Online privacy has a broad scope and impacts our culture at multiple levels, including: personal level, organizational level, market level and national level. GDPR does a good job of defining the scope of privacy to include consent, collection, storage, processing, sharing, retention, user rights for access, deletion, correction and porting. Online privacy impacts each of us and all want the best outcome. The opportunity for the NIST Privacy Framework is make it easy for people, organizations, markets and governments to make right choices. As with any project we must begin with the end in mind and do first things first.

End in Mind: EU GDPR is not perfect, but provides a great starting point for consideration of the final NIST privacy work product. Worthy EU/GDPR concepts include, charter of human rights that specifies a right to data privacy. Recognition that individuals own their data. Exploration of privacy impacts at each stage of online relationships. Regulatory mandates for compliance.

First things first: Common sense and recent history show weak identity and authentication are the most common root causes of both large-scale privacy breaches and smaller targeted privacy attacks. Identity and authentication are the foundation for all other data privacy, including privacy of: health data, financial data, legal data and employment data.

Payfone provides identity and authentication as API-based services to organizations that value identity efficiency. In addition to privacy, Identity efficiency includes security, user experience and operational economics. Privacy is the long pole and through collaboration with advanced, innovative and progressive organizations Payfone has identified five important building blocks for identity privacy, these are:

1. Data Minimization to reduce overall privacy attack surface
2. Tokenization for privacy of data stored in the cloud
3. Hardware root of trust to provide silicon isolation for privacy of device-based credentials
4. Zero-knowledge proofs for privacy during exchange / sharing
5. Attestation to enable relying parties to remotely prove data privacy and security characteristics

These guiding principals enable a practical approach to solve what many perceive to be un-solvable.

From collaborating with many advanced organizations, comes the realization that domain-centric identity is the cause of many of todays privacy issues. Organizations largely issue their own domain-centric identities to users. In most cases these domain centric identities a weak from a privacy and security perspective. Most frequently based on username and password, which necessitates leveraging multiple 3rd party services to mitigate new account fraud, account takeover fraud and transaction fraud fraud. The net impact is that user identity attributes are scattered across many domains, which explodes the potential for privacy theft and privacy leakage.

Several initiatives have sought to promote user-centric identity as an alternative to the domain-centric approach. The privacy logic of BYOI (bring your own identity) is compelling, but historically security, ease-of-use and overall identity efficient have fallen short. Simcard based identity is a strong proxy for user-centric identity and enable strong overall identity efficiency. The advantage of Simcards is that they have a unified dual identity, which include a globally unique identity in the real-world and a globally unique identity that can be strongly authenticated in the online world. This strong bind between online identity and real-world identity inherently mitigates mostly-all online fraud schemes. Simcards also meet the five guiding principals for privacy, which are outlined above.

Must of the discussion at the NIST meeting in Austin in late 2018 revolved metrics, risk-based and an outcome-based approach as a focus for the framework. Continuing, this focus would be an opportunity lost. Due to massive interconnection and dislocations in time, it is challenging to attribute all adverse outcomes to specific weak privacy practices. NIST 800-63 has done a great job in defining metrics for identity, authentication and federation. Metrics beyond the NIST 800-63 metrics would be confusing, consensus driven and pseudo-scientific.

The NIST Privacy framework group work-product will offer greater value to more parties sooner, if it clearly and unambiguously shines light on what effective privacy is and provides practical steps for implementing it.