Request for Information (RFI) on Public and Private Sector Uses of Biometric Technologies: Responses

DISCLAIMER: Please note that the RFI public responses received and posted do not represent the views or opinions of the U.S. Government, the Office of Science and Technology Policy (OSTP), or any other Federal agencies or government entities. We bear no responsibility for the accuracy, legality, or content of these responses and the external links included in this document. Additionally, OSTP requested that submissions be limited to 10 pages or less. For submissions that exceeded that length, the posted responses include the components of the response that began before the 10-page limit.
Good Afternoon,

I am responding to the RFI on Public and Private Sector Uses of Biometric Technologies. My background is in mobile privacy where I do research primarily in how mobile applications use data that is both sensed, stored, and inferred from a smartphone. I was very pleased to see that the government is taking action when it comes to biometrics and creating a "Bill of Rights" in regards to how AI is implemented and being used.

From my research, the larger concern is how the data used in artificial intelligence is gathered. In mobile apps, users do not have a bill of rights, yet spend a considerable amount of time a day interacting with their devices. One study showed the average American spends over 4 hours a day on their smartphones. When we think about this interaction, there is quite a bit of data that can be gathered and when we think about the revenue from companies such as Facebook and Google, which do not sell most consumers a service where it is primarily driven from advertising, the more precise they are with their advertising (from the data they collect), the more profitable they become. Tangentially, these services and the algorithms that serve content to the users, whether they be advertisements or recommendations, have been found to put users in content bubbles and serve content that can be misinformation and addictive. I think if we truly want to provide a bill of rights for consumers, we need to start where the data is collected, and mobile devices seems to be a prime candidate based on the amount of time that users interact with the device and the data that is stored, sensed, and inferred from the device.

The more transparency that consumers are provided, the more their attitudes change with concerns on privacy and data collection. Past studies have shown this including our own. Also, when controls that limit data collection are made available to users and not hidden away in an application (dark patterns), more users adopt these controls. An example of this is the recent change in iOS where an application requests if they can track the user. In one study, an overwhelming majority of users chose the option not to allow tracking. This is critical because if we want the public to buy into the effort, they need greater controls and abilities to see their data. When they have this, they can then better understand the value in these efforts and be more interested in the outcomes of these efforts. The capabilities to provide great transparency and controls to users already exist and have been shown in previous research to be effective. Recently, some of these have been incorporated partially in iOS and Android where users have more fine-grained control of their data. However, the pace of implementing these controls and transparency natively have been slow. Additionally, two companies (Apple and Google), solely control 100% of the smartphone operating system market in how these controls are implemented.

I believe we need to start with the source of the data first, which is why I'm advocating for greater transparency and controls on mobile device, and perhaps even a Bill of Rights on the intrusive data collection that is performed on the devices we interact with the most.

Thank You,
Brian Krupp
Dr. Brian Krupp  
Associate Professor of Computer Science  
MOPS & CS+ Faculty Advisor  
Baldwin Wallace University

>https://mops.bw.edu<