1. Introduction

Since the advent of wireless communication and especially Web 2.0 services, we've come to depend on being constantly connected and meaningfully engaged with the world around us. Yet the ubiquitous nature of data has led to a loss of privacy that threatens the growth of data intensive, collaborative consumer applications as well as innovative, commercial opportunities for the enterprise.

InterDigitial believes that data privacy should be considered from a holistic viewpoint, considering aspects of identity, authorization and access control, personalization, security and trust to provide a convenient, centralized, secure solution for managing data privacy.

2. Identity

Data comes from somewhere. It has a source, provenance and ownership. Any meaningful solution to address data privacy will have to consider aspects of Identity and Identity Management. A user-centric open identity framework can give everyone the opportunity to manage their own identity and customize it for their particular purpose. As we establish our identity with the services around us, we gain confidence that the data we rely on comes from a safe, trusted, known place.

Without trusted identity management, the major threats we face are identity theft and a maligned reputation, both issues that are long lived and costly in our internet dependant lives.

3. Access Control and Authorization

The loss of data privacy can be construed as a failure to control access to data or a failure to control how that data is used. As the services we use become more instantaneous, immediate and customized, controlling access to our information or the data we rely on around us has to occur in real time, based on our personal preferences. Granular access to data and authorization of how that data can be used becomes an important requirement to ensure trust and confidence. In addition, if that access control becomes complex to manage or cumbersome to use, it won't be used. Therefore, access and authorization to data needs to be automatically context dependent, aware of purpose, location, presence, and use.

Failure to properly control the access and authorization of data leads to mistrust, abuse and personal safety issues.

4. Security

Data privacy can be considered a security issue. If our data is not properly secured, then identity, access control and authorization aspects are meaningless. We have to consider secure storage, processing and transmission of data. Without a guarantee of confidentiality and data integrity, we can't rely on the data we receive. If we can't authenticate the user or service, how can we have confidence that our data is used as intended and by whom it was intended?

Data integrity needs to be verified as part of data privacy management. The periodic validation that our data has not been corrupted intentionally or unintentionally needs to be assured, since data

whose integrity is suspected of compromise naturally raises questions about the privacy of that same data or its source.

Privacy is not only about confidentiality. It also includes anonymity. We have to be able to feel safe and comfortable on the internet, and sometimes that means that our transactions, where we go and who we talk to, are not disclosed without our explicit authorization, just like they are in real life.

In addition, the security and privacy policies need to be flexible to adapt to a wide variety of services and use cases, as it is improbable to predict how our data may be used. Our data needs can traverse multiple public and private networks, users and services and has to be responsive and accessible throughout.

A lack of data integrity, authentication, privacy and anonymity can undermine the growth of the next generation internet entirely.

5. “Privacy in your Pocket”

When we consider how ubiquitous, continuous and transparent our data is and how data privacy has to be tailored to a user’s specific needs, it become apparent that an implementation to protect data privacy needs to be under a user’s control and facilitated by a trusted Service Provider.

The mobile device provides an easily accessible, secured trusted environment with which to establish credentials, store data and tailor privacy settings and controls on the device itself.

The privacy stack can be envisioned as follows:

Identity Management -> Authentication -> Access Controls -> Privacy Policies

In conjunction with a Service Provider or Operator, a distributed implementation of these components across the mobile device and the network brings the control of our data into the palm of our hands. The mobile device serves as the source of our data and a portal to interact with the world around us in a personal and customized way. The trusted operator implements our data policy choices and provides safe transport and protection against data privacy loss and abuse.

6. Conclusion

Thank you for your attention and consideration for attendance to the joint Internet privacy workshop on 8 and 9 December 2010: "How Can Technology Help to Improve Privacy on the Internet?"

InterDigital is committed to providing compelling technology solutions in the internet and wireless areas and we hope to secure an invitation to the Workshop.