Privacy Compliance for Esports Leagues

CS 3750: Project Deliverable #3

Suha Hussain

John Jones

Haolin Ye

Yayun Huang

Nealie Glasser

Project Description:

Esports leagues utilize large quantities of data from their players, often forgoing privacy when developing individual agreements. However, new data privacy regulations are being passed as players are beginning to form player associations. Hence, noncompliance with pertinent regulations can incur costs of billions of dollars. Nonetheless, privacy compliance is a nuanced, multi-faceted issue. The complexity of compliance limits the growth of esports leagues and businesses, prevents players from controlling their data, and prevents professionals from implementing systematic changes. Verify Privacy, our proposed system, aims to facilitate transparency and privacy compliance. This app enables esports employees, players, and other trusted parties to analyze the privacy ramifications of league operations by providing recommendations, compliance checklists, and other ancillary information. Privacy compliance for esports can be divided into three major categories of tasks: compliance direction, violation detection, and information analysis that are entirely dependent on the results of each other. These three tasks answer three questions respectively:

1. Compliance direction: What needs to be done to comply with privacy laws?
2. Violation detection: Are there any privacy violations within the league currently?
3. Information analysis: What data is being collected and how is it used?

Requirements Summary:

The system must be able to complete compliance direction, violation detection, and information analysis in order to fulfill its mission of facilitating privacy compliance for esports leagues. Thus, the key requirements are that Verify Privacy:

1. Ensures that a league knows what privacy laws they must comply with
2. Informs league employees, minimally, of steps for compliance
3. Alerts users of potential compliance violations
4. Allows players to understand what information is being collected from them and where that is being sent
5. Informs users of the consequences of each of their decisions
6. Does not require extensive experience in privacy or league operations

7. Can be easily accessed and used at various locations
8. Is intuitive and not highly cognitively demanding

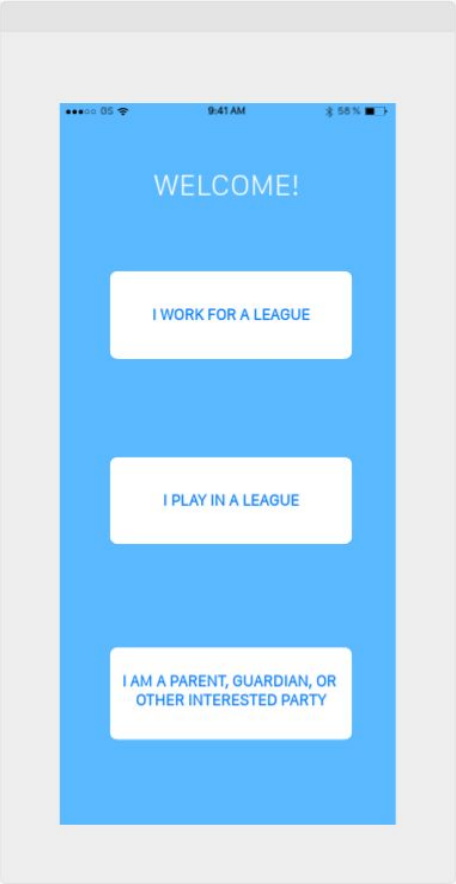
Design Summary:

The three major categories of tasks for privacy compliance in esports are compliance direction, violation detection, and information analysis. Our system is designed to guide esports employees to make the optimal choice and to let players (and trusted parties) know about the consequences of each choice in accordance with the previously mentioned requirements. Verify Privacy designates each user as a player, esports employee, or trusted party, affording them more personalized and effective services. Once registered, different buttons with different services will be displayed on the screen. These services include compliance checklists, compliance reports, recommendations, player data flows, and other supporting features. The most important factors influencing the design of Verify Privacy were effectiveness and intuitiveness. Throughout the creation of the interface, emphasis was consistently placed on prioritizing the lucidity of the design above comprehensiveness or other factors.

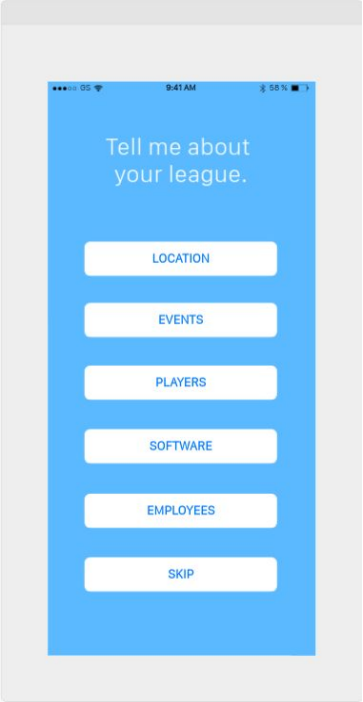
Prototype:

The prototype is a Google Slides document with multiple screenshots of the app that exploits the linkability of slides to simulate the experience of clicking a button. The screenshots of the Verify Privacy interface was generated using FluidUI. This current prototype does not cover all the potential use cases for compliance direction, information analysis, and violation detection as these cases are both quite broad and require extensive research into present privacy issues. Henceforth, the design was formed from a series of scenarios, which will be described in more depth in the evaluation plan. Unfortunately, due to the scope of privacy legislation, it was quite difficult to integrate multiple compliance checklists as well as a comprehensive registration system for leagues beyond merely adding information that affects recommendations. Verify Privacy is the first app geared towards esports privacy compliance; it is also one of the few privacy services that prioritizes clarity and convenience.

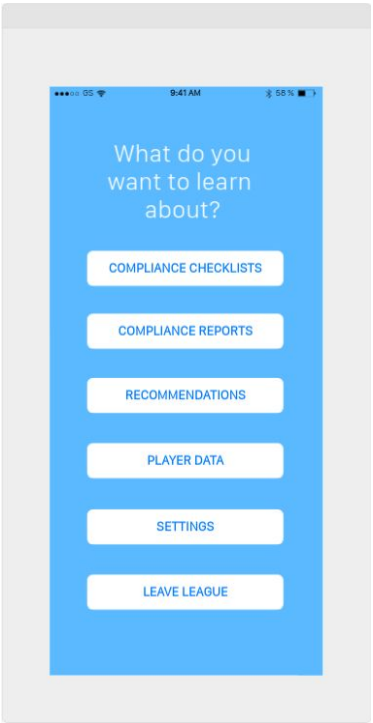
The first scenario tested asked a league manager to choose the optimal messaging system for his league, an example of a compliance direction task. The manager would download and open the app to find the screen below.



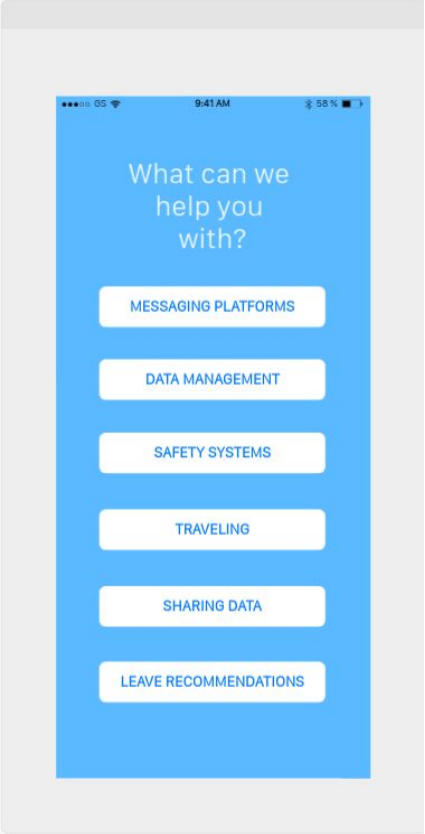
We opted for a minimalist design to reduce the cognitive overhead for users as understanding the inherent privacy and league operations aspects within the app is taxing in and of itself. Logically, the league manager would click on the button on the top, which would bring him to the next screen.



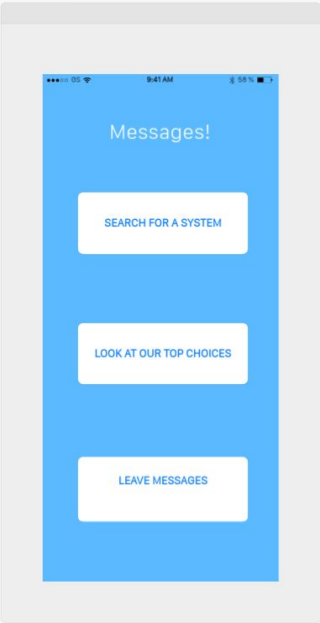
Here, the league manager is allowed to share information about league operations that would propagate itself to the rest of the app. If the manager decides to press ‘Skip’, he will be brought to this next screen.



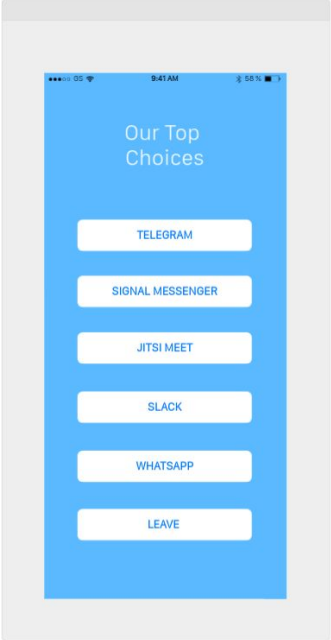
The manager is presented with a multitude of options. Compliance checklists is another tool for compliance direction- one that is more comprehensive. Violation detection can be fulfilled with compliance reports, and information analysis can be fulfilled by clicking on player data. However, the objective of the scenario was to determine the optimal messaging system; thus, the manager would click on recommendations.



This screenshot highlights the different league operation systems that can be evaluated on the basis of privacy. This is likely a very small version of the final prototype's list. The manager would, once again, click on the button at the top, resulting in the next screen.



Assume that the manager prefers to be presented with a system instead of researching systems he was already aware of. This would lead the manager to click on the button in the middle of the screen.



The manager has seen multiple optimal messaging systems and is now on the path to making an informed, confident, and privacy-aware decision due to Verify Privacy.

Evaluation Plan:

Usability Criteria

- ➔ For compliance direction, information analysis, and violation detection, a majority of users only deviated by three clicks at most from the optimal number of clicks
  - ◆ For compliance direction tasks, a majority of users rated their confidence in their decisions at least a four out of seven
  - ◆ For information analysis and violation detection tasks, a majority of users rated their resulting understanding at least a five out of seven
- ➔ A majority of users considered Verify Privacy to be at most a four out of seven when rating the interface's cognitive demand, pacing, and required effort
- ➔ At least seventy percent of users were able to complete their given task
- ➔ A majority of users responded with positive feedback regarding the intuitiveness, convenience, and clarity of Verify Privacy
- ➔ Users with little to no background knowledge provided ratings within thirty percent of users with background knowledge

Overall Methodology

With our prototype of Verify Privacy, we plan to conduct multiple field observations of various users. Several esports employees, players, and other trusted parties have been recruited to perform a given task on the prototype over Zoom. The participants will answer pre-session and post-session questionnaires after being presented with a specific scenario. The participants will be given scenarios commensurate with their background in order to accurately model real-world situations. Furthermore, they will provide feedback on the ease and comfort of use, effectiveness, and lucidity of the interface throughout the session verbally or visually. Each participant will only be asked to model one scenario in order to increase the veracity of results related to prior knowledge and cognitive workload. Presently, we have interviewed two players and one esports employee on each of the three categories. We plan to expand our evaluation to at least ten esports employees, ten players, and ten trusted parties for a total of thirty unique scenarios. The overall procedure for the sessions is:

1. Schedule a Zoom call with the participant

2. Conduct a pre-session questionnaire that ascertains their background knowledge
3. Provide them with their scenario
4. Share the prototype
5. Observe them as they attempt to complete the task using the prototype
6. Wait for them to finish or for thirty minutes to pass
7. Deliver a post-session questionnaire
8. Organize observations from the session

Several factors within the proposed evaluation plan may mitigate the fidelity of the experience. All the use cases were not mapped. Google Slides is utilized instead of a more concrete app, preventing the incorporation of the minitua of app behavior. However, diverse, realistic scenarios were formed and assigned to participants with compatible backgrounds. This will assess user experience more accurately for this early prototype of Verify Privacy.

Pre-Session Questionnaire

Our evaluation system includes a pre-session questionnaire for the user to complete before beginning their prescribed task, so that we could collect information about their background and expertise in order to properly analyze their performance against our expectations. In other words, we would like to ensure Verify Privacy can be utilized by those with little to no background knowledge in privacy or league operations. The pre-session questionnaire is as follows:

1. How often do you play video games?
2. How often do you play video games in a team setting?
3. How familiar are you with esports?
4. Are you currently or have you ever been in charge of managing any team of any sort? (Y/N)
5. Are you currently or have you ever been part of a professional esports team? (Y/N)
6. How familiar are you with the various privacy laws an esports team may have to comply with? (ex. COPPA)

7. How familiar are you with services an esports team may use? (ex. communication services)
8. How confident do you feel in your ability to locate information regarding privacy laws an esports team may have to comply with?
9. How confident do you feel in your ability to verify the privacy of an application? (ex. Does ___ service comply with x y z)
10. How familiar are you with current esports team management software that is available?

Scenario 1: Compliance Direction

As previously stated, there are three major categories of tasks Verify Privacy is expected to complete: compliance direction, violation detection, and information analysis. We developed multiple scenarios for each of these tasks to be performed by esports employees or players. A league manager was presented with the script below describing one of the designed scenarios.

> *You are a league manager of a new league in California. As your league is new, you want to put the word out to the world about some of your most important players, and employees, so you have decided to draft up some biographies to post on your league's affiliated websites and social media platforms. However, you want to ensure the biographies are privacy compliant, and avoid sharing potentially sensitive or personal information that is not willingly shared by the subjects. Essentially, you want to understand what relevant information you are allowed to share under privacy laws.*
>
> *The shared Google Slides document will act as the app for you. Click on the buttons you believe will bring you closer to accomplishing your task. Feel free to express yourself and your thoughts as you are working on your task. Let us know when you believe you have reached your conclusion.*

This task addresses the requirements of ensuring that a league is aware of privacy laws to comply with, informing league employees of the steps to compliance, alerting league managers of potential violations, and informing users of the consequences of their actions. With regards to usability, the optimal number of clicks for this is six. Ideally, users will be left with enough information to make a confident, clear decision about messaging, but not too much to significantly increase the cognitive demand, pacing, and required effort, and decrease the convenience of Verify Privacy.

Scenario 2: Violation Detection

Information analysis is more relevant for players and trusted parties. Thus, our designed scenarios were tailored toward those users. A user completed the task given the script below:

> *You are the parent of an up-and-coming player in an esports league in Illinois. Recently, you have become quite concerned about the privacy practices of the league. You've learned as much as you could about the league prior to downloading Verify Privacy, but you want an expert privacy analysis of the league.*
>
> *The shared Google Slides document will act as the app for you. Click on the buttons you believe will bring you closer to accomplishing your task. Feel free to express yourself and your thoughts as you are working on your task. Let us know when you believe you have reached your conclusion.*

This task is most directly linked to the requirement of Verify Privacy being able to alert users of potential privacy violations. Optimally, this task would require seven clicks. It should not be cognitive demanding, especially on the privacy side due to the background of the participant.

Scenario 3: Information Analysis

Information analysis is more relevant for players and trusted parties. Thus, our designed scenarios were tailored toward those users. A user completed the task given the script below:

> *You are an up-and-coming player in a new esports league in California. As your league is new, your league manager wants to put the word out to the world about you and some of the other new players, so they have decided to draft up some biographies to post on your league's affiliated websites and social media platforms. However, you want to make sure that you have not been sharing any personal or sensitive information that the league manager could use in this biography. Essentially, you would like to see which of your data and information your league manager has access to.*
>
> *The shared Google Slides document will act as the app for you. Click on the buttons you believe will bring you closer to accomplishing your task. Feel free to express yourself and your thoughts as you are working on your task. Let us know when you believe you have reached your conclusion.*

This task addresses the requirements of allowing players to understand what information is being collected from them, and not requiring extensive experience in privacy or league operations.

Study Measures

During the observation session, we collected the results of the pre-session survey, actions undertaken by the participant during the task, feedback given by the participant during the task, and the results of a post-session survey. With regards to the actions undertaken by the participant, this is focused upon deviations from the optimal path. Observable behaviors in relation to the system are recorded anecdotally in our team's notes as another qualitative measure, in addition to the user's out-loud commentary/feedback. The post-session survey incorporates an adapted NASA TLX in order to gauge the workload of the system. It directly attaches to the aforementioned

usability criteria. The survey is as follows (note that participants are asked to respond from 1 to 7):

1. (NASA TLX) How mentally demanding was the task?
2. (NASA TLX) How hurried or rushed was the pace of the task?
3. (NASA TLX) How successful were you in accomplishing your task?
4. (NASA TLX) How hard did you have to work to accomplish your level of performance?
5. (NASA TLX) How insecure, discouraged, irritated, stressed, and annoyed were you while attempting to complete the given task?
6. Answer this question only if you had a compliance direction task. How confident are you in your decision?
7. Answer this question only if you had a compliance direction task. How much did you feel over informed by Verify Privacy?
8. Answer this question only if you had a compliance direction task. How much did you feel under informed by Verify Privacy?
9. Answer this question only if you had a violation detection task. How hard did you have to work to understand what the violation was?
10. Answer this question only if you had an information analysis task. How well do you think you can articulate what is being collected from you and where it is going?
11. How confident are you in the ease of fulfilling privacy compliance?
12. How much did your prior knowledge of privacy and esports (if any) assist you?
13. How convenient did you feel Verify Privacy made privacy compliance?

Data Analysis:

Our data analysis schemes incorporate word clouds and numerous statistical tests. We would like to investigate deviations from the optimal path and potential causes. Moreover, we want to utilize the Likert scale to discover the advantages and disadvantages of our cumulative design decisions. An important point of exploration is to test for correlations between the pre-session questionnaires regarding background

knowledge and the feedback; it is imperative that a necessity does not exist to be well-versed in privacy or league operations for effective usage of Verify Privacy.

Summary and Reflection:

Our very first proposal for a privacy compliance system not only incorporated privacy professionals, but prioritized effectiveness over convenience and usability. Through interviews with users, we formulated the concept for Verify Privacy, realizing the utility of clear recommendations and roadmaps in a notoriously complex area. The initial usability criteria centered on functional requirements, but they shifted to clear indicators of usability, and the requirements evolved to integrate more abstract guidelines for privacy compliance systems. Assessing three design alternatives in conjunction with user interviews underscored the most influential usability metrics. These metrics formed the basis of the requirements and usability criteria, which, in turn, evolved into the questionnaires and data collection contained within the evaluation plan. The proposed system, Verify Privacy, was prototyped using Google Slides and FluidUI around specific use cases based upon the three major categories of tasks for privacy compliance. It will be evaluated through detailed field sessions complete with pre-session and post-session questionnaires.

Breakdown:

Name:	Tasks:
Suha Hussain	Project Description Prototype Evaluation Plan
John Jones	Requirements Summary Prototype
Haolin Ye	Data Analysis Prototype

Yayun Huang	Design Summary Prototype
Nealie Glasser	Evaluation Plan Prototype