**Future Work**

Due to limited time constraints there were some privacy enhancing functionality that we were not able to schedule. As we learned about different privacy concepts in our EPS class along with other privacy classes we discussed which concepts we would like to incorporate if we had the time and resources. Of those concepts was a privacy notice.

**Privacy Notice**

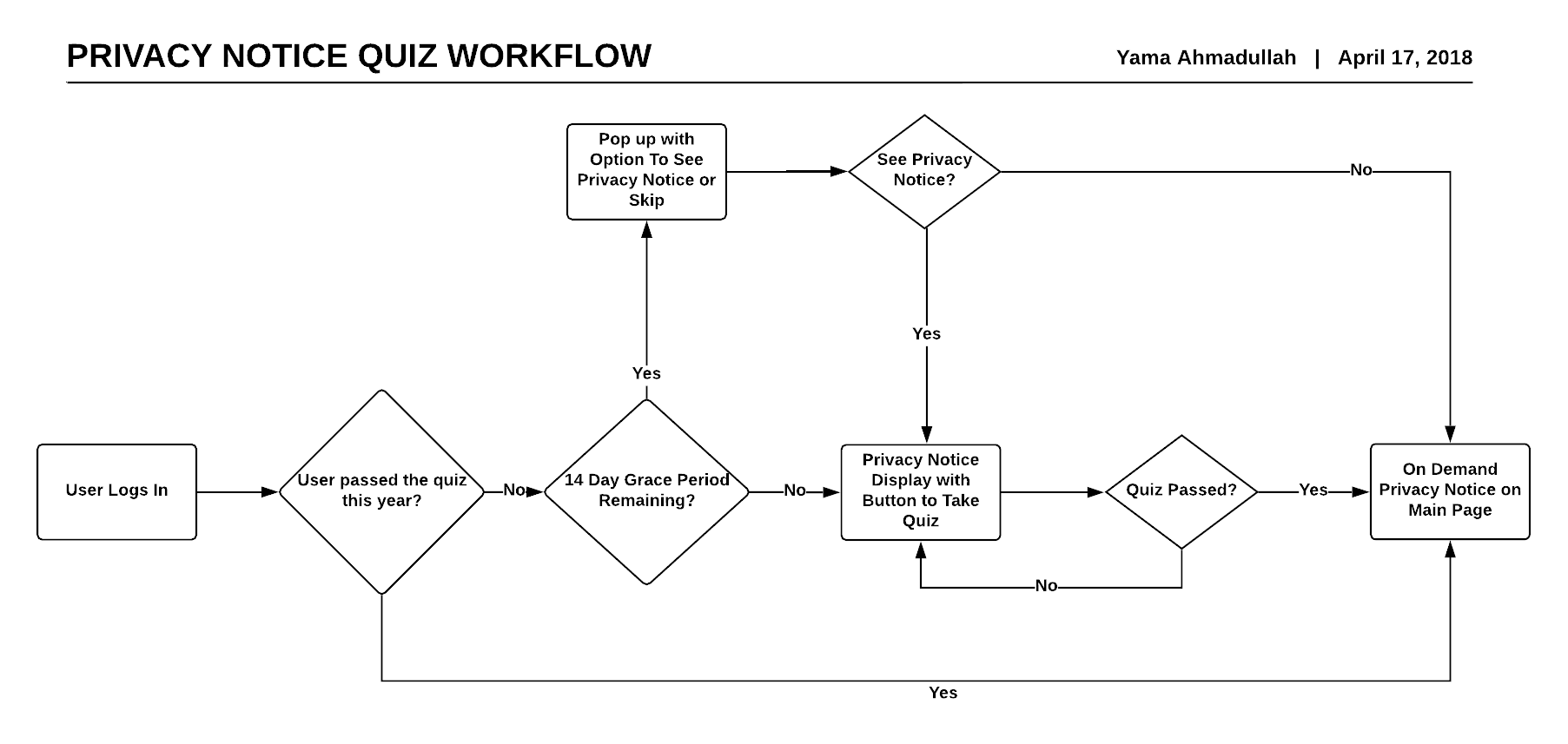
We had several discussions within the team and in class trying to determine if we needed a privacy notice. The basis for our application is for police officers to gather evidence regarding a criminal investigation and in most situations the suspect is unaware of these actions. In this scenario it is not appropriate to provide the user notice or give the user a choice. Additionally, a law enforcement officer would generally not be looking at data that pertains to them, the question was then who was the privacy notice intended for? But not providing a privacy notice did not seem okay either. It was then that we realized that the police officer will be dealing with very sensitive data and that we could change the paradigm a little in regard to a privacy notice and instead treat the notice as way to educate the police officer on their responsibilities handling this sensitive data. We came up with a privacy notice but as mentioned this would be for future development cycles.

As we have learned in class, a key aspect of any application is an effective privacy notice. The challenge is to create a notice that not only informs the user on how their data is being used but also a notice that is succinct, readable, and easy to find. For our application, we have made a key security assumption. We assume the police department will run our application on their local server. The data will not leave the police department’s network. While this put the onus on the police department’s IT department to ensure proper security protocols are followed, this allows us to focus on spending time on more functional parts of the application. Also, privacy notices usually involve input from a legal team which we did not solicit.

As noted by several authors, most people do not read privacy notices. For example in a report by the President’s Council of Advisors on Science and Technology stated, “ In some fantasy world, users actually read these notices, understand their legal implications …, negotiate with other providers of similar services to get better privacy treatment, and only then click to indicate their consent [2:38].” Getting the users of our application to the read the privacy notice is not the only challenge. We also wanted to the users of our application to retain what they read in the privacy notice. In a smartphone privacy notice research, the authors determined “showing the notice during app use significantly increased recall rates over showing it in the app store [1:1].” We wanted to take this method and apply it to our application.

To encourage the users not only read the privacy notice but also retain the information, we decided against showing the user the privacy notice at set up. We decided that the user had to pass a short quiz based on the information in the privacy notice before they could use the application. This would highly motivate the users to not only read the notice but try to retain the information. To keep users from forgetting the information in the privacy notice, we would require that the user pass the quiz each calendar year. We understand some police departments may find this practice somewhat inflexible. To alleviate this, we would allow a decision maker at the police department determine if they want to enable the quiz. Additionally, the user would have a 14-day grace period to take the quiz. For example, if Sam Smalltown has an account created on September 1, 2017, they would have 14 days after the first login to take the quiz before they are forced to take the quiz to use the application. On January 1, 2018, the quiz will need to be taken again, plus a 14-day grace period.

Diagram 1 Privacy Notice Quiz Workflow



The flow of our privacy notice is:

* User logs In
  + On the main screen there is a button to display the privacy notice
* If the quiz setting is set to no:
  + User can access the privacy notice at any time by clicking the privacy notice button on the main screen
* If the quiz setting is set to yes:
  + If this is the first time the user logs in, a pop up highlights the location of the privacy notice and the user is asked if they want to go the privacy notice or skip for now.
  + If the user skips, they will be allowed to skip going to the privacy notice for 14 calendar days. At the end of the 14 days, the use must go to the privacy notice or they will not be able to access the rest of the application.
  + When the user clicks on privacy notice, they will be redirected to the privacy notice page.
  + If this the first time that the user has logged in or the quiz is due, at the bottom of the notice, a button will be displayed directing the user to the quiz.
  + If the user has already taken the quiz, they can review the last quiz they took.
  + Once the user takes the quiz, they need to score an 80% (4 out of 5) in order to use the application.
    - If they score less then 80%, they will be redirected to the privacy notice and then asked to take the quiz again. After three attempts, their account will be locked out and a System Administrator will have to reset their account and ideally help them take the quiz.
  + Once the user has passed the quiz, they will not be prompted to take the quiz until Jan 1, of the following year.

**Privacy Notice Draft**

The privacy policy is effective April 15, 2018.

**Summary:**

Nothing in the privacy policy contradicts the following statements:

1. We do not collect any of your information, including your account details, search requests, warrant information, or location information, including IP Addresses.
2. We do not sell your department contact information to advertisers or other third parties.
3. We will only share your department contact information if legally required.
4. You have some requirements:
   1. You are not allowed to share any sensitive social media information with anyone not legally assigned to your case.
   2. You must report to social media if wrong user information is shared with you.
   3. You must report to social media if you come across any inconsistent user data.

**Complete Terms**

**Our Obligations**

1. We do not collect any of your information, including your account details, search requests, warrant information, or location information, including IP Addresses. This application is hosted on your department’s IT server. We do not have any access to any requests you submit. Your department’s IT department is responsible for ensuring proper security protocols.
2. The only information we collect is your department contact information and sales and marketing information. This information is only accessible by your specific sales person and the database is encrypted. We only use this information to conduct periodic sales inquiries. We will never sell this information to advertisers or other third parties.
3. The only time we will ever share your department contact information is if we are legally required. A proper warrant, reviewed by our lawyers, would need to be submitted.

**Your Obligations**

As a law enforcement officer investigating suspects’ social media data, you may come across very sensitive data. To preserve the general social media users’ privacy, you agree to the following requirements by using our application.

1. Under no circumstance are you are only allowed to share social media user data with individuals not legally assigned to the specific case.
2. Only request data for the narrowest time frame. You can filter the results by specific communicants, keywords, and time. Do not submit overly broad requests.
3. You must have a valid warrant signed by the judge before you can submit requests.
4. You are required to report to social media company if they send you the incorrect user data and data all filtered results. For example, you request information for username badguy1 and social media accidentally sends you information on badguy11. You would need to delete all filtered results and report to the social media company of the error.
5. You are required to report to social media company any inconsistent user data. For example, you believe that Bad Actor has an account with the username badactorforever. You send social media company a request for badactorforever and send the data for that user. Once you look at the data for badactorforever, you see that it is an account by a third person unrelated to the case who is pretending to be Bad Actor. Social Media company would typically close accounts where people are impersonating someone else. You should report this account to social media company.

**Changes to the policy:**

If there are major changes to the privacy notice, you will be alerted through the application to the specific changes. There may be minor changes to the application so please visit this page periodically to see any changes.

Change Log

|  |  |  |
| --- | --- | --- |
| Date | Type | Details |
| April 15, 2018 | Major | Policy Created |
| April 16, 2018 | Minor | Typos and Grammar Changes |
| April 18, 2018 | Major | Policy accidentally deleted and recreated – true story! |

**Quiz**

You are required to pass a quiz related to the details of this privacy notice every calendar year. The quiz consists of 5 questions and you must get 4 correct (80%) to pass. After three attempts, your account will be locked out and you will need to work with your system administrator to reset your account. You will have a 14-day grace period to take the quiz.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Year | Status | Date | Score | Quiz |
| 2017 | Passed | September 1, 2017 | 80% | Link to Quiz |
| 2018 | Failed | Jan 3, 2018 | 60% | Link to Quiz |
| 2018 | Failed | Jan 4, 2018 | 60% | Link to Quiz |
| 2018 | Failed | Jan 5, 2018 | 60% | Link to Qiuz |
| 2018 | Locked |  |  | Account Locked |
| 2018 | Reset | Jan 7, 2018 |  | Account Reset |

Return to Application

Skip Quiz

Take Quiz information we collect is department contact information and sales and marketing information. z

**Sample Quiz Questions**

You will need to get 4 out of 5 (80%) questions correct to pass the quiz.

1. The judge is on vacation and will be back next Monday and will sign your warrant then. You are working on a very violent case and need evidence as soon as possible. She has signed many requests like these before. You are probably safe if you submit the request today.
   1. True
   2. False (correct)
2. The forensic expert assigned to the case is on vacation, but you need their help in analyzing some social media messages. You can get the help of another expert from another department that is not assigned to the case.
   1. True
   2. False (correct)
3. Social Media employee uploaded the incorrect data, even though it is there mistake, you are required to report the error to social media company.
   1. True (Correct)
   2. False
4. You can contact the vendor anytime to get the details and statistics of how many requests you have submitted.
   1. True
   2. False (correct)
5. Sending requests for wide data ranges is appropriate. This way you do not have to submit many requests to Social Media.
   1. True
   2. False (correct)

**References**

[1] Rebecca Balebako, Florian Schaub, Idris Adjerid, Alessandro Acquisti, and Lorrie Cranor. 2015. The Impact of Timing on the Salience of Smartphone App Privacy Notices. 63–74. DOI:https://doi.org/10.1145/2808117.2808119

[2] John P Holdren, Susan Graham, and William Press. 2014. *Big Data and Privacy: A Technological Perspective*. Retrieved April 18, 2018 from https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast\_big\_data\_and\_privacy\_-\_may\_2014.pdf