IEEE Access
Multidisciplinary : Rapid Review : Open Access Journal

Received January 12, 2021, accepted January 12, 2021, date of current version January 26, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3051825

COMMENTS AND CORRECTIONS

Corrections to "Preference-Based Privacy Markets"

RANJAN PAL[1,2,8], (Member, IEEE), JON CROWCROFT[2], (Fellow, IEEE), YIXUAN WANG[1], (Student Member, IEEE), YONG LI[3], (Senior Member, IEEE), SWADES DE[4], (Senior Member, IEEE), SASU TARKOMA[5], (Senior Member, IEEE), MINGYAN LIU[1], (Fellow, IEEE), BODHIBRATA NAG[6], (Senior Member, IEEE), ABHISHEK KUMAR[5], (Student Member, IEEE), AND PAN HUI[5,7], (Fellow, IEEE)

[1]Department of Electrical Engineering and Computer Science (EECS), University of Michigan, Ann Arbor, MI 48109, USA
[2]Department of Computer Science and Technology, University of Cambridge, Cambridge CB2 1TN, U.K.
[3]Department of Electronic Engineering, Tsinghua University, Beijing 100084, China
[4]Department of Electrical Engineering, Indian Institute of Technology Delhi, New Delhi 110016, India
[5]Department of Computer Science, University of Helsinki, 00100 Helsinki, Finland
[6]Indian Institute of Management Calcutta, Kolkata 700104, India
[7]Computer Science and Engineering Department, Hong Kong University of Science and Technology, Hong Kong
[8]Department of Pure Mathematics and Mathematical Statistics, University of Cambridge, Cambridge CB2 1TN, U.K.

Corresponding author: Ranjan Pal (palr@umich.edu)

This work was supported in part by the NSF under Grant CNS-1616575 and Grant CNS-1939006, in part by the Army Research Office (ARO) under Grant W911NF1810208, in part by the Hong Kong Research Grants Council under Project 16214817, in part by the 5GEAR Project, Academy of Finland, under Grant 319017, and in part by the FIT Project from the Academy of Finland.

In the above article [1], *we importantly missed out on generalizing the application scope* to the inter-disciplinary contributions made in the article. It is essential to educate the readers on an increasing variety of novel and highly practical *modern-day application families* where the contributions made in [1] are equally applicable—not just the evident application pertaining to mobile-ad ecosystems, as in [1].

I. BACKGROUND PREVIEW

The authors in [1] proposed a general mathematical skeleton to model the preference-based privacy trading scenario between multiple data sellers and a single buyer – information privacy being measured in composable tangible units (e.g., differential privacy). The skeleton, closely adapted on existing work in [2]–[4] on a compromise—inducing supply-function preference theory, reflects both, perfectly competitive and oligopolistic privacy trading structures, where the focus is on aggregate (over multiple consumers) data sellers who are mobile apps and data buyers that are ad-networks/retailers/cloud provider. However, the theory in [1] is directly applicable to two state-of-the-art, socially timely, and industry-viable application environments mentioned below—both of which target individual data sellers.

Private Federated Learning (FL) Environments—This environmental category subsumes a plethora of corporate applications [7], [8]; social networking applications (e.g., Facebook, e-shopping); most applications in the IoT network category mentioned above; and also the recently popular

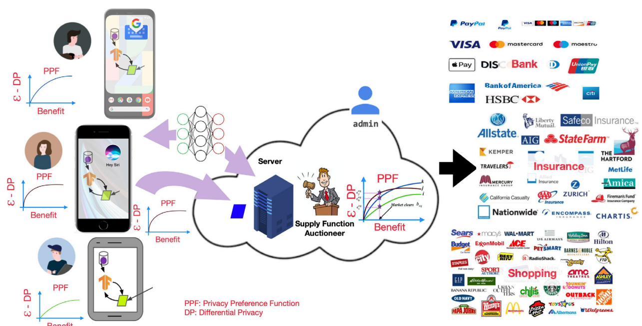

FIGURE 1. Privacy Trading in FL environments.

contact tracing applications during COVID times. In addition, FL demands the constraint that running ML algorithms on individual data be done at the personal devices, and NOT at the data aggregator. The aggregator simply communicates (using wired or wireless communications standards such as WiFi, UMTS, LTE, ZigBee) with the individual devices to **share ML model parameters**, and iteratively converges on the optimal configuration. Though FL by default is a significantly privacy-enhancing technology, recent efforts have showcased the possibility of privacy breaches using such a technology [9], [10]. Consequently, a proposed solution has been to add a privacy layer atop FL [9]. As a result, we advocate for preference-based privacy trading to be social-welfare improving for private-FL applications. More specifically,

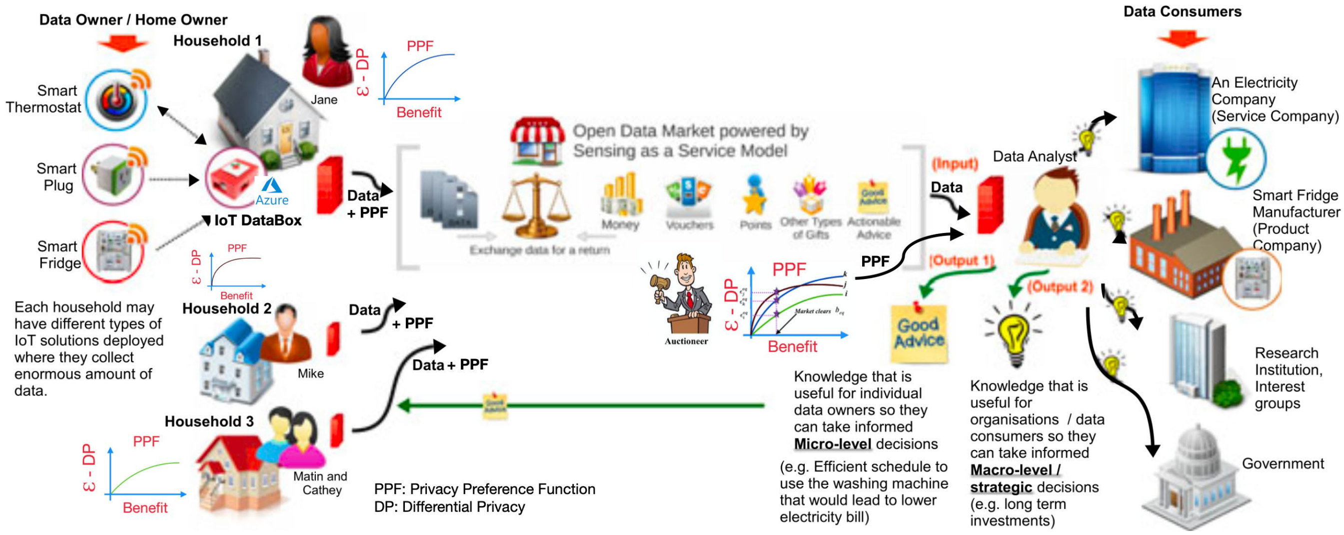

FIGURE 2. **Privacy Trading in IoT environments.**

the **data sellers become individual personnel (e.g., mobile device) dealing with private ML parameters**, and the **data aggregator assumes the role of the data buyer—***privacy compromises iteratively taking place on the communicated ML parameters until the market converges (see Figure 1).*

IoT Environments for Societal Applications—This environmental category includes, but not limited to (a) wearable sensor networks (e.g., body-area networks); (b) connected smart car networks supporting intelligent traffic and safety applications (e.g., collision avoidance); (c) machine to machine home systems which are used in both industrial CPSs, as well as in smart homes that are intelligent and responsive to human beings, and (d) remote healthcare systems. The main features shared by these different categories of devices are (i) the almost continuous connectivity through a wide range of wireless communications standards (e.g., WiFi, UMTS, LTE, ZigBee) and (ii) the ability of a personal data collector (e.g., DataBox [5]) to collect personal/individual application data and use it, post-AI/ML processing, to act on the individuals (as part of QoS) present in such an environment. *The data of personnel present in the environment can often be related to each other in time and space and can pose privacy risks if not managed effectively.* In view of the recent recommendations made in [6], for the ethical design of IoT systems, our proposed privacy trading mechanisms for improved social welfare are directly applicable to such environments. More specifically, the **data sellers (e.g., via an IoT DataBox) become individual personnel** in pervasive environments, and the **data collecting device/app assumes the role of the data buyer (see Figure 2).**

REFERENCES

[1] R. Pal, J. Crowcroft, Y. Wang, Y. Li, S. De, S. Tarkoma, M. Liu, B. Nag, A. Kumar, and P. Hui, "Preference-based privacy markets," *IEEE Access*, vol. 8, pp. 146006–146026, 2020.
[2] P. D. Klemperer and M. A. Meyer, "Supply function equilibria in oligopoly under uncertainty," *Econometrica, J. Econ. Soc.*, vol. 1, pp. 1243–1277, Nov. 1989.
[3] R. Johari and J. N. Tsitsiklis, "Parameterized supply function bidding: Equilibrium and efficiency," *Oper. Res.*, vol. 59, no. 5, pp. 1079–1089, Oct. 2011.
[4] N. Li, L. Chen, and M. A. Dahleh, "Demand response using linear supply function bidding," *IEEE Trans. Smart Grid*, vol. 6, no. 4, pp. 1827–1838, Jul. 2015.
[5] A. Chaudhry, J. Crowcroft, H. Howard, A. Madhavapeddy, R. Mortier, H. Haddadi, and D. McAuley, "'Personal data: Thinking inside the box," *Aarhus Ser. Hum. Centered Comput.*, vol. 1, no. 1, 2015.
[6] G. Baldini, M. Botterman, R. Neisse, and M. Tallacchini, "Ethical design in the Internet of Things," *Sci. Eng. Ethics*, vol. 24, no. 3, pp. 905–925, 2018.
[7] P. Kairouz *et al.*, "Advances and open problems in federated learning," 2019, *arXiv:1912.04977*. [Online]. Available: http://arxiv.org/abs/1912.04977
[8] L. Li, Y. Fan, M. Tse, and K.-Y. Lin, "A review of applications in federated learning," *Comput. Ind. Eng.*, vol. 149, Nov. 2020, Art. no. 106854.
[9] H. B. McMahan, D. Ramage, K. Talwar, and L. Zhang, "Learning differentially private recurrent language models," in *Proc. Int. Conf. Learn. Represent.*, 2018, pp. 1–14.
[10] C. Ma, J. Li, M. Ding, H. Yang, F. Shu, T. Suek, and H. V. Poor, "On safeguarding privacy and security in the framework of federated learning," *IEEE Netw.*, vol. 34, no. 4, pp. 242–248, Jul./Aug. 2020.