# Interfaces for Defining the Privacy of Sensor Data based on Users' Preferences

Shunsuke Aoki and Kaoru Sezaki
Graduate School of Information Science and Technology, The University of Tokyo
shun@mcl.iis.u-tokyo.ac.jp, sezaki@iis.u-tokyo.ac.jp

The utilization of sensor data from individual users is a significant component in the area of crowd sensing, smart grid, E-health, and transportation management services, while the privacy issue has become a very serious problem in these applications. For the purpose of preserving the privacy, numerous researchers have presented technical approaches, such as encryption, data perturbation, or personal database systems [3, 5]. On the other hand, some researchers in HCI, social science, or public policy [4], have investigated users' perceptions with questionnaires about the data utilization in these applications, for defining the appropriate privacy level in our society. Despite these researches, our society could not avoid the phenomenon of the 'Flaming' in the area of data mining and data utilization. In fact, East Japan Railway Co. tried to sell and launch the personal data collected from IC train tickets in 2013, but immediately elicited social disapproval [1].

The root of the privacy issue in pervasive computing is the difficulty of defining the appropriate privacy level. Firstly, privacy is not same as security and the definition of privacy is constantly changing with social situations, common sense, and application administrators [2]. The perceptions of general users are easily influenced by the accessible pervasive computing technologies in our daily lives and the benefits from the data mining. In addition, technical approaches, such as encryption and data perturbation, are evaluated with quantitative ratings, even though social science and public policy have analyzed the users' perceptions with social investigations.

In this context, this abstract presents a novel framework, *Democratic Privacy*, where the *Public Privacy Level* is constantly calculated and shared based on general users' privacy settings. Democratic privacy is an interface enabling general users to express their perceptions about the data utilization, and the system would provide an incentive for the application administrators to design secure and reliable applications. In addition, each user are able to set the privacy level, being judged by reference to the shared statistical privacy level. The system with democratic privacy would motivate the general users and the application administrators to avoid improper behaviors and violent criticisms.

Democratic privacy would give the authority of personal data to each user him/herself. Therefore, democratic privacy is designed for enabling users to process their data in the user-side, to express their perceptions, and to contribute to service administrators. To meet the requirements, we adopt the data perturbation for processing the sensor data [5].

As shown in Fig.1, each user submits the perturbed data to the Application Server (AP Server) after data processing in the user-side, and continuously reports the privacy level to the Privacy Level Storage Server (PLS Server). The PLS Server gathers the privacy level which are set by each user, and forwarding the statistics of the privacy level, to the AP Server. The public privacy value could be opened to the public, as if share prices in the stock market. The AP Server gathers the processed data, and reconstructs the original data distributions with the statistics of the privacy level. In other words, the general users are able to contribute to service applications via the AP Server, and express their own opinions and feelings via the PLS Server.

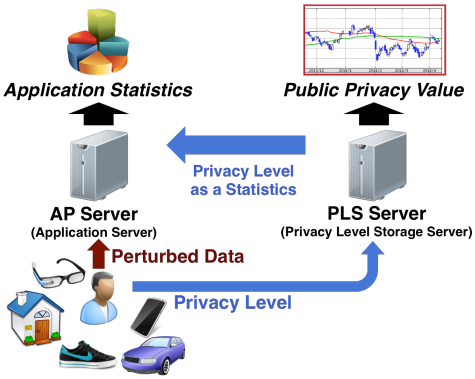


**Figure 1: The concept of Democratic Privacy. Each user send the perturbed data to the AP Server, and the privacy level to the PLS Server.**

There are a number of major challenges that must be solved to realize the vision of democratic privacy;

***Calculating Public Privacy Value***: It would enable us to monitor and know the social privacy perceptions of each application constantly, as if share prices in the stock market.

***Constructing Reliable Statistics for Application***: Our framework preserves the privacy of sensor data, while sharing the social perceptions of data utilization.

***Designing Intuitive User-Interface***: Intuitive user-interface is essential to knowing the users' perceptions accurately.

***Ensuring Reliability over System***: For keeping the reliability of public privacy value and application statistics, the secure system with user authentication is indispensable.

The Concept of *Democratic Privacy* is based on the assumption that the definition of the privacy will keep changing with the social situations, pervasive technologies, and common sense. The ultimate objective of the research is building up the environment encouraging general users to willingly share their sensor data, which does not include the true sensitive information.

## REFERENCES

[1] The Japan Times. *JR sells commuters' data.* 2013.

[2] Krumm, J. A survey of computational location privacy. *Personal and Ubiquitous Computing 13*, 6 (2009), 391–399.

[3] Choi, H., Chakraborty, S., Charbiwala, Z. M., and Srivastava, M. B. SensorSafe: a framework for privacy-preserving management of personal sensory information. In *Secure Data Management*. Springer, 2011, pp. 85–100.

[4] Brush, A. B., Krumm, J., and Scott, J. Exploring end user preferences for location obfuscation, location-based services, and the value of location. In *Proceedings of the 12th ACM International Conference on Ubiquitous Computing*, Ubicomp '10, ACM, pp. 95–104.

[5] Aoki, S., and Sezaki, K. Privacy-preserving community sensing for medical research with duplicated perturbation. In *Communications (ICC), 2014 IEEE International Conference on* (June 2014), pp. 4252–4257.