

## Understanding the Economics of Electronic Identity: Theoretical Approaches and Case Studies

Anssi Hoikkanen, Margherita Bacigalupo, Wainer Lusoli, Ioannis Maghiros,  
Stavri Nikolov

► **To cite this version:**

Anssi Hoikkanen, Margherita Bacigalupo, Wainer Lusoli, Ioannis Maghiros, Stavri Nikolov. Understanding the Economics of Electronic Identity: Theoretical Approaches and Case Studies. Elisabeth Leeuw; Simone Fischer-Hübner; Lothar Fritsch. Second IFIP WG 11.6 Working Conference on Policies and Reseach Management (IDMAN), Nov 2010, Oslo, Norway. Springer, IFIP Advances in Information and Communication Technology, AICT-343, pp.41-58, 2010, Policies and Research in Identity Management. <10.1007/978-3-642-17303-5\_4>. <hal-01054401>

**HAL Id: hal-01054401**

**<https://hal.inria.fr/hal-01054401>**

Submitted on 6 Aug 2014

**HAL** is a multi-disciplinary open access archive for the deposit and dissemination of scientific research documents, whether they are published or not. The documents may come from teaching and research institutions in France or abroad, or from public or private research centers.

L'archive ouverte pluridisciplinaire **HAL**, est destinée au dépôt et à la diffusion de documents scientifiques de niveau recherche, publiés ou non, émanant des établissements d'enseignement et de recherche français ou étrangers, des laboratoires publics ou privés.



# Understanding the Economics of Electronic Identity: Theoretical Approaches and Case Studies

**Anssi Hoikkanen, Margherita Bacigalupo, Wainer Lusoli,  
Ioannis Maghiros & Stavri Nikolov**

European Commission's Joint Research Centre – Institute for Prospective  
Technological Studies (JRC-IPTS)  
Anssi.HOIKKANEN@ec.europa.eu

**Abstract:** This paper discusses the economics of electronic identity (eIdentity) from both theoretical and practical perspectives. Personal identity data are becoming increasingly important in online transactions, and they have never been monetised to the extent they are today. Consequently, there is a need for an improved understanding of the economic externalities resulting from the electronic use of identities in transactions. In this context, we distinguish four main theoretical approaches for understanding economics of identity: identity as a consumption good, identity as a capital asset, identity as a social good, and identity as a cost. We analyse each of these approaches in terms of their benefits to understanding economics of identity, their drawbacks, and the bearer of the cost of identity provision. After the theoretical part, we go on to discuss three case studies, BBS, eBay and IdenTrust, and apply an appropriate concept of economics of identity to analyse each business case. Finally, we conclude the paper by discussing the implications that each of the different concepts of economics of identity has for policymakers.

## Introduction

### Background

Identity as a concept has been known for centuries. In the past identity has often been treated as a social good with some externalities or simply as a cost, but its full economic significance is becoming increasingly apparent. Today, personal identity data are vital to the way Internet services are provided, and to citizens' everyday life. Especially in online transactions, personal identity data are becoming an important enabler of the digital economy. They have a crucial role to play in setting the framework conditions so as to sustain this shift while maximising the benefits for economy and society.

The economic importance of electronic identities is increasing for several reasons. Firstly, electronic identification is today indispensable to ensure access to public and private services – including health, education and security. More and more of the personal sphere is recorded, stored and analysed (for example, in the case of nominal e-ticketing, in which identity tags are attached to transactions that were previously anonymous). Identity transactions are based on an increasing number and variety of identity systems. In the Internet, a heterogeneous system of identity assurance has emerged over time, through a mix of open standardisation, engineering ingenuity and sheer monopolistic inertia. There is today a plethora of sector specific solutions

(based on e.g. SSL encryption, PIN, tokens) and e-services (e.g. based on a PKI infrastructure with either strong or weak authentication).

Secondly, the personal identity data of citizens are being used today in two different ways. The first one is to provide access to information and services; this is the 'authentication function' of identity. In addition, however, the personal identifiers used for authentication leave digital traces that may also be used for other, unintended purposes. Profiling – the attribution of identity based on data mining criteria – both for profit (mainly businesses) and security (mainly governments), is on the rise. Other non-personal identifiers may be linked to personal data (as in the case of IP addresses and object tags), and there may be increasing linking of EU citizens' identity to their online and offline activities.

Thirdly, the number of transactions carried out with personal identity data has grown significantly in the past few years, and will most likely continue to do so. Consequently, businesses are increasingly trying to profit from the use of personal identity data for their own gain. There is a tension between the collection of personal data in business-to-consumer transactions and the respect for consumers' privacy preferences. This presents new challenges for policymakers: how to ensure that business abide by current regulations, addressing the challenges to privacy and data protection, while at the same time supporting the economic development of electronic identities and services based on them. Overall, the purposes for which identity data are used today cover a significantly larger spectrum than just authentication. Most significantly, activities such as targeted advertising, based on collected identity data, are becoming more and more common, and in this context there has been an emergence of numerous profiling models (advertising, crime detection, compliance with rules, health monitoring). The economic attractiveness of such activities is clear; indeed, personal identity data have never been monetised to the extent occurring today. While the economic significance of such activities is largely invisible at the moment, emerging mobile, sensor and social networking technologies facilitate the creation of novel services that, in addition to their other functions, enable users to perceive the economic importance of their electronic identities. Furthermore, as distributed systems are assembled from components that have been created for different purposes, economic incentives are becoming as important as technical design in achieving system dependability; without economic incentives there may not be sufficient motivation for different companies to ensure the compatibility of their applications with large-scale systems.

Due to the economic importance of electronic identity, the economics of identity need to be understood in a much more systematic and formalised way than has traditionally been the case. Relatively little is known about how identities are used in economic transactions (either as an enabler or as part of the transaction), what is the economic value of the identity data, how it could be measured, and what business models support the use of electronic identity. This analysis is necessary to quantify the economic significance of the identity market, and to understand how the dynamics of the identity markets function. It is only through this understanding that policymakers are able to effectively regulate the identity space. The drawback of analysing economics of identity in this sense is that to date, there is no clearly defined framework for this analysis; therefore it would take policymakers a significant amount of additional effort to carry out this task reliably and in appropriate detail.

In this paper, the term eIdentity is used to indicate a set of personal information and data relevant to a human's identity (personal and/or collective identity data) when stored and transmitted via electronic systems, including but not limited to computer networks. The terms electronic identity, digital identity and eID are also used to the same purpose in the literature.

### **Research questions**

Evidently, there is a clear need for improved understanding of the economic externalities of electronic identification. A much more detailed analysis is needed of how exactly identity functions as an economic object, what kind of consequences this has both from a theoretical perspective and for policymakers, and how these consequences can be efficiently managed and regulated. To gain a fuller understanding of these issues, we need a framework that looks into the economics from various angles, distinguishes between different ways of understanding them, and looks at how they can be applied in different business contexts.

We foresee that different concepts of economics of identity can be classified into distinct approaches, or schools of thought. Each of them will have different consequences in terms of how identity is defined as an economic object, and how the associated economic externalities can be analysed. Further, each approach has its own set of benefits and drawbacks, with regard to what kind of analysis it allows; researching these benefits and limitations provides an overview of the different issues and considerations that must be taken into account. In order to arrive at a fuller understanding of the economics of identity, it is necessary to map out the various economically relevant aspects of eIdentity.

We therefore propose the following research questions that this paper seeks to answer: 1) What approaches to economics of identity can be identified? 2) How does each of them contribute to our understanding of the economics of eIdentity? 3) How can these approaches be applied to existing companies in the marketplace? 4) In light of all this, what kind of policy implications does this raise for policymakers?

## **Ways of understanding economics of identity**

In this chapter, we discuss four possible approaches to understand economics of identity by defining each, describing the challenges each one solves, discussing their limitations, providing an example of how each approach can be applied, and finally by concluding how this approach helps us understand economics of identity.

### **Identity as a consumption good**

One way to grasp the economics of identity is to analyse **identity as a consumption good**, in which case users choose their identity according to how and where they want to use it<sup>1</sup>. In this case, identity results from *explicit* choices by the individual. This implies that personal identity data are transactable and can be sold, either temporarily or permanently. In turn, this understanding of identity raises questions of what purposes identity can be used for, how long it remains valid for, and what contractual regimes would be applicable. Identity could also be stolen; this raises issues concerning trust in the transaction environment, accountability, individual responsibility, and appropriate adoption of identity. The classic economic

approach to analyse identity as a consumption good is economics of choice. Identity can then be analysed by introducing it as a factor in the utility function as in general economics<sup>ii</sup>.

'Identity as a consumption good' provides several insights into how these economics function. First, it describes in detail how identities can be used in economic transactions and the possible value of identity in such transactions. Second, the approach allows taking into consideration the fact that people have different identities in different situations and use cases, and that personal identity data can be used in varying ways according to the context. Thus this approach goes a long way towards explaining why the value of the person's identity or personal identity data can differ significantly in varying circumstances. Third, it also brings to the fore the *active role* that the user may have in managing her personal data: as the user chooses which data are the most relevant to the context. The economic consequences that result from this choice of personal data, and the level of personal responsibility required from the user, vary according to the type of data.

Despite the above described assets, this approach has some clear limitations. The approach is quite complex and to accurately determine the value of identity in a particular case would be very difficult. It would be necessary to have a detailed understanding of the case in question and would mean that a lot of data is at the disposal of the stakeholder assessing the value of the identity. The approach also places a heavy burden on the user: the user may have to not only collect and manage, but to process large amounts of information to make informed decisions.

As a consequence of these limitations, the resultant identity markets would likely be very complex, as the circumstances in which identities are used can vary immensely. This would probably lead to inequity between stakeholders and inefficiency in the market. The problem could also be exacerbated by the technical constraints of the transaction environment. Secondly, this approach may require too much effort or access to information on the part of the users: not everyone will be active enough, or well-informed enough, to adequately manage her personal identity data in all circumstances. The most ICT-savvy users would possibly be ready and willing to manage this information, but this would not be the case for all users. Thirdly, there is a significant contrast between user-stated privacy attitudes and their actual privacy-related behaviour. In general, it may be unreasonable to expect complete individual rationality in the context of online transactions. Models of self-control problems and immediate gratification studied by some scholars may offer more realistic descriptions of users' decision-making processes, and explain why even individuals who genuinely want to protect their privacy might not do so. These risks become even higher when the individuals concerned do not perceive the risks resulting from not protecting their privacy as significant.<sup>iii</sup>

As an example of the contrast between user attitudes and user behaviour, Acquisti et al. have conducted an experiment for two scenarios: willingness to pay for protecting personal information, and willingness to accept a proposal to sell information. Their results show a clear preference for money over data across the vast majority of participants in both information protection and information release scenarios, even when the monetary advantage is low. In addition, the average willingness to accept (the second case) is dramatically higher than the average willingness to protect.<sup>iv</sup>

Acquisti et al. have also studied why consumers do not always act as rational agents. Their research confirms that consumers often lack enough information to make privacy-sensitive decisions and, even with sufficient information, are likely to trade off long-term privacy for short-term gains. The three most important reasons for consumers not to act rationally are incomplete information, bounded rationality (inability to process and act on vast amounts of data), and systematic psychological deviations from rationality. The latter includes the tendency to favour immediate gratification to future benefit, the possibility to avoid loss being more important than the possibility to win a profit (of the same magnitude), notions of altruism, and fairness instead of private gain.<sup>v</sup>

Spiekermann et al. conducted an experiment in which they compared the self-reported privacy preferences of 171 participants with their actual behaviour during an online shopping episode. Their findings suggest that current approaches such as legislation to protect user privacy may not do so effectively, since they assume that consumers are privacy conscious and act accordingly. In the study it was found that most people did not live up to their self-reported preferences, and in fact tended to respond to the majority of questions asked from them during an online shopping session, even if they were highly personal. The varying privacy statements on different websites had no impact on the type of information disclosed. This suggests that people are prone to disregard privacy concerns once engaged in a transaction.<sup>vi</sup>

To conclude, to deal with identity as a consumption good contributes to our understanding of economics of identity according to classical and behavioural economics. It is market-centric: the cost of identity provision can be understood to be borne by the market, i.e. the highest bidder will manage "my" identity. A significant drawback of this approach is that it requires some idealised assumptions about user behaviour, and how users behave in real life may not conform with theory.

### **Identity as a capital asset**

We can also discuss **identity as a capital asset**. In this case, identity is regarded a property that can be publicly traded. Identity will have a changing value over time and space, because people's valuation of their identity changes with time and social context. When identity is understood as property, the value of pieces (i.e. value of identity in different contexts) does not equal the value of the ensemble. Therefore, the changing value of identity is considered both over time (time inconsistency in value of identity, deferred rewards) and over space (people value their identity differently in different social spaces, use of identity changes the value of identity).

In common with the understanding of identity as a consumption good, 'identity as a capital asset' recognises the changing value of identity data in different use contexts. It also allows for the time value of identity, recognizing the fact that the same person may place a drastically different value on his personal identity data purely because time has passed and this information has a different value in the new situation. This approach also recognises the fact that the value of identity can change when it is used, and may increase or decrease in value depending on the changes caused by the use.

Understanding identity as a capital asset carries with it a number of challenges. Firstly, there are obvious difficulties in measuring the value. There is also the risk of misrepresentation. This may occur through an erroneous combination of parts of the whole by not recognizing all value-generating aspects of identity, or by considering

only the most recent information and ignoring what was done a long time ago. We must also take into account the difficulties in predicting future behaviour, which mean that to estimate the value of identity in future carries with it a large inherent risk. All these challenges mean that to analyse identity as a capital asset, though in theory feasible, can in practice result in unreliable estimates of its value.

However, the *dynamics* of identity as a capital asset can be studied through behavioural economics and game theory. In his paper, Cave (2004) discusses the economics of trust according to some simple game theoretic models of specific aspects of trust, in order to analyse how balanced and efficient they are. He discusses the potential tension between efficiency and equilibrium, both in terms of the prevalence of trust behaviour and the network of relationships to which the need to trust others gives rise. In addition, he seeks to identify conditions under which different levels of trust may be widespread and conditions under which a diversity of behaviour is likely. One unexpected consequence of the latter conditions is the existence of ‘catastrophes’ – discontinuous jumps in the level of trust in response to small changes in underlying conditions.<sup>vii</sup> Acquisti et al. have also carried out trust modelling for online transactions. The increasing amount of spam, phishing and other attacks increase users' uncertainty over the consequences of their actions and their distrust towards other online parties. From this starting point, they have developed a theoretical model to represent and compare the online trust decision processes of users, though they do not give any direct results of user behaviour.<sup>viii</sup> Furthermore, Ba et al. have discussed the problem of uncertain quality in electronic commerce transactions. They investigate how the trust necessary for online exchange of products and services can be promoted when individuals have short-term temptations to cheat. As a solution, they propose a design of an economic incentive mechanism that serves to encourage consumer confidence in conducting online business transactions.<sup>ix</sup>

On the whole, understanding identity as a capital asset is a valuable addition to theory, especially with regard to changes in the value of identity according to its use and the passing of time. It also helps us understand the dynamics of economics of identity in different use contexts. A significant limitation is that it requires a very high amount of data to yield accurate results about the economic value of identity. It is worth noting that when we deal with identity as a capital asset, the cost of identity provision rests primarily with the individual. In this respect, this approach clearly differs from understanding identity as a consumption good.

### **Identity as a social good**

The third way to analyse economics of **identity is as a social good** (where the esteem and reputation of a person have economic externalities). In this case, identity (or to be more precise, aspects of the personal identity data of individuals) is understood to have network effects, meaning that identity increases in economic value by its increased use (by companies, by people). If identity is understood as a social good, one question to ask is if identity is to be publicly provided, and as such cannot be used in transactions. In this case, it would mean that identity is permanent: one (nationally provided) identity would stay with the citizen for the duration of his life. Another possibility for the provision of identity is that it be provided by a collective of persons or organisations. This would mean expanding the concept of identity to groups, i.e. not only individuals, but also social networks composed of individuals

would have identities of their own. New research activity has emerged around analysing social networks and studying "communities of interest"; this research field has largely been driven forward by sociologists, though there is also relevant work by economists such as Amartya Sen<sup>x</sup>. 'Identity as a social good' can most gainfully be applied to social networking sites (SNSs) such as Facebook and mySpace.

Identity as a social good is a valuable point of view especially because it provides tools to understand the *network effects* of personal identity data. It gives insights into how the value of identity increases as more people use it, and as it becomes more widely diffused. It gives us a means to analyse how SNSs actually function from an economic point of view, by explaining the means through which they provide economic value to their users. The central concept here is that of *reputation*: how other people's perception of what you are like affects their relations with you, and the resulting economic value of these relations.

While this understanding of identity has several advantages, there are also some moot points. First, it leaves unclear the role of the identity provider. As discussed above, if it is provided publicly, identity cannot then be analysed as a transactional good. It would also be unclear whether identity would be a permanent or temporary one; hence, this understanding leaves open questions of the time value of identity. Second, this approach does not address questions of collective identity, or what their dynamics would be like. To understand the collective aspects of identity is essential to any comprehensive analysis of identity, since so many of today's transactions are carried out between groups or organisations, not individuals.

Some research exists on what kind of information citizens wish to share and what they wish to keep to themselves. For example, Varian has argued that consumers will *rationally* want certain kinds of information about themselves to be available to the public, but other types not (e.g. financially sensitive information). Varian says that there are cases where there is a public interest in having some personal information publicly available; making information available about owners of motor vehicles may ensure their safer operation. In these cases, the public does not really care about *your* personal information, but desires access to the information because it is relevant to *their* interests.<sup>xi</sup>

Overall, analysing identity as a social good brings valuable contributions to our understanding as it introduces network effects and the changing value of identity (according to esteem and reputation) into the discussion. However, by itself this is not sufficient, as the analysis for the most part does not take into account the transactional nature of identity. Further, when we discuss identity as a social good, its value increases with its diffusion in the network, while its cost stays the same; in other words, the more you use your identity data, the more added value you are able to gain from it. This has a tendency to boost the use of the data by citizens, thereby contributing to the growth of the market. However, as the use of identity data increases, so do the associated problems.

### **Identity as a cost**

Finally, the conventional way to understand **identity** is purely **as a cost**. This means that the economic value of identity is only recognized as far as it incurs costs for the different stakeholders (governments, companies, consumers). For example, the costs of privacy enhancing technologies have been studied in this context. Another



possibility is to look at costs of identity theft: what is the economic loss, both direct and indirect, caused by the theft of people's online identities. Governments, for example, incur huge infrastructure costs to protect their identity management systems from unauthorised access. In this approach to economics of identity, the concept of cost has at least two meanings: the cost of what people have lost, or the cost they have to pay in order to protect their identity.

The key benefit of this approach is that it allows us to distinguish and study the various identity related costs. The main limitation is equally obvious: the identity related benefits are not considered. However, the costs associated with identity are much easier to estimate than the gains, which makes studying them worthwhile, if only to help us understand how much identity related transactions would have to contribute to the economy to offset the related costs. Therefore, the cost of identity provision will most likely be borne by the market, through the benefits brought about by increased security and control.

As an example, some scholars have studied the cost of privacy breaches in terms of their impact on the company's market value. These studies show that there is a negative correlation between data breaches and the company's market value. Although initially significant, the effect decreases and loses statistical significance rather quickly (even within days), suggesting that the public will quite rapidly recover its confidence in the company.<sup>xii</sup>

Another example of analysing identity as a cost is the economics of malicious software (malware). While its origins clearly lie in criminal behaviour, some scholars have argued that the magnitude and impact of the malware threat have also been influenced by the decisions and behaviour of legitimate market players such as ISPs, software providers, hardware vendors and consumers. Namely, in many cases these stakeholders may not be adequately incentivised to operate in ways that contribute to the highest possible security, and there may even be market-based incentive mechanisms that contribute to misuse of information. For example, it is often very easy for companies to collect information about their customers, their preferences, habitual ways of using the system, and so on; while this information may be appropriately used by, financially beneficial for, the company in question, there is always the possibility of a third party finding out this information and using it for illegal purposes.<sup>xiii</sup>

In this context, Laudon (1997) has studied market mechanisms of pricing information. He posits that the crisis in the privacy of personal information is a result of market failure, not rapid technological development. He believes this to be a market failure, which has occurred as a result of a poor allocation of personal property rights: the collector of the information has too many rights, the individuals concerned too few. While the financial rewards for privacy invasion can be huge for companies, the individuals do not understand how their personal data will be used, the means of individuals for obtaining information about the use of data are limited, and the costs of finding out this information can be very high.<sup>xiv</sup>

Hann et al. (2002) have studied the value of information privacy in the presence of potential benefits from sharing personal information. They found that the potential benefits, both direct monetary rewards and future convenience, significantly affect user preferences in relation to the use of websites with different privacy policies. They also investigated the monetary value of website privacy protection, and

estimated that among US subjects in September 2002, the value of protection against errors, improper access, and secondary use of personal information is between \$30 and \$45 per person annually.<sup>xv</sup>

Furthermore, Andrew Odlyzko has studied security as a component of a complex economy (not as an isolated good). In his view, it follows that security can never be optimally effective, but instead will always be subject to severe constraints created by other parts of the economy. He further argues that the interactions of human society and human nature suggest that security will continue to be applied as an afterthought, not as a primary design goal of ICT systems. Therefore, it would be most productive to think of security not as a way to provide ironclad protection, but as the equivalent of speed bumps, which decrease the velocity and impact of electronic attacks to a level where other protection mechanisms can operate.<sup>xvi</sup>

On the whole, the definition of identity as a cost does not really deal with identity, but more with privacy and data protection. The positive, i.e. value-generating, effects of identity are not taken into account, which makes this definition somewhat unsatisfactory. However, this approach can be used to highlight the fact that the cost of identity provision could (and probably should) be borne by the associated benefits such as increased security and better control of the use of identities.

#### Summary of different approaches

In the table below we summarise the benefits and limitations of each approach to economics of identity, with special emphasis on the consequences that each one has for the analysis of economic externalities.

**Table 1. Benefits and drawbacks of various approaches to understanding economics of identity.**

|                              | <b>Consumption good</b>                                                                                                                                                                                                                                     | <b>Capital asset</b>                                                                                                                                                                                                                                                       | <b>Social good</b>                                                                                                                                                                                                                                      | <b>Identity as a cost</b>                                                                                                                                                                                             |
|------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Benefits for analysis</b> | <p>Identity as a transactional good: different externalities depending on type of transaction</p> <p>Changing value of identity according to context: identity as a 'market good'</p> <p>Identity chosen and managed by the user, who gains control and</p> | <p>Identity as a transactional good: economic externalities vary depending on type of transaction and user actions</p> <p>Changing value of identity according to context: identity traded in the public marketplace</p> <p>Time value of identity: time factor can be</p> | <p>Economics of esteem and reputation: analyses the economic value of how we (our identities) are appreciated by others</p> <p>Network effects of identity: explains how increased use and recognition of identity contribute to the economic value</p> | <p>Distinguishes between different identity related costs and explains how each affects the identity's value</p> <p>Provides estimates of costs for privacy enhancing software, online fraud, identity theft etc.</p> |

|                                 |                                                                                                                                                                                                                                                                                                                       |                                                                                                                                                                                                                                                                                           |                                                                                                                                                                                                                             |                                                                                                                                    |
|---------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|------------------------------------------------------------------------------------------------------------------------------------|
|                                 | <p>ownership</p> <p>A solid theoretical basis from classical economics</p>                                                                                                                                                                                                                                            | <p>introduced to economic analysis</p> <p>Changing value of identity according to its use; helps understand fluctuations in value of identity</p> <p>Recognises that value of pieces <math>\neq</math> value of all; value can be measured in specific cases without analysing others</p> | <p>of the system</p> <p>Analysis of economics of SNSs; how do such companies generate value?</p>                                                                                                                            |                                                                                                                                    |
| <b>Draw-backs</b>               | <p>Results in very complex identity markets; hence limited possibilities to understand and regulate the market</p> <p>Requires significant effort from user; what are the user liabilities in case of misuse of identity?</p> <p>Privacy paradox: users are less concerned by their privacy than they claim to be</p> | <p>Difficulties in measurement; possible lack of reliable financial data</p> <p>Difficulties in recognising all value-generating aspects of identity; a lot of groundwork to be done before economic analysis</p> <p>Requires many assumptions about users' future behaviour</p>          | <p>Does not clearly define the role of identity provider: it is not clear who controls the identity data and how, and how they will be affected by economic externalities</p> <p>Does not address collective identities</p> | <p>Only analyses the costs, not the value-generating aspects of identity; thus the analysis will only provide "half a picture"</p> |
| <b>Cost to provide identity</b> | <p>Will be borne by market or company, enabling the use of more advanced e-services</p>                                                                                                                                                                                                                               | <p>Will be borne by user, who retains control and ownership</p>                                                                                                                                                                                                                           | <p>Bearer unclear; should decrease the more identity is used</p>                                                                                                                                                            | <p>Should be offset by increased security, control, etc.</p>                                                                       |

## CASE STUDIES

In this chapter, we analyse the activities of three companies as practical examples of how different approaches to economics of identity can be used to understand the identity market. For our analysis, we have chosen BBS, eBay and IdenTrust because they have three clearly different product and service offerings and three distinct ways of operation. BBS is used to illustrate identity as a consumption good, eBay identity as a social good and IdenTrust identity as a cost.

### **BBS Global Validation Service<sup>xvii</sup>**

BBS is a Nordic company offering identity solutions to manage risks and provide certification services. Their service offering includes managed public key infrastructure (PKI), managed one-time passwords, validation services, smartcards, and tokens. These services are accepted by several government organisations in addition to the marketplace, which distinguishes them from other similar services. This is a significant development, given that governments in general are very wary of accepting commercial credentials and instead prefer to rely on their own solutions. As the security standards of the commercial products are constantly improving, this lack of acceptance may be more of an issue of suitability of commercial credentials for governmental purposes, rather than concerns about their lack of reliability.

In general terms, international companies need to handle the complexity of verifying different kinds of signatures and to validate certificates from various issuers worldwide. This is the main challenge that BBS seeks to address. They offer validation services that seek to solve the complex problem of offering signature verification and certificate validation as a service for the receiving party. In this way, their customer can obtain a solution designed to manage different signatures and certificates worldwide. Effective use of digital signatures, especially across national frontiers, reduces costs and complexity of using PKI in global e-business. The service also effectively helps to connect different closed eID communities. Ultimately, BBS aims to function as a single, independent trust provider, which offers one set of standards and one software package for processing of signatures and certificates, as well as effective risk management for using PKI in global business transactions.

BBS operates in two distinct segments of the eidentity market: they offer multi-purpose ID schemes for heterogeneous citizen-merchant markets, and tailored PKI solutions, with more stringent security parameters, whose users are typically enterprise customers with transactions taking place in closed environments<sup>xviii</sup>. The most important product of BBS is the Identity Management Platform. Developed in 2008, it is used for issuing, managing and using digital certificates online. It can handle different Certificate Authority (CA) platforms and validation technologies, thereby providing BBS with the flexibility to adapt their certification to the specific needs of individual customers and transactions. The BBS Identity Manager is used to provide all their identification services, including enterprise PKI, mobile PKI, EU-qualified and standard certificates. It can also be used to provide one-time passwords and validation of individual transactions. Because of these characteristics, the BBS Identity Management Platform works well as an example of identity as a consumption good. The service incorporates the nature of identity as a transactional good, something that can easily play one role in a certain context and a different one in

another. Moreover, these services take into account the changing value of identity depending on the type of transaction, and accordingly there are different types and levels of security for specific transactions as appropriate. In general, BBS services have been developed with a modular design, allowing their customers to choose the most appropriate combination of identification mechanisms.

The activities of BBS in these markets are complemented by their participation in international expert groups such as European Committee for Banking Standards (Mobile Payments Workgroup) and Mobey Forum (Mobile Authentication and Business Ecosystem), and standardisation groups such as European Payment Council (EPC) and European Committee for Banking Standards (ECBS). Their participation in these bodies enables them to offer identity solutions that fit better with specific use cases and transactions, as well as influence the future development of the industry.

When we analyse identity as a consumption good, identity is something chosen and managed by the user. In the BBS case, the customer company gains control and ownership of the certified identity, enabling them to manage the identity according to their particular needs. This also means that the customer company can use several identities and sets of identity data. In this situation, it is obvious that the value of identity depends on the transaction and context it is used in; the identity may even be part of the transaction itself, as befits this school of thought, though this is not explicitly specified by BBS.

Even though the customer company manages its own identity, we must bear in mind that BBS, as the identity provider, has a large role in assisting the customer choose the form of identity to be used. This may in practice lessen the influence that the customer company has over the choice and use of their identity. However, it is always the customer who makes the ultimate decision, with BBS having just an advisory and supportive role. The large role of the provider may also be an advantage: as discussed in this paper, one of the key drawbacks of analysing identity as a consumption good is that it requires significant effort from the user, but in this particular case the effort is mediated by BBS.

The activities of BBS also go some way towards addressing the privacy paradox: although users are generally less conscious of their information security than they claim to be, a company such as BBS helps them see the risks more clearly and manage them appropriately. We might even say that such companies are *needed* because their customers don't understand the risks well enough. Hopefully, this state of affairs will change over time as both personal and business users become more conscious of the benefits and risks associated with online identification; however, at the moment, companies like BBS still have a useful role to play/

In the business model of BBS, the cost of identity provision rests with the customer companies, as they need the electronic identities to provide their financial services. Generally, these companies are able to charge these costs from their own customers in the form of service fees and the like, so ultimately the cost of identity provision rests with the market. In this way, too, the BBS services deal with identity as a consumption good.

### **eBay<sup>xix</sup>**

eBay is a US-based company specialising in online auctions and sale of nearly any type of merchandise. In eBay, each seller has his own profile that is rated by the

people who have bought products from this particular seller. The most highly rated sellers acquire the status of "Power Seller", while lowly rated sellers may be excluded from eBay altogether. In this way, eBay closely resembles any social networking site with significant user interaction and rating of individual users by their peers.

The key to operations of eBay is the economics of reputation. It is not possible for the buyer to directly examine the product, and so he must rely on whatever information he can get of the seller when deciding on how to bid. The way a particular seller handles his sales, how reliably he ships the purchases, how promptly he answers requests from information, and so on, all affect his rating in eBay. Therefore the identity of a user has a particular value in eBay; the higher the rating, the higher the value of user identity. This is in line with considering identity as a social good.

Several studies have been made on how to quantify the value of the identity in eBay. Resnick et al. conducted an experiment in which a high-reputation, established eBay dealer sold matched products both under his regular identity and under new seller identities, which were in reality also operated under him. As predicted, the established identity fared better. They found that the difference in buyers' willingness-to-pay was 8.1% of the selling price. They then conducted a second experiment in the same format, but compared sales by relatively new sellers with and without negative feedback. Surprisingly, they found out that one or two negative feedbacks for the new sellers did not affect willingness-to-pay.<sup>xx</sup> Melnik et al. have made a similar empirical study of the value of the seller's reputation in eBay. Their conclusion is that the seller's reputation has a positive and statistically significant, but small, impact on the price.<sup>xxi</sup>

The rating structure of eBay generates network effects, which are a cornerstone of understanding identity as a social good. As the ratings of individual sellers change, the ones with higher ratings are likely to attract more business with regard to peers who have the same product. If users buy more from a particular seller because of his high rating and are satisfied, they may then rate the seller highly, boosting his rating yet again. Conversely, low ratings may generate distrust and a tendency to rate a seller lowly even if he does not "really" deserve it, thus creating a polarising effect. People tend not to form their opinions in a vacuum, but instead rely heavily on the opinions and prejudices of other people. These network effects are often magnified online, as people have access to the opinions and experiences of a much higher number of people than would be possible in the physical world. In effect, eBay functions as a trusted third party who "guarantees" the credit ratings of individual sellers. By providing its credit rating information, they give buyers and sellers the confidence to trade with unknown trading partners, improving market liquidity.<sup>xxii</sup>

When analysing identity as a social good, a significant drawback is that it often leaves some important questions unanswered. For instance, it does not address the question of collective identities; in eBay, by analogue, there is no possibility for such an actor as a "collective seller". Similarly, the eBay example can only be used to understand the economic value of identities of individual actors. Also, there may be issues of too strict or too lenient ratings by buyers, meaning that two sellers with similar products cannot be directly compared.<sup>xxiii</sup>

In this particular school of thought, the bearer of the cost of identity provision is not specified. However, in the eBay business model the bearer of this cost is very

clear, as it rests squarely with the user. This is the case because eBay charges a fee both for placing an item for sale and for each transaction, generating income according to economic value and number of products.

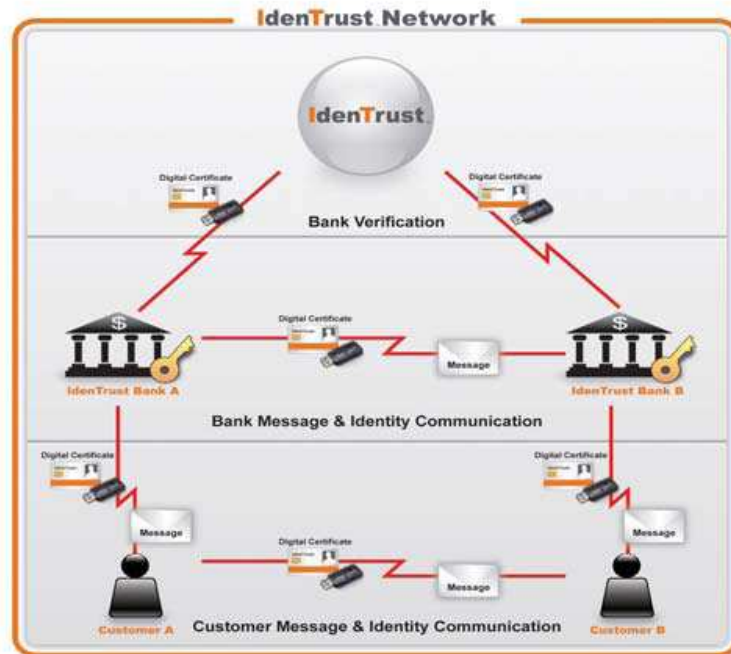
### **IdenTrust<sup>xxiv</sup>**

IdenTrust is a technology provider whose main product is a PKI-based identification system, used both by governments and private companies, with the finance sector as their main client. They issue credentials and provide a supporting infrastructure including operational, technological and legal services. The IdenTrust credentials are designed to provide three key capabilities: authentication (provision of identity), encryption (safeguarding content, eliminating unauthorised access) and digital signing (user-level signatures of specific transactions).

The IdenTrust credentials are designed to provide three key capabilities: authentication (provision of identity), encryption (safeguarding content, eliminating unauthorised access) and digital signature (user-level signatures of specific transactions). In addition, IdenTrust credentials are designed to comply with relevant anti-money laundering or other anti-abuse regulations (i.e. Sarbanes-Oxley and HIPAA health data regulations).

IdenTrust products enable companies make authentication an integral part of their business processes and so to be able to conduct their operations reliably and securely over the Internet beyond fulfilling their legal obligations. IdenTrust products rely on an open standard that can be used by financial institutions to gain interoperability and legal acceptance in 120 countries. The membership of the IdenTrust network is restricted to institutions that agree to abide by the conditions set by IdenTrust, thereby ensuring that the standard is utilised in an appropriate manner. IdenTrust policies govern who receives the identity and how each individual or business is vetted to guarantee they really are who they say they are, along with making certain that the process is done consistently everywhere around the world. IdenTrust identities encrypt and control the process flows, in order to prevent the interception of a transaction, in this way combating phishing and man-in-the-middle attacks.

The Trust Network operates as follows. It first specifies how a digital identity certificate can be issued and how it is validated. The transaction data and signed certificate are exchanged between the stakeholders involved in the transaction. The messages related to the transaction data are exchanged between the customers on either end of the transaction. IdenTrust only validates the identities used by these customers, not the data associated with the transaction. The transaction data itself is never passed to IdenTrust; the only information IdenTrust receives and sends back to the banks is validation of participant identities. All individuals and systems using the network are identified using IdenTrust digital certificates.<sup>xxv</sup>



**Figure 1. Functioning of the IdenTrust Trust Network.** (source: IdenTrust, ref. #25)

Overall, IdenTrust supplies the technology and legal mechanisms to let Internet trading partners trust in another's identity. This enables their customer companies to use the Internet to open new markets, reduce transaction costs and create auditable records of their transactions. Hence the costs incurred by identity products are ultimately beneficial or even necessary for such companies, even if they at first look appear as a cost alone.<sup>xxvi</sup>

Nevertheless, the primary benefit of analysing the IdenTrust products and services is that it helps us understand in detail the economics of identity as a cost. The IdenTrust products differentiate between costs associated with electronic identification: the PKI technology itself, infrastructure, support services, service setup and management, as well as specific transactions for which credentials are needed. In addition, the IdenTrust products can also be used to provide estimates of the costs more specific identity related issues, such as protection against online fraud, or the setup of an account for a particular purpose. Once the different types of identity related costs are distinguished, they become easier to quantify, though arriving at exact figures remains very challenging.

The obvious drawback of looking at identity just as a cost is that the positive value of the identification services is, quite often, not fully recognised. Instead, it is taken (almost) for granted that companies will need to purchase these services as a regular part of their operations. While this may be true, this lack of recognition of the value-



generating aspects of identity could mean that companies such as IdenTrust are unable to fully capitalise on the economic possibilities of electronic identity. Hence, we can say that looking at identity from a pure cost perspective is viable only as a partial approach. It is helpful in assessing the related costs, but to arrive at a fuller understanding of economics of identity, methods and insights from other schools of thought are also needed.

In this approach, the cost of its provision will be paid for by companies purchasing the services from IdenTrust, but will ultimately be charged to their customers. Whether the client companies need an electronic identity of a certain kind and level of security to comply with governmental regulations, to satisfy their customers' expectations, or to be able to run their operations more efficiently and attract more business, the advantages brought about by the services offset the cost of the identification services. Therefore the economic benefits of the eidentity services are always implicitly recognised.

## Conclusions for policymakers

It is evident that the various economic approaches allocate a different, but by itself incomplete, function to identity as an economic object. Consequently, we believe that none of the approaches suffices by itself to analyse economics of identity in a satisfactory way. Instead, this can only be achieved by combining the understandings and methodologies of each one.

Each of the schools of thought has specific consequences for regulators and other policymakers, both on a national and European level. As discussed above, the traditional approach is to treat identity as a cost. This has the advantages of **making policymakers aware of the magnitude of identity-related costs** as well as the fact that there must be significant benefits to render positive the overall economics of deploying identity infrastructures. There is a wide variety of economically significant identity, privacy and data protection issues, recognised by identity management companies such as IdenTrust, and who seek to address these issues through their product portfolios, including the identification and measurement of the various associated costs. By following the activities of such companies and the markets they address, it becomes **easier for policymakers to monitor the various identity related costs in different markets**, and consequently formulate suitable policy actions in each of them.

Understanding identity as a consumption good or as a capital asset both have the advantage of **emphasizing the transactional role of identity**. In many transactions, it is not necessary or even appropriate to link a participant to a transaction with a specific living individual. For example, in cash transactions, the buyer only has to be in possession of a sufficient amount of money, not to reveal her identity; while in other cases it may be necessary for either the buyer or the seller to identify herself. In yet other transactions, identities themselves form a part of the transaction. Companies such as BBS function as identity providers for all these different types of transactions, while their customer is the stakeholder that ultimately remains in control of (and responsible for) the actual use of the identities. What this means for policymakers is that they have to be prepared to recognise the various ways in which personal identity

data is used in different transactions, and be ready to adopt regulatory measures most suitable to each particular situation.

However, one difficulty with this understanding of economics of identity is that it is not always easy for users to understand how their personal identity data are used. This issue is made more serious by the privacy paradox: the fact that users are in practice not as conscious of privacy implications of transactions as they claim to be. This is already partly addressed by BBS and other identity providers: these companies offer identity management and support services precisely because their customers need advice on how to manage their identities and identity data more securely and efficiently. However, as valuable as the corrective actions within the marketplace are, these issues also need to be addressed by policymakers. They should **make it as easy as possible for business and citizens to manage their personal information**. This can take place by improving citizen awareness, by providing them accurate and reasonably detailed (but not overly so) information about electronic identities and personal data management, and by making it necessary for companies to clearly disclose their privacy policies and practices.

Analysing identity as a capital asset has the particular advantage of acknowledging the various roles, and hence economic values, that an electronic identity can have depending on the situation. As the value of identity changes according to the extent of its use and the passing of time, so do the ways in which the identity generates value. However, this granularity complicates things for policymakers: it can be difficult just to recognise all the different roles of identity, let alone to reliably measure the monetary value that each one may have. It is therefore **necessary for policymakers to create appropriate tools**, both conventional and novel, **to measure the value of identity in different situations**. This should include the monitoring and quantitative analysis of the activities of the major players in the marketplace, including IdenTrust and BBS. Only this makes it possible to accurately analyse identity as a capital asset.

Finally, when identity is considered as a social good, the main benefit that emerges from this approach is **recognising the economic value of identity in social networks**. By analysing how and why the value of identity increases as more stakeholders become aware and use it in transactions, for example in the business models of eBay and other online retail companies, policymakers become more conscious of the ways in which the identity of one stakeholder can interact with those of others, and how these interactions create value in the whole network. However, for this kind of analysis to be possible, it has to be clearly defined who the provider of identity actually is (e.g. state or private, which private stakeholder), and how the identity can in practice be used in transactions. The eBay business model is again useful for understanding these issues better, because it very clearly demarcates the roles and varying responsibilities of buyers, sellers and the service provider itself.

## References

---

<sup>i</sup> G. A. Akerlof and R. E. Kranton, "Economics and Identity," Quarterly Journal of Economics 115.3 (2000).

<sup>ii</sup> Ben Fine, "The Economics of Identity and the Identity of Economics?," Cambridge Journal of Economics Advance Access.October 26, 2008 (2008), J. B. Davis, "Akerlof and Kranton on Identity in Economics: Inverting the Analysis," Cambridge Journal of Economics 31.3 (2007).

<sup>iii</sup> Alessandro Acquisti, "Privacy in Electronic Commerce and the Economics of

Immediate Gratification," (H. John Heinz III School of Public Policy and Management, Carnegie Mellon University), vol. 1.

<sup>iv</sup> Alessandro Acquisti and Jens Grossklags, "When 25 Cents Is Too Much: An Experiment on Willingness-to-Sell and Willingness-to-Protect Personal Information," Workshop on the Economics of Information Security 2007 (2007), vol. 1.

<sup>v</sup> Alessandro Acquisti and Jens Grossklags, "Privacy and Rationality in Individual Decision-Making," Workshop on the Economics of Information Security 2004 (2004), vol. 1.

<sup>vi</sup> Sarah Spiekermann, Jens Grossklags and Bettina Berendt, "E-Privacy in 2nd Generation E-Commerce: Privacy Preferences Versus Actual Behavior," Electronic Commerce Conference 2001 (Tampa, USA: 2001), vol. 1.

<sup>vii</sup> Jonathan Cave, The Economics of Trust between Cyber Partners (London: ForeSight - UK Department for Innovation, Universities and Skills, 2004). Also Jonathan Cave and Chris Marsden, "Quis Custodiet Ipsos Custodes in the Internet: Self-Regulation as a Threat and a Promise," 36th Research Conference on Communication, Information and Internet Policy, 26 - 28 September 2008 (George Mason University School of Law, Arlington, VA: 2008), vol. 1.

<sup>viii</sup> Alessandro Acquisti, "Trust Modelling for Online Transactions: A Phishing Scenario," Privacy, Security, Trust Conference 2006 (2006), vol. 1.

<sup>ix</sup> Sulin Ba, Andrew Whinston and Hang Zhang, "Building Trust in the Electronic Market through an Economic Incentive Mechanism," International Conference on Information Systems (1999), vol. 1.

<sup>x</sup> Amartya Sen, Identity and Violence: The Illusion of Destiny (Penguin Books, 2007).

<sup>xi</sup> Hal Varian, "Economic Aspects of Personal Privacy," (UC Berkeley, 1996), vol. 1.

<sup>xii</sup> Alessandro Acquisti, "Is There a Cost to Privacy Breaches?," International Conference on Information Systems 2006 (2006), vol. 1.

---

<sup>xiii</sup> OECD, Economics of Malware: Security Decisions, Incentives and Externalities (2008).

<sup>xiv</sup> Kenneth Laudon, "Extensions to the Theory of Markets and Privacy: Mechanics of Pricing Information," (New York: Leonard N. Stern School of Business, New York University, 1997), vol. 1.

<sup>xv</sup> Hann Il-Horn, Kai-Lung Hui, Tom S Lee and I P L Png, "The Value of Online Information Privacy: Evidence from the USA and Singapore," (Marshall School of Business, University of Southern California

Department of Information Systems, National University of Singapore, 2002), vol. 1.

<sup>xvi</sup> Andrew Odlyzko, "Economics, Psychology, and Sociology of Security," (Digital Technology Center, University of Minnesota), vol. 1.

<sup>xvii</sup> <http://www.bbs-nordic.com/>

<sup>xviii</sup> Bishwajit Choudhary, "European E-Id Services: Future Trends and Nordic Experiences," FST Europe (2010).

<sup>xix</sup> <http://www.ebay.com/>

<sup>xx</sup> Paul Resnick, Richard Zeckhauser, John Swanson and Kate Lockwood, "The Value of Reputation on Ebay: A Controlled Experiment " Experimental Economics 9.2 (2005).

<sup>xxi</sup> Mikhail I Melnik and James Alm, "Does a Seller's Ecommerce Reputation Matter? Evidence from Ebay Auctions," Journal of Industrial Economics L.September 2002 (2002).

<sup>xxii</sup> B. Mahadevan, "Business Models for Internet Based E-Commerce: An Anatomy," California Management Review 42.4 (2000).

<sup>xxiii</sup> Chrysanthos Dellarocas, "Analyzing the Economic Efficiency of Ebay-Like Online Reputation Reporting Mechanisms," 3rd ACM conference on Electronic Commerce (Tampa, USA: 2001), vol. 1.

<sup>xxiv</sup> <http://www.identrust.com/>

<sup>xxv</sup> IdenTrust, The IdenTrust Rule Set:Providing Secure Identities While Protecting Privacy (London: IdenTrust, 2007).

<sup>xxvi</sup> IdenTrust, Identity Authentication as a Critical Growth Strategy (London: IdenTrust, 2007).