?
    - Why?
    - What if Amazon/Twitter/etc. started running corresponding onion sites?
- Are you operating any websites? If yes, would you consider setting up a corresponding onion site?
- How would you improve onion services?

Part 5: Maintaining privacy and anonymity online

- How would you improve Tor Browser to improve the browsing experience?
- Tell me more about any specific anonymity/privacy needs you have that are not currently being met when you’re online.
    - Why?
- What kinds of tools would help to address these needs?

Part 6: Conclusion

1. Thank interviewee.
2. Hand over business card so interviewee can get in touch with us.
3. Ask if interviewee can recommend anyone else for an interview. If so, ask them to forward the link to our volunteer page.
4. Explain what we are going to do with the data.
5. Ask if interviewee has any final questions or any feedback on our study.
6. Give them gift card and Tor stickers.