Re: Developing a Privacy Framework/Docket 181101997-8997-01

In response to the National Institute of Standards and Technology's (NIST) Request for Information (RFI) regarding the development of a Privacy Framework, Brainwaive, LLC., is pleased to provide the following comments based on our experiences and mission for consideration to help inform the development of the Privacy Framework.

We note in the RFI under the section of Specific Privacy Practices, the question whether practices contributed by organizations are relevant for new technologies like the Internet of Things and artificial intelligence. We would like to bring to your attention immersive technology as a new technology to consider in the development of the framework.

Immersive technologies such as virtual and augmented reality are gaining significant popularity. Over the past two years, there has been a strong interest in immersive technologies from the likes of advertising agencies, game developers, manufacturing companies and more, as it has the potential to transform how we interact with information and our world. Immersive technology is not a new concept, but it does bring to the forefront and put into new contexts concerns and issues regarding security and privacy as these technologies enable users to interact with virtual content in fundamentally new ways. The applications of these technologies capture input from a user's surroundings, such as video, depth sensor data, or audio and they overlay output (e.g., visual, audio, or haptic feedback) directly on the user's perception of the real world, through devices like smartphones, head-mounted displays (HMDs), or automotive windshields. Through these interaction points there is an incredible amount of data capture, direct and indirect, that impact the user's privacy and the privacy of others who are within the view of the user.

Immersive technology is any technology that extends reality or creates a new reality by leveraging a 360-degree sphere or physical surface. Because immersive technology leverages a 360-degree sphere, users can look in any direction and see content. It can extend reality by overlaying digital images on a user's environment or create a new reality by "disengaging" users from their physical world and fully immersing them in a digital environment. With this, the use of immersive technologies raises new overarching ethical challenges, from issues of access, privacy, consent and harassment to undefined future scenarios.

To illustrate this, we can look specifically at Augmented Reality (AR). What sets apart AR from other technologies is its immersive nature. It allows technology to directly mediate a person's perception of and interaction with the physical world. From the perspective of how we might use AR for good, this presents exciting opportunities, but it also makes security and safety concerns much more pressing, and potentially dangerous, compared with any issues raised by more traditional technologies like phones or laptops, which don't directly affect our view of reality.

As AR systems have the ability to provide immersive experiences that directly impact users' perceptions and actions within the physical world, it is critical that we anticipate and address these questions now, before they are widely deployed and their designs "hard wired."

There is a cadre of concerns that arise in the privacy realm, primarily connected to the use of person's and company data—and they go beyond data ownership and having control over one's data. These include concerns centered around:

- Physiological attacks
- Deception
- Unwanted virtual content
- Inappropriate content
- Privacy for bystanders
- Display content on people (people as a surface)
- Access Control
- Managing personal space in AR

To put these concerns into context, we need to look at AR applications and technologies characteristics, that in addition to the traditional definition of aligning real and virtual objects in real-time, a complex set of input devices and sensors are always on (e.g., camera, GPS, microphone); there are multiple output devices (e.g., display, earpiece); platforms can run multiple applications simultaneously; and there is the ability to communicate wirelessly with other AR systems.

To provide their intended functionality, AR applications may require access to a variety of sensor data, including video and audio feeds, GPS data, temperature, accelerometer readings and more. As in desktop and smartphone operating systems, an important challenge for AR systems is the balance the access required for functionality with the risk of an application stealing data or misusing that access.

One of the features that renders immersive reality tools particularly advantageous is the shared access to the information pool that may be enjoyed simultaneously by multiple parties. Indeed, a database collating information about all stakeholders involved, visualized in an intuitive manner and made available as a matter of one click can be of a great convenience. At the same time, such a liberal approach to data sharing invokes a set of confidentiality red flags since the environment may often control highly sensitive personal data collected by immersive components, trade secrets and further intellectual property (IP) of a substantial business value. All of these have to be assigned appropriate confidentiality protocols.

A Privacy Framework that is inclusive of such immersive technologies and takes into consideration how organizations developing and deploying such technologies and devices, be it for enterprise or consumer use, and individuals using such technologies is paramount as we anticipate increased use of AR and other immersive technologies in the near future. These technologies hold tremendous promise to improve enterprise efficiencies, but also holds the potential to introduce new or additional privacy vulnerabilities and concerns, and may compromise in particular the enterprise in regard to compliance issues, financial loss and reputation and brand. Likewise, for consumers these technologies hold great promise as they enable convenience and new ways to interact with brands, friends and family, but introduce privacy challenges that can compromise one's personal data.

We thank you for the opportunity to provide input.

Respectively,
Rob LaBelle
Partner at Brainwaive, LLC

About Brainwaive, LLC
Brainwaive is a consultancy and solutions firm working at the critical intersection of emerging technologies and cyber security in the enterprise. We are committed to ensuring that companies exploring, deploying and refining Augmented Reality (AR), Virtual Reality (VR) and other immersive and mobile solutions have the insight, knowledge and tools they need to fully understand security risks and how to mitigate them.