[Project Summary]

“I’m” is a new paradigm to switch corporation driven personal data management environment to user driven personal data management environment. First of all, “I’m” encapsulates personal data and encode before saving in the user’s mobile device. Also, “I’m” can become the bridge of trust between the company and the users. Lastly, the company requests the data they need through this bridge, and the user is the last one to approve. Through this, consumer and the company would trust each other, and furthermore it makes clean personal data ecosystem.

[Benefits for end-user]

The main benefits end-user will gain are “ownership”, “traceability”, “convenience” of personal data. First, “I’m” strengthens the user’s ownership of personal data. Specifically, the personal data will be saved in user’s mobile device and when the corporation wants to access to the data, “I’m” informs the user to select either access or reject the access of the company to one’s own personal data. Only when approved, the company will be able to gain the information of the user, which improves the ownership of the user.

Secondly, “I’m” helps the users to trace the uses of their personal data. When the user allows the company to use his/hers private data, the record of which company and what kind of data it took from the server will be written in the “I’m” server. By using this record, the application visualizes the trace of data. This visualization will be the important foundation of managing the personal data, and will be the powerful counter measure to the imprudent personal data leakage.

Finally, “I’m” offers the convenience to user when filling in or modifying the personal information. When a user takes advantages of a service which requires private data, the user does not need to type in by himself or herself. The service the user is trying to use will take the information from the “I’m” server freeing user from inconvenience of filling all the information needed. Also when the consumer’s private data has changed, user can modify all the information on the websites he or she is using at once by only modifying the data on “I’m”. If the data in “I’m” is changed, the company will request “I’m” for the modified data. By this simple work, modifying personal data becomes easy and it keeps from wrong phone calls and postal receptions.

[25 words]

“I’m” is a powerful system to build a clean personal data ecosystem which lets the “individual” to possess “personal data”.

[Business Model]

For an individual to take service from a company, he/she needs to provide personal data to the company. At this point, he/she is not allowed to know where the data is being used, and the company loses his/hers credit. “I’m” aims for the improvement of this relationship, and tracing and managing where one’s personal data is being used. Through this service, the enterprise could earn user’s credibility, improve corporate identity, and could reduce database maintenance expenditure - since some part of original database would be handled by “I’m”, personnel expenses, and costs for security. The user could be free from anxiety of personal data leakage by the view showing where one’s own personal information is being used.

“I’m” makes profit from the corporations and the users who need these functions. The corporations offer “I’m” service to end-users with their own service by using API. The charging policy of “I’m” depends on number of daily use. “I’m” has limitation and if the number is lower than the limitation, there will be no charges for those companies using API, but if the count exceeds, the companies will be charged of over-number. By this way “I’m” forms initial market, and profits of the geometrical increase of the API requests in order to the increase of the users is the main income for “I’m”.

To get closer to the completion, “I’m” needs cooperation with security company to store personal data safely since there are multiple outside dangers during transmission of data. Through cooperation with “I’m”, the security company could strengthen influence in security market for both mobile application and corporation, and this cooperation will set the stage for the company to become a worldwide security company.

[Technical Approach]

“I’m” consists of three major parts – user application, enterprise API, and “I’m” server. User application is the practical part that interacts with the end-user to help our customer - corporation or company, send the requests to “I’m” server or to get notifications from “I’m” server. Specifically, it provides such views as following – 1) end-user register page, 2) personal data storage page where data is encoded before storing and the decoding key is stored on “I’m” server, preventing mobile hacking, 3) page that asking user to accept/reject company to use personal data, 4) page showing trace and management of user’s personal data usage, 5) page requesting for modified data. The end-user can take advantages of various services through these pages.

“I’m” server is the major part of building reliability between the end-user and the company. It helps communication between user application and enterprise API, and offers diverse functions to both. The server informs each company of data modification, and also senses the time-out and notifies to the company. Moreover, the server receives the requests and then sends the request to the end-user for approval, and at last gives the answer back to company. These requests are stored in the database of “I’m” server, so that end-users could look up their records, and trace their data with the application.

Enterprise API is an essential portion of the system for the companies to take services from “I’m”. It is offered in JavaScript API form, and Android API form, and the followings are the main functions – 1) form to get personal data from end-user, replacing existing form, 2) information requesting function through user ID, 3) function that provides event listener of modified data, and noticing time-out. Enterprise can easily produce web application covering these services by using “I’m” API.

[Sample Demonstration Scenario]

As the user implements the application and starts for the first time, user is supposed to type one’s own email account and password to sign in. And then user needs to fill in the information which the application demands. As the user fills in the information, the data will be encoded and saved in the user’s mobile device, and the key to decode the data will be saved in the server. After this process, when the user joins a website such as the shopping mall website, the user can easily sign in by clicking ‘Join In with “I’m”’ button. The shopping mall will request the user’s data needed to join the website to “I’m” server, and as the request is received, the server sends the permission form to the user to get agreement to let the shopping mall to use the personal data. When the user agrees, the information saying what kind of data is being used from the website will be recorded in the application. The shopping mall saves the data in its own server and “I’m” will set the timer to fix the time limit of the data to make it sure to delete the data as the timer stops. This timer will notify the shopping mall of modified data and the time limit. To finish the purchase, the only thing that user need to do is to click ‘Purchase with “I’m”’ button. Then the shopping mall will use not-expired data of user to precede purchase.