

Statement of Latanya Sweeney, PhD
Associate Professor of Computer Science, Technology and Policy
Carnegie Mellon University
Visiting Professor: Harvard University and MIT
Director, Data Privacy Lab

before the Federal HIT Policy Committee

“Constructing Provably Appropriate Technology”

September 18, 2009

Respected Chairman, Vice Chair, and the Members of the Committee, thank you for the opportunity to talk today on constructing provably appropriate technology.

My background: On one hand, I have exposed many fallacies in well-intentioned privacy protection schemes. On the other hand, I have developed technical solutions for sharing data with provable guarantees of privacy protection. My results have been within and beyond healthcare and reportedly widely. (See <http://privacy.cs.cmu.edu> , and my CV at <http://privacy.cs.cmu.edu/people/sweeney/cv.html> for examples.)

Most important lesson learned: My experiences reveal that the best way to address most stakeholder concerns (e.g., privacy, usability, liability, accountability) is through technology design. Unfortunately, technology is usually deployed, and then afterwards, privacy and other stakeholder barriers emerge, leaving society in a “take it”, “leave it”, or “try to mend it” position. We can do better. When technology developers consider privacy and stakeholder concerns throughout the design process, resulting technology promises to be “worry free,” and therefore likely to enjoy user acceptance, societal adoption, and organizational uptake. (See <http://privacy.cs.cmu.edu/dataprivacy/projects/dialectics/> for more information about a paradigm for constructing provably appropriate technology.)

Extending current approaches before design: Most of the privacy concerns voiced today can be resolved through strategic design decisions. But design should precede adoption of existing standards, practices, and overarching principles. Otherwise, we risk igniting new stakeholder problems and exasperating old ones by applying existing approaches in a different context and on a different scale.

Example: Consider data segmentation as a means of de-identifying patient records. Linking segmented data to other datasets often leads to re-identifications. Promoting data segmentation for use in the national infrastructure in the absence of an overall design puts more patient information at risk and precludes more effective design and technical remedies.

Example: Consider the use of encryption to link de-identified patient records. The existence of a shared key introduces re-identification risks. Promoting encryption for use in the national infrastructure in the absence of an overall design makes more patient information vulnerable and discourages use of other stronger cryptographic solutions.

Existing standards and practices are not enough: Another problem with exalting existing approaches is a lack of coherency and fitness of purpose. Industry and standards organizations lacked the authority and perspectives to resolve many stakeholder concerns, including most of the privacy issues voiced here today. Additionally, there is a functional gap between the vision of a responsive national health information infrastructure and existing approaches.

Example: Consider the task of locating records for patient Alice. A naïve approach may require a national index of all patients, relating Social Security numbers to locations of provider records. To satisfy the request, the central authority that maintains the index looks up Alice and returns the list of places holding provider records for her. This is similar to what was originally proposed in HIPAA, but was met with such privacy outcry that the Privacy Rule resulted.

ONC's crucial role: ONC has the unique strategic opportunity to design a national health information infrastructure that is appropriate for its personal, professional, societal, organizational, and legal context.

Closing the gap: A key problem is the timetable on which ONC has to operate under ARRA and the lack of available well-formed possible designs. We want ONC to be able to contemplate competing designs for various interoperable parts of the infrastructure, to compare and contrast critical stakeholder issues in each proposed design, and then to construct a final design based on rigorous analyses and consideration.

Identifying well-formed possible designs is not as simple as calling on industry to propose designs. Industry will respond, but will do so, without needed knowledge of stakeholder concerns and without leveraging newer technologies from other areas.

Instead, I believe we can help industry develop the best solutions by first providing them with well-formed problem statements that identify needed functions and stakeholder interests to consider. Many of us in academia are willing to help. Our idea is to join with industry and other stakeholders for intense, in-depth analyses sufficient to generate well informed designs. Our mission is not to directly construct technical solutions or to insert ourselves into solutions. We will produce publicly available white papers that provide detailed analysis. Our approach offers a kind of “pre-certification” by promising viable technology designs that have a better likelihood of user acceptance, societal adoption, and organizational uptake before they are built.

We are launching the AdvanceHIT Project (<http://AdvanceHIT.org/>) on Monday with initial research foci at Carnegie Mellon, Harvard, and MIT. Our work and reports will be publicly available for free. We welcome industry participation, stakeholder involvement, other academic contributors, and public comments. Success: helping industry provide 5 viable competing designs for ONC's consideration.

Thank you.

Latanya Sweeney, PhD.

latanya@seas.harvard.edu