There's No Anonymity
Review Questions
Answer Key

1. What are cookies? Specifically:
    a. Explain in one sentence what a cookie is.

    Target answer: A small text file websites can store on your computer and read later.

    b. Give at least *two* examples of what various types of cookies are used for.

    Examples might include:

    Keeping you logged in to a website.

    Remembering your shopping cart.

    Tracking your visits across different websites.

    Saving your progress in browser-based games.

2. Do you have to visit a website for it to create or use a cookie on your computer? Explain your answer.

    Answers should demonstrate understanding that advertising and social networks can also use their own cookies through other websites that embed their content. For example, the Facebook "like" button on other websites reads and writes Facebook cookies.

3. What do "private browsing" or "incognito" modes in web browsers do? Specifically:
    a. Name at least one thing "private browsing" or "incognito" modes do to protect your privacy.

    Answers might include:

    Clears any new cookies left by websites during your browsing session, when you close the browser window.

    Prevents your browsing history from being saved on your computer after you close the browser window.

    Prevents your passwords and login information from being saved after you close the browser window.

b. Who do these modes protect your information from?

Answers might include:

They protect you from other people who might snoop through your computer in person.

They protect you from websites trying to use cookies to track your activity between different browsing sessions.

4. Name *two* types of information that can *still* be collected by websites when you're using "private browsing" or "incognito" mode.

   Examples might include: IP address, browser and operating system type, browser configuration, cookie data from the current session, your login credentials and profiles for that website, information saved by browser extensions.

5. What is the relationship between the amount of information available about you online and your ability to use the Internet without being recognized? Explain briefly.

   Answers should demonstrate understanding that more information about you being available makes it likelier that you can be correctly and uniquely identified on the Internet. There aren't many people who completely share your combination of interests, opinions, friends, habits, devices, location, etc.

6. Name *two* types of people, businesses, or institutions who might compromise your online anonymity, and explain how each could compromise it.

   Example answers might include:

   Friends and family, for example by sharing tagged pictures of you, which means you may be added to a facial recognition database; or by making posts (on their pages or yours) with identifying information like names and birthdays -- revealing your real name might break a pseudonym, and revealing a birthday allows data aggregators to confirm you're THAT Jesse Smith.

   Data aggregators, by compiling information about you to make a detailed profile; the more detailed the profile is, the more uniquely it picks you out.

   Schools, churches, or other organizations you are involved with, by collecting, saving, sharing, and/or selling and storing personal information that can be added to data aggregators' and marketers' profiles.

7. Sasha checks into Cognito Cafe on Foursquare as user "shu44" and posts a photo-supported review of Cognito Cafe as Yelp user "ahsas" an hour later.

    a. Name *two* methods someone (or some computer) could use to figure out that the two posts were by the same person.

    b. For each method you named in part (a), name one precaution Sasha could use to make themself less likely to be identified in that way.

    Example answers might include:

    Matching the IP address or unique device identifier for her phone; could be avoided using a proxy.

    Guessing based on timestamp and geotags; could be avoided by removing geotags from photos and delaying posting.

    Language modeling; hard to avoid except by leaving no other clues that would lead anyone to bother checking.

    Matching information in the two user profiles; could be avoided by giving minimal or false profile information.

    Using a tracking cookie associated with an ad shown on both websites; could be avoided by setting their browser to refuse third-party cookies.

    c. For each method you named in part (a), would a regular person (not a hacker) be able to use those to figure out Sasha wrote the two posts? Explain your answers.

    Example answers might include:

    Users generally aren't able to see each other's IP addresses on a website.

    Timestamps for posts are usually visible to everyone on a website, so users can try to correlate those in order to build evidence linking the two accounts to Sasha.

    Geotags may or may not be available to regular users, as websites might strip out that data.

    Language modeling is possible, as the post text is visible to everyone.

    If there's enough information in Sasha's two user profiles, other people can try to link them by seeing if those aliases occur together elsewhere on the Internet.

    Tracking cookie data is only available to the website/service, so regular users can't use those to link Sasha's accounts.

8. *Not including* private-browsing modes and the methods you named in your answer to (5)...

    a. Name one thing you can do, or a tool you can implement, to make it less likely that someone could associate your online activities with you.

    b. Explain in one to two sentences how the tool or method works.

    c. Name one limitation or weakness of the tool or method.

    Examples might include:

    (a) Ask your family and friends not to post about you or tag you in pictures or posts. (b) Reduces the amount of information about you that can be added to data profiles or used to identify your own posts/communications. (c) There is no way to ensure compliance, and it could potentially be socially off-putting.

    (a) Limit the information you share with apps/websites/services. (b) Reduces the amount of detailed data that can be compiled by data aggregators. (c) Sometimes the information is necessary for the service to function properly (and sometimes falsifying can be illegal or at least against terms of service), and apps/websites/services may still collect information about you in the background in not-so-obvious ways.

    (a) Use privacy settings for your social-media accounts to limit how many people can see your posts. (b) Reduces the amount of identifying information people might be able to see about you and use to link your accounts together. (c) People can repost/reshare information, and the companies that own the sites can still sell it to aggregators.

    (a) Use anti-tracking plugins. (b) Disallow cookies and/or loading of content from third parties (not the actual website you're visiting) if they match a database of marketers that are known to track people/match a database of third parties that have been tracking you. (c) Not everything is in the database, and the plugins may accidentally block cookies or content that are necessary to functionality or that you actually wanted to see.

    (a) Use anonymization proxies, VPNs, etc. (b) Route your Internet traffic through an intermediary so it looks like your communications are coming from a different IP address. (c) Other identifiers like browsing history may leak through, and in most cases (except Tor), the service still knows your actual IP address.