**Use Case ID:** SOS17 – Ensure Privacy

**Use Case Level:** Security.

**Details:**

* **Actor:** User
* **Pre-conditions:**
  1. The target Member has profile information set to private or with restricted access.
  2. The Misuser does not have privileges to see the target Member’s private data.
* **Description:**
  1. Use case begins when the Misuser attempts to view the private information belonging to the target Member (e.g., a private feed, or a private membership, or ranking).
  2. The system shall check the Member’s privacy settings.
  3. The system shall check the Misuser privileges.
  4. The system shall check the Misuser against the Member’s whitelist.
  5. The case ends when system rejects the Misuser and present him or her with a standard page indicating that the page is private.
* **Relevant requirements:**

None

* **Post-conditions:**
  1. The system has stopped the misuser from seeing the target Member’s private data.
  2. The system has logged the Misuser’s attempt to see the target Member’s data.
* **Alternative Courses of Action:**
  1. In step D.2, if the privacy settings are not **private**, then system shall provide access.
  2. In step D.3., if the Misuser privileges allow it, then the system shall give access (i.e., the Misuser is an **admin** or has similar privileges).
  3. In step D.4, if the Misuser is in the Member’s whitelist, then the system shall provide them access.

**Extensions:**

None.

**Exceptions:**

None.

**Concurrent Uses:**

None

**Related Use Cases:**

SSLS14 – Check Privileges.

**Decision Support**

**Frequency:** On average, 20 attempts per day.

**Criticality:** Medium. The system should not allow Misusers to easily access non-privileged pages, but implementing private Member, Organization, and Event pages is a secondary objective to the main functionality of the system.

**Risk:** Medium. This is a standard security measure that does not require a lot of work to implement.

**Constraints:**

* Usability
  1. User must be aware of their privileges and what actions those privileges permit.
* Reliability
  1. Mean Time to Failure – 1% failure yearly is acceptable.
  2. Availability – 30 minutes in a 24-hour period for backup and maintenance.
* Performance
  1. Privilege Checks should be done within 2 seconds.
  2. The system should handle 20 privilege checks in 1 minute.
* Supportability
  1. Should be supported by all browsers.
* Implementation
  1. Using Java-based software for back-end.

**Modification History**

**Owner:** Armando J. Ochoa

**Initiation date:** 09/01/2019

**Date last modified:** 09/01/2019