

(Position paper) Where personalization, privacy, and security meet

Chris C. Demchak¹ and Kurt D. Fenstermacher²

¹ School of Public Administration and Policy and ² Management Information Systems, Eller College of Management, University of Arizona, Tucson, AZ, 85721, United States

¹ demchak@u.arizona.edu and ² kurtf@eller.arizona.edu

Abstract. We have been developing dynamic user modeling techniques, while also pursuing policy research to strike a balance between an individual's privacy and society's security. We analyze user modeling through our policy lens, known as the behavior-identity knowledge (BIK) framework and offer suggestions on how to protect user privacy.

Existing work by Kobsa [1] and Cranor [2] has highlighted personalization's risks to privacy — to personalize systems requires gathering personal data, which is then used to guide the adaptation process. Much of this personalization can be captured by the single question, "What will the user do next?" By anticipating the answer, systems can better serve users by adapting the presentation of information [3] and other user interaction aspects. We view this conflict between personalization and privacy as similar to national security concerns in a post-9/11 world. Rather than asking "What will the user do next?", however, people ask, "What will the suspect do next?" Instead of gathering data on user preferences, new profiling and tracking technologies accumulate data on suspects and others. Indeed, even data gathered in service of user modeling might later be used to hunt for terrorists and others. Advances in scale, scope, and the accuracy of user modeling inevitably place these technologies squarely in the debate on how to balance security with freedom, and particularly the freedom of privacy.

In previous work on balancing privacy and security, we have described privacy as an aggregate of two independent concepts (shown in Fig. 1): knowledge of behavior and knowledge of identity, which we call the Behavior-Identity Knowledge (BIK) model. We argue that privacy is not at risk unless an organization (or a person) knows both a person's identity and behavior. From a policy perspective compromising between knowing one or other, society should focus its efforts

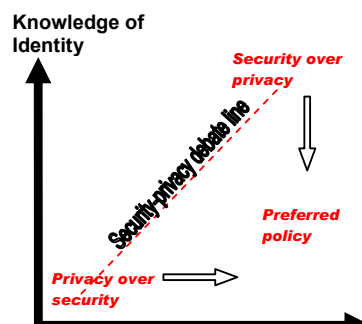


Fig. 1. Decomposing behavior and identity

on monitoring behavior, initially without regard to identity. Only when there is reasonable cause, do we allow the institution revelation of the identity of suspicious persons. Moreover, we must have BIK-implementing institutional safeguards such that, whenever organizations consider behavior and identity together, we can quickly

validate the underlying data and offer a rapid appeals process to redress errors in the systems.

We will start small this fall with a simulation of this interplay using randomly created identities with varying identifiers including simulated fingerprints and DNA, and personal goals. We will use AI planners with time-stamped action sequences, and unrelated human like random actions. Simulated institutions will mask identities with validation and appeal (V&A) processes and also monitor stochastically the actions to model the difficulty in learning everything about everyone. Including organizational sharing of information as well, we will work to create a modular design that would enable varied user modeling techniques to apply in the simulation. We will model the organizations as searching for suspicious patterns of behavior, but the agencies will not have access to the plans and goals of the population, but instead only the actions that are the realization of those plans and goals. In the simulation, organizations will be able to petition for the resolution of a pseudonym once the likelihood of a match between a person's actions and a suspicious pattern of activity exceeds a threshold, just as law enforcement agencies must today meet escalating burdens to authorize more invasive actions against citizens.

In this work, we address the challenge of security, privacy, and the double-edged sword of advancing personalization in a widely networked society. We suggest a framework and hope to provide a design to help resolve this dilemma technically and institutionally, in the form of a simulation to test both the BIK framework and user modeling techniques in a controlled environment.

References

- [1] A. Kobsa and J. Schreck, "Privacy through pseudonymity in user-adaptive systems," in *ACM Transactions on Internet Technology*, vol. 3, pp. 149-183, 2003.
- [2] L. F. Cranor, "I didn't buy it for myself' privacy and ecommerce personalization," presented at 2003 ACM workshop on privacy in the electronic society, Washington, D. C., U.S.A., 2003.
- [3] A. Kobsa, "Personalized hypermedia and international privacy," in *Communications of the ACM*, vol. 45, pp. 64-67, 2002.
- [4] E. Alderman and C. Kennedy, *The Right to Privacy*. New York, NY, USA: Alfred A. Knopf, 1995.
- [5] R. O'Harrow, Jr., "In Age of Security, Firm Mines Wealth Of Personal Data," in *The Washington Post*. Washington, D.C., 2005, pp. A1.
- [6] C. C. Demchak and K. D. Fenstermacher, "Balancing security and privacy in the information and terrorism age: distinguishing behavior from identity institutionally and technologically," in *The Forum*, vol. 2, pp. Article 6, 2004.