The Payment-Privacy-Policing Paradox:  
*Toward a Privacy-Conscious Internet Identity System for Payments*

The Web has fundamentally transformed the way the world's people and organizations publish and interact with information. However, the transmission of monetary value has not yet changed. The Web’s foundation offers unrealized potential to transmit and receive funds with the same ease and rigor as sending and receiving email.

Making payments on the Web simpler and more accessible has more than superficial advantages. By distributing to everyone the payment methods that have been traditionally only available to banks and large corporations, the world's economies can benefit from financial system changes that both reduce transaction costs and create new kinds of innovative e-commerce applications. The goal is not to just enable simpler payments, but also to spur innovation in capital formation that helps entrepreneurs of any size, in any location, earn a legitimate living.

One prominent global trend that could greatly benefit is crowd-funding, which is currently constrained by less than elegant and cost-inefficient payments methods. In general, the Web has already boosted funding opportunities for startups, eased tax collection, and increased payment security; and there is room for more improvement. The World Bank reports that 2.5 billion people around the world don't have bank accounts and have no ability to save money due to lack of banking services and/or high fees, which inhibits their ability to make a living. Online payments development enabled by telecom providers in some parts of Africa has served as a remarkable proof-of-concept, though it is restricted by limited competition.

It is evident that whilst bringing new or powerful tools to the general public will foster competition and innovation, open Web payments can also bring about more basic societal change. The promise of Web payments is about more than just an exciting future, it is about one that is at the same time far more egalitarian, and far more efficient for business.

**The Identity Problem on the Web**

It is currently difficult to establish a verifiable identity on the Web. Since identity is one of the fundamental mechanisms that we use to trust the parties in a financial transaction, not having an identity solution for the Web is harming a good payments solution for the Web. The problems with identity for payments on the Web are:

- There is no simple decentralized standard for asserting aspects of your identity on the Web.
● Identities are not discoverable after you login to a website. For example, after you log in, there is no resolvable address that you can provide the website where it can discover more about you. Technologies like Mozilla Persona are a step in the right direction, but more is needed for financial transactions.

● It is not possible to attach verifiable machine-readable information to an identity via 3rd parties. This means that Know Your Customer clearing, required by banks, is very difficult to achieve on the Web because there is no standard way to associate government-issued credentials, like an electronic passport, with your identity on the Web.

● There is no standard access control mechanism to expose both public and private identity data to external sites, based on who is accessing the resource. A vendor cannot easily verify that a person is of legal age or licensed to purchase a particular item.

● There is no standard secure digital signature and encryption mechanism for identity data.

In order for payments to become more trustworthy and secure on the Web, an identity solution that takes payment use cases into account must be created.

Questions that will be explored during the group work include:

● Should you be able to have many identities for payments, including anonymous ones?
● How certain do you need to be that the person is who they say they are that is using the thing that you are interacting with? For a small value transaction? For a large value transaction? For buying 50 litres of milk? For buying 50 litres of ammonia?
● Should identity be traceable? Or should it be unlinkable from a transaction?
● Does a merchant need to know the identity of the person buying something, or should the financial institutions keep this information from the merchants?
● How will the search companies conspire with the banks to track detailed spending habits and sell them to third parties? Should there be legislation against this behavior?
● Who owns their identity data?
● Should identity data be portable from service provider to service provider as a fundamental design criteria?
● Are anonymity and non-traceability the same thing?
● Privacy for online actions is important. Anonymity when it comes to financial transactions and moving of money is problematic. How do we address both?

Technical Background

More background for those that are technically inclined and want to learn about the Identity Credentials specification: http://manu.sporny.org/2014/credential-based-login/