

The Economic Models of On-Line Digital Identity, Identity Management Systems and Service Interconnection Policy

Junseok Hwang and Alexandre Repkine

junhwang@snu.ac.kr

Seoul National University, Techno-Economics & Policy Program, Seoul, Korea

Abstract

It is rather obvious that the national governments have an important role to play in maintaining the structure of identity management systems ensuring the existence of a sound balance between the authentication requirements and consumers' rights to privacy (JHU, 2003). While it appears natural that more safety in transactions involving personal identification requires more information on consumers' identity (see e.g. Ogata et al., 2004) consumers will be also likely to be more reluctant to reveal their personal data as they are required for more such data to be revealed (Olivero and Lund, 2004). The focus of this paper is on investigating this type of tradeoff by employing a theoretical framework with agents whose utility depends on the amount of private information revealed, and on making policy recommendations related to the issue of interconnection between alternative IMS-s.

We developed a theoretic economic model of identity management systems and provide a framework permitting an analysis of the social, economic and technical issues raised by the emerging IMS-s and their interconnections. The resulting theoretical model yields several inferences and policy implications stemming from the predicted relationship between private and social optima with respect to the service interconnection issue.

JEL - Codes: L14, D85, D78, L25, L43, L51

Keywords: Networks, Interconnection, Identity Management, Regulation Policy, Information Security and Privacy Policy

A. Introduction

Identifiers and identity management systems (IMS) are attracting a growing amount of attention from business, government and technologists. (Clarke 1994; Bechtold 2002; Computer Science and Telecommunications Board 2002; Greenwood, Combs et al. 2002) By “identifier” we mean any name, number or token that distinguishes one human being from another on a network or in an information system; examples would be E-mail addresses, Social Security Numbers, and employee or student ID numbers or cards, among many others. By an “identity management system” we mean any infrastructure designed for making identities operational in the processes of authentication, data storage and retrieval and in mapping of identifiers to the information needed for identification and authorization.

Interest in this topic is well-founded. Solving the problems associated with identity management in the “virtual” world is proving to be one of the keys to full realization of the economic and social benefits of networked information systems. As one Internet technical veteran put it, "It's recently become clear that the software for managing user identity and authentication is one of the key building blocks of the emerging Internet operating system."¹ By definition, the virtual world lacks the rich combination of sensory and contextual cues that permit organizations and individual humans interacting in the physical world to reliably identify people and authorize them to engage in certain transactions or access specific resources. Being able to determine who an online user is and what they are authorized to do thus requires an identity management infrastructure. Some of the most vexing problems associated with the Internet (the deluge of spam, the need to regulate access to certain kinds of content, securing networks from intrusion and disruption, problems of inter-jurisdictional law enforcement related to online activities, impediments to the sharing of distributed computing resources) are fundamentally the problems of identity management. And yet, efforts by organizations and governments to solve those problems by producing and consuming identity systems may create serious risks to freedom and privacy. Thus the implementation and maintenance of identity management systems raises important public policy issues.

The emergence of such IMS-s often requires the users submitting substantial amounts of information about their identity, therefore it is natural to ask whether one can be sure if this information is used in

¹ Tim O'Reilly, founder and chief executive officer of technology publisher O'Reilly & Associates, quoted by Thor Olavsrud, “Sun's Vision: Network Identity Through Hardware,” siliconvalley.internet.com, March 12, 2002.

<http://siliconvalley.internet.com/news/article.php/990001>

an appropriate way, e.g. if all or specific parts of it are revealed or sold to the third parties, whether there is a chance for the identity information to be stolen or whether inferences on the details of one's identity not explicitly asked for can be made based on the submitted information that the users would not like to be made.

In light of these issues the issue of interconnection between several Identity Management Systems (the IMS) becomes important because it often involves sharing the individuals' private information between two or more IMS. One example of such sharing is given by Davis (2000). While the U.S. law forbids soliciting information on race and marital status by the credit issuing agencies, such information can be fairly easily obtained by the credit agency since this is contained public records that require the very basic information such as name and address for access. Other examples include the illegal revelation of private information by an Internet website to the third party in the violation of the U.S. privacy act (Kastenmeier, 1986) and the outright frauds such as the credit card fraud, selling out the information on one's bank balance, medical history or criminal records accounts of which can be easily found in the press. This study concentrates on the issues of government policy related to the legal interconnection deals between the IMS-s, thus leaving the juridical part of the problem out of the scope of the study.

In this paper, we find it most useful to approach the issue of interconnection between two or more IMS-s from the point of view of the networks literature (see a primer on it in Economides, 1996). We judge on the social desirability of alternative IMS structures by assuming that each one of these structures results in different levels of the consumer surplus. The differences in the latter result from the fact that, while soliciting more information from the consumers allow the IMS firms more opportunities to extract larger fractions of consumer surplus, it also results in the decrease of the level thereof since we assume our consumers are privacy-concerned so their utility does not increase indefinitely with the amount of private information they reveal. We model consumers' utility as a function of the extent of revealed partial identity (Clauss and Kohntopp, 2001) and build on the network interconnection model by Heal and Kunreuther (2002) to model the incentives of the identity management firms.

This paper is organized as follows. Section II starts with modeling the individual consumers' utility as a function of identity and proceeds with the description of incentives of the IMS firms. Section III derives and analyzes the outcomes predicted by the model developed in the previous section. Section IV discusses the issues of empirical applications of our framework to the real-world situations and Section V summarizes the paper and offers several policy implications.

B. Literature Review

As important as identity management is, a survey of the literature reveals an almost complete absence of scholarly research on its *economic* aspects. There is a strong tendency to view identity management primarily as a technical problem, and to devote most analytical attention to the choice between alternative technological architectures of IMS-s.² There is, however, a growing recognition among technical researchers of the need for research that bridges economic and technical analysis of security and identity issues. A short “position paper” by (Feigenbaum, Freedman et al. 2002), for example, describes the gulf that exists between research that solves technical problems in privacy/encryption and an understanding of how privacy-related technologies will actually be deployed in the real world. Real-world actors, the authors point out, are subject to economic incentives that may act as barriers to the deployment of “the best” privacy-enhancing technologies. A more sustained argument along the same lines is made in (Anderson 2001). Many [security] problems, he argues, “can be explained more clearly and convincingly using the language of microeconomics: network externalities, asymmetric information, moral hazard, adverse selection, liability dumping and the tragedy of the commons.” Ross makes a few observations about how Microsoft Passport’s IMS is as much an effort to control the web server and purchasing information market” as a security product. Both of these papers offer valuable observations about possible ways in which economic analysis might be relevant to understanding the deployment of identity management systems, but they do not develop models or systematic analyses of how economics may help clarify the issues related to IMS. Interesting but less directly relevant examples of attempts to bring economic analysis to bear on problems of technical security include (Anderson 2002; Varian 2002). There is also a growing policy literature on identity issues, but it is highly pragmatic and little if any of it is based on theory, except perhaps for the legal literature. (Clarke 1994) provides a very useful overview of some of the legal and economic issues of identity management. (See Froomkin 2002 for a good survey of legal opinion on identity issues)

Improving our understanding of the economic and cost features of identity management is important. Research into the unique economic characteristics of networks in the 1970s and 1980s set the terms for telecommunications policy discourse for the ensuing two decades. (Rohlfis 1974; Taylor 1980; Farrell and Saloner 1985) As digital identity systems become increasingly central to the aspects of online environment, the need for a scientifically grounded method of assessing the costs, benefits, industrial organization and policy consequences of various identity solutions also increases. Such an analysis will be needed to understand the sources of efficiency and inefficiency in identity management systems so that better systems may be designed. As emerging controversies over a national ID card

² As evidence, consider the standards work on security and interoperable identity and access management done by standards groups such as OASIS.

and Microsoft's Passport identity system make clear, the public policy makers will need to know how the digital identity industry is organized, understand what economic forces drive its market structure, and understand actual and potential sources of market failure. They will need to have a more fundamental understanding of the differences between governmental and private provision of identity and what advantages or disadvantages might be associated with either one of the two provision types. Policy makers will also need to be in a position to rationally assess the value of conflicting social claims related to identity management systems. For example, privacy versus convenience and security, or the risks of centralization versus the costs associated with the IMS-s' heterogeneity.

Designing policies aimed at regulating the type and/or the amount of personal information solicited from individuals is commonly referred to as identity management (Clarke, 2004). Although identity management has many aspects to it (e.g. prevention of identity theft or development of authentication requirements), we concentrate on the issue of multiple identities, or alternatively, the issue of the optimal choice of the structure of the identity management systems. Our choice is motivated by two factors. First, most existing literature on identity management concentrates on the supply-side of the phenomenon, such as security of access, authentication algorithms etc. Second, despite of the postulated necessity (OECD, 1980) for the consumers to be able to control the process of collecting and using their personal data, consumers are as yet not able to exercise sufficient control over the information they disclose. One reason behind the latter might be that the only lobbying party with respect to identity management appears to be the representatives of identity management systems themselves who are naturally interested in soliciting as much information from the consumers as possible. In particular, the issue of multiple identities has been receiving a considerable amount of attention in recent years. The focal point of discussion is the choice between an all-encompassing single identity management system that knows everything about everyone on one side of the IMS spectrum and a multitude of highly specialized small IMS-s that perform narrowly defined operations and solicit minimum information from each individual at a time. Such keen attention to the issue appears to be primarily caused by the fact that individuals as well as businesses get increasingly more concerned about the way their personal information is being solicited and used. Thus, the Microsoft Passport IMS fell far short of the expectations of its creators because consumers did not like the idea of a lot of personal information about themselves collected from different places be stored in one place on the one hand, and on the other hand, businesses who foresaw such unwillingness to take place were unwilling to pay thousands of dollars a year for access to the Passport services. Another salient example is the recent debates on the introduction of a single identifier in the countries of European Union and Australia. Especially in the latter case, recognizing all of the perils associated with multiple identities abuse, the Australian government has forsaken the idea of a uniform omnipotent identity card for its citizens.

An example of how unregulated interconnection may infringe on an individual's privacy is given by Davis (2000). While the U.S. law forbids soliciting information on race and marital status by the credit issuing agencies, such information can be fairly easily obtained by the credit agency since this is contained public records (e.g. Lexis-Nexis) that require the very basic information such as name and address for access. It is rather obvious that national governments have an important role to play in maintaining the structure of identity management systems ensuring the existence of a sound balance between the authentication requirements and consumers' rights to privacy (JHU, 2003). While it appears natural that more safety in transactions involving personal identification requires more information on consumers' identity (see e.g. Ogata et al., 2004) consumers will be also likely to be more reluctant to reveal their personal data as they are required for more such data to be revealed (Olivero and Lund, 2004). The focus of this paper is on investigating this type of tradeoff by employing a theoretical framework with agents whose utility depends on the amount of private information revealed, and on making policy recommendations related to the issue of interconnection between alternative IMS-s.

Clarke (2004) notes that "Many scheme designers fail to demonstrate any appreciation of the need that individuals have to sustain many identities, and to avoid linkage among them." The existence of multiple identities is often frowned upon as an inconvenience to individuals (hence the introduction of Microsoft Passport for example), with the role of multiple identities as a means of protecting people's privacy often overlooked. PINGID: "The issue is how to manage the linkage or sharing multiple identities." Liberty Alliance: "to gain access to portions of the user's identity information that may be distributed across multiple providers." Proponents of sharing: "consumers are concerned about need to have to remember multiple username/password pairs; consumers are concerned about re-authentication requirements; want dealings with multiple organizations to be seamless." Clarke 2004: "Consumers would like to avoid being subjected to large amounts of personal data disclosure, and that are able to continually add to that data in order to locate and track them."

We judge on the social desirability of alternative IMS structures by comparing the values of total consumer utility accruing to each one of the alternatives. We model consumers' utility as a function of the extent of revealed partial identity (Clauss and Kohntopp, 2001) and build on the network interconnection model by Heal and Kunreuther (2002) to model incentives of the identity management firms. The resulting theoretical model yields several inferences and policy implications stemming from the predicted relationship between private and social optima with respect to the interconnection issue.

Since there clearly is a tradeoff between the extent to which privacy is protected and the effectiveness with which the Government is able to control individuals' actions, privacy must be compromised to a

certain degree. Or, as the Open Group put it, "... the desire for privacy and individual dignity must be reconciled with the desire for effective government and with legal needs and national security needs." (Open Group) Limited acceptance of Microsoft Passport due to "the reluctance of the public to trust any single organization to provide a universal identity management solution, reinforced by the fact that security question marks have been raised relating to the specific Passport implementation." (Open Group) Hansen et al. (2003) "On the one hand, in particular legal contexts reliable identification of a person is necessary; and, on the other, the structuring and representation of identity is based in human rights law."

In this study we are looking for the scope for balanced solutions to the problem of identity management focusing on the issue of interconnection between alternative IMS firms. We are especially interested in identifying the type of environment in which the individual incentives of IMS firms push them to interconnect in a way that is socially suboptimal. Designing policies for this type of environment is a challenging goal for the policy makers that can be better achieved when backed by a better understanding of the economic processes behind interconnection.

D. Modeling and Analysis

In this section we develop a general economic model of the provision of and demand for an IMS. We describe the model's key elements, their characteristics and the basic game-theoretic model applications.

I. Model Definitions

An *informational atom* is the smallest possible piece of information about an individual that cannot be split into any smaller pieces of information. There are a finite number of such atoms, \bar{A} , and \mathbf{A} is the set comprising all of those atoms:

$A = \{a_i, i = 1.. \bar{A}\}$, where a_i is an information atom. Atoms may be of various nature and they can be measured in different units. Examples of atoms would include E-mail addresses, mobile phone numbers, hair color, the car brand etc.

Set \bar{A}_j that is a collection of all atoms that pertain to an individual is called an individual's *identity*, or:

$\bar{A}_j = (a_{j_1}, a_{j_2}, \dots, a_{j_{\bar{A}}})$, where j is an individual's index and $J < \bar{A}$ is the amount of atoms that describes individual j 's identity. As follows from the above definition, some atoms from \mathbf{A} are not included into some individuals' identity sets \bar{A}_j . Examples include “an individual does not have a car” or, in case individual is not married, an informational atom “age of spouse” will be irrelevant.

An individual's *partial identity* is defined as any subset of \mathbf{I}_k . Partial identity can be thought of as a piece of personal information an individual is willing to reveal in order to obtain a specific type of an *information service* provided by an *information management system*. The size and composition of a specific partial identity depend on the type of the information services to acquire as well as the amount of *risk* associated with disclosing the partial identity.

The *information management system (IMS)* is a sort of production unit that supplies *informational services* to consumers in exchange for the *partial identities* the latter provide for the former.

The set of the *informational services atoms*, \mathbf{S} , is defined by analogy with the set of the *identity atoms*,

namely,
$$S = \{s_i | s_i = \text{information service}\}, i = 1.. \bar{S}$$

$$\bar{S} = \text{number of information services}$$

For convenience, we call the *informational services atoms* just *service(s) atoms*, while simply *atoms* refer to the (partial) identity atoms.

Define user k 's demand for the informational services as $\bar{S}_k = (s_{k_1}, s_{k_2}, \dots, s_{k_{S_k}})$, where S_k is the number of informational services required/demanded by user k .

II. Model Attributes and Interactions

The set of the services atoms \mathbf{S} and the set of identity atoms \mathbf{A} are linked through the assumption that supplying (by the *IMS*) any one service atom s_i requires one or more *identity atoms* a_j . In other words, we postulate a mapping of \mathbf{A} into \mathbf{S} , so that each element of \mathbf{S} can be in general a multivariate function of \mathbf{A} .

The rather technical assumption we have to make at this stage is that the union of all possible

information services requires exactly the set of existing information atoms, or

$$\bigcup_{j=1}^{\bar{s}} \bar{A}_j = A, \text{ where}$$

$$\bar{A}_j = (a_{j_1}, a_{j_2}, \dots, a_{j_{J_s}}) = (s_{J_s})^{-1}$$

and J_s is the number of *information atoms* required for the provision of *informational service s*.

The basic tradeoff in the setting developed above is that the amount of the informational services a consumer can receive is directly proportional to the type of the *partial identity* revealed to the *IMS*, but so is the risk associated with the possible theft of the identification information.

Partial identities vary at least along two dimensions. (1) the *volume* of the provided information measured as the ratio of the number of atoms in the individual partial identity to the total number of the identity atoms. The risk associated with the theft of a partial identity is a (monotonically) increasing function of the *volume of partial identity*, not necessarily linear; (2) the *structure* of the partial identity, reflecting the fact that (a) not all atoms are equally important from the point of view of both the quality and amount of information services they give access to and the degree of risk associated with their theft (b) different combinations of atoms may imply different amounts of services and risks. For example, the loss of a mobile phone number may be not as harmful as the loss of a credit card number (case 2a) and the theft of a login nickname for the Internet banking website is not likely to do much harm *per se*, whereas in combination with the theft of the corresponding password the damage will be much more essential (case 2b).

Since modeling case (2) is clearly more complicated compared to case (1), I would suggest starting with the *partial identity volume* as the only determinant of the user's risk and the informational services' supply.

According to our definition of the *IMS* above, the latter provides *informational services* in exchange for the *identity information*. Two extreme (and, of course, unrealistic) cases are illustrative.

- (1) The *centralized IMS* is one single *IMS* that provides all feasible *informational services* and their combinations, while requiring each individual's *complete identity* information in exchange. From the point of view of production, processing and maintenance costs (to be considered later) it is the cheapest long-run *IMS* solution since, even if it may involve sizeable fixed costs, the variable costs are likely to be very low. On the demand side, the users will only have to maintain a uniform *partial identity* for access to all information

services, which in this extreme case is their *complete identity*. Of course, the extent of risk associated with the theft of such a uniform identification “card” is the highest compared to the other *IMS* since, once stolen, this information can be used for access to all existing information services.

- (2) The *service-by-service IMS* is another extreme form of the *IMS* whereby each service s_i is provided by its “personal” *IMS*, so that the user has to maintain as many *partial identities* as there are *informational services*, or \bar{S} in our notation. In contrast to the *centralized IMS*, the amount of risk involved is minimal in this extreme case.

To summarize, the *centralized IMS* minimizes the long-run average costs and only requires maintain one partial identity, but it maximizes the risk of theft and the associated losses to the user, while the *service-by-service IMS* is costly both in terms of construction and maintenance, but the risks to the user are minimal, even if he or she has to maintain multiple login/passwords.

It is a fact that most users maintain multiple user IDs and passwords (for example, the information that is needed in order to open a bank account is different from the type of information one needs to provide for access to the University online library). It is also true that due to the interconnection between various *IMS*-s, the amount of partial identities is considerably less than the number of the information services (Microsoft Passport is one example). That is, in real world the “equilibrium” provision of the *IMS*-s is somewhere in between the two extreme cases described above. Below we consider a few likely factors that affect this “equilibrium”.

III. Supply Side Model

In accordance with the general economic principles, maintaining an *IMS* involves fixed and variable costs. Fixed costs are an increasing function of the power of the encryption algorithm. Variable costs increase with the complexity of the authentication process and bandwidth. [Other factors influencing both types of costs are of course possible].

Fixed and variable costs are interrelated with each other. Thus, the more powerful the encryption mechanism, the smaller the one type of variable (authentication) costs, while the other type of variable costs (bandwidth/processing) is higher. Conversely, the development of a less powerful an encryption mechanism involves smaller fixed costs, higher costs of authentication and lower bandwidth/processing costs.

In general, the information service providers may wish to outsource the process of development of an IMS to the existing IMS-s through *interconnection* to the latter. For example, a credit card company may have an agreement with the banks by which the latter provide information on a person's credit limit and credit card use once the bank's customer has successfully logged in to the bank's website. At the same time, the credit card company may maintain its own IMS for independent access, with different requirements as to the type of the partial identity needed for access compared to that of the bank. The issues here include pricing of access to such information and costs of the development of the authentication algorithm on the side of the credit card company.

Using the functional relationships between the encryption and authentication power, and the amount of risk of the partial identity theft involved, the IMS producers will choose how much partial identity to require for each set of the informational services they provide.

The IMS producers face the same type of constraints regular firms do by deciding how much to produce depending on the relationship between fixed and variable costs. In our case, though, *the fixed and variable costs* are interrelated, which should be incorporated into the model.

IV. Demand Side Model

On the demand side, users' key concerns are (1) the risk associated with the theft of his or her partial identity and (2) the costs of maintaining multiple ID-s/passwords. Presumably, (1) is the more important factor behind consumers' choice of IMS.

Define $P(\bar{A}_j)$ as the probability of the event of theft of partial identity \bar{A}_j . Assuming that the thieves will increase their efforts on breaking the access codes proportionally to the increase in the "completeness" of the partial identity, $P(\bar{A}_j)$ is an increasing function of \bar{A}_j , or $P = P\left(\bar{A}_j\right)_{(+)}$. Since for now we are abstracting ourselves from the issue of the structure of partial identities, an increase in vector \bar{A}_j means simply the increase in the number of information atoms \bar{A}_j is comprised of.

Some simple functional relationships between probability of theft and characteristics of the IMS

Denoting ε the encryption power of the *IMS*, we assume that the probability of theft is a decreasing

function of the former: $P = P\left(\begin{matrix} \bar{A}_j \\ (+) \end{matrix}, \varepsilon\right)$.

Denoting α the power of the authentication mechanism, $P = P\left(\begin{matrix} \bar{A}_j \\ (+) \end{matrix}, \varepsilon, \alpha\right)$.

The more powerful authentication mechanism requires provision of more information on identity:

$$\alpha = \alpha\left(\begin{matrix} \bar{A}_j \\ (+) \end{matrix}\right)$$

More encryption requires less authentication and vice versa:

$$\varepsilon = \varepsilon\left(\begin{matrix} \alpha \\ (-) \end{matrix}\right).$$

The users choose the type of IMS by maximizing their utility U , which is a function of the extent of risk associated with identity theft and the amount of services provided.

In our notation,

$$U = U\left(\begin{matrix} P, S_j \\ (-) \end{matrix}, \begin{matrix} (+) \end{matrix}\right) = U\left(\begin{matrix} P\left\{\begin{matrix} \bar{A}_j \\ (+) \end{matrix}, \varepsilon\left(\begin{matrix} \alpha\left(\begin{matrix} \bar{A}_j \\ (+) \end{matrix}\right)\right) \end{matrix}\right\}, \alpha \\ (-) \end{matrix}, \begin{matrix} S_j \\ (+) \end{matrix}, \begin{matrix} \bar{A}_j \\ (+) \end{matrix}\right)$$

Users maximize their utility by choosing the type of partial identity they are willing to provide to an IMS. In the most primitive case, they choose the volume of partial identity:

$$\text{Max}_{\bar{A}_j} U\left(\begin{matrix} P, S \\ (-) \end{matrix}, \begin{matrix} (+) \end{matrix}\right)$$

In the simple case of measuring users' partial identity \bar{A}_j as a fraction of informational atoms in user j 's complete identity, a solution that falls short of 100% will imply the existence of at least two information management systems. Adding the interconnection/switch costs/access pricing issues is of considerable interest.

V. Game-Theoretic Model and Examples

We assume that each informational service s_i requires provision of exactly one identity atom a_i , which implies that the amount of identity atoms equals that of the informational services. (In the continuous case that can be rephrased in terms of the capacity of identity and services' sets.) In terms of our notation, $\bar{A} = \bar{S}$, and the partial identity provided by a consumer is equal to the fraction of all

information services he or she receives: $\frac{\|\bar{A}_j\|}{\|A\|} = \frac{\|\bar{S}_j\|}{\|S\|}$. In the discrete case we are considering, the norm

of either set A or S is simply the number of identity or service atoms in it. Finally, we denote by s_b the amount of services consumed by consumer b , so that the ratio $\frac{s_b}{S}$ also measures the completeness of consumer b 's identity he or she is revealing in exchange for the services.

The utility consumers derive from connecting to the (interconnected) IMS systems increases in the amount of services they receive and decreases in the norm of partial identity they reveal as required by the IMS-s. The utility function can thus be represented as a composition of utility and disutility. The positive effect exhibits diminishing marginal utility, while disutility's marginal product increases with the partial identity norm.

The above description can be presented formally in the following way:

$U = U\left(s_b, \frac{s_b}{S}\right)$, such that

$$\frac{\partial U}{\partial s_b} > 0, \quad \frac{\partial^2 U}{\partial s_b^2} \leq 0, \quad \frac{\partial U}{\partial \left(\frac{s_b}{S}\right)} > 0, \quad \frac{\partial^2 U}{\partial \left(\frac{s_b}{S}\right)^2} \geq 0$$

It is important to realize that, even if technically the above utility function can be formulated in terms of one independent variable s_b , we use the two-variable representation so as to make a difference between the positive and negative effects induced by the consumption of informational services.

The following is an example of the above utility function:

$$U = U\left(s_b, \frac{s_b}{S}\right) = \gamma s_b^\alpha - \delta \left(\frac{s_b}{S}\right)^\beta, \text{ where } \alpha \in (0,1) \text{ and } \beta > 1$$

The two partial derivatives of U describe the positive and negative effects separately:

$$\frac{\partial U}{\partial s_b} = \gamma \alpha s_b^{\alpha-1}$$

$$\frac{\partial U}{\partial \left(\frac{s_b}{S}\right)} = -\delta \beta \left(\frac{s_b}{S}\right)^{\beta-1}$$

Given the restrictions imposed on parameters α and β , the positive effect of consuming more services is in fact positive, while the negative effect of revealing more of one's identification information is negative.

The composite effect of an increase in the consumption of services is given by the following formula:

$$\frac{dU}{ds_b} = \alpha \gamma s_b^{\alpha-1} - \frac{\beta \delta}{S^\beta} s_b^{\beta-1}$$

Assuming a money-metric utility function, for any amount of consumed information services s_b , the corresponding value of $U\left(s_b, \frac{s_b}{S}\right)$ is also the consumer's willingness to pay (WTP) for this amount of services, which can also be regarded as consumer surplus. From now on, we use the terms "utility" and "consumer surplus" interchangeably.

The IMS is defined as an entity (a "black box") that provides informational services in exchange for the customers' partial identities. The assumption here is that no two IMS-s can provide the same service atom, or the intersection of the sets of services provided by any two IMS-s is an empty set. Accordingly, the identity requirements by any two IMS-s are different.

- a) Consumers get access to more services
- b) Consumers have to reveal more private information about themselves
- c) The risk of (partial) identity theft increases due to network externalities

As mentioned before, different IMS-s exert differing identity provision requirements, so that the customers of IMS A have to reveal the identity atoms necessary for access to IMS B when IMS A

decides to interconnect with IMS B.

There are at least two ways in which one can think about the process of choice between alternative structures of IMS (e.g. the choice between the centralized and the proprietary one). In both cases comparing consumer utility (or, equivalently, surplus in our interpretation) resulting in each case plays a crucial role. One way of thinking emphasizes consumers' ability to choose the IMS structure. With several groups of consumers enjoying various combinations of consumer surplus values contingent on the IMS structure, the equilibrium IMS structure will be desirably the Nash outcome. Another way of thinking is to assume that the IMS firms are able to extract all or part of the consumer surplus, resulting in the same game matrix.

In both cases, three possibilities are possible: (1) do not interconnect and provide services only to "one's own" customers—equivalent to the choice of two different standards, say A and B that are not compatible with each other (2) interconnect by adopting the same standard A or B (3) stay out of the market. Denote s_a and s_b the number of services provided by an IMS operating under standard A and B, respectively. Assume interconnection under any standard grants access to all existing services. The resulting game matrix is given below (choices of IMS₁ are represented by the rows, choices of IMS₂ are represented by the columns):

	A	B
A	$U(\bar{S}, 1), U(\bar{S}, 1)$	$U\left(s_a, \frac{s_a}{\bar{S}}\right), U\left(s_b, \frac{s_b}{\bar{S}}\right)$
B	$U\left(s_b, \frac{s_b}{\bar{S}}\right), U\left(s_a, \frac{s_a}{\bar{S}}\right)$	$U(\bar{S}, 1), U(\bar{S}, 1)$

Interconnection (that is, outcomes A,A or B,B) occurs when the following condition holds:

$$\begin{cases} U(\bar{S}, 1) > U\left(s_a, \frac{s_a}{\bar{S}}\right) \\ U(\bar{S}, 1) > U\left(s_b, \frac{s_b}{\bar{S}}\right) \end{cases}$$

The game above has only two Nash equilibria, (A,A) or (B,B), if there is no disutility to revealing one's partial identity. In other words, if $\frac{\partial U}{\partial\left(\frac{s_b}{\bar{S}}\right)} = 0$, the equilibrium outcome is the one with the two

IMS interconnecting with each other (or, equivalently, choosing common standard).

The IMS firms may extract all or part of the consumer surplus of the customers to whom they provide their services. This follows from the basic discussion in microeconomics of the importance of information on customers to the successful implementation of price discrimination. Thus, perfect screening allows for the first-degree price discrimination.

We assume the fraction of the consumer surplus extracted by an IMS firm (or by many of them, in case of interconnection) depends on the amount of partial identity provided, so that consumer surplus gets modified in the following way:

$CS\left(s_b, \frac{s_b}{S}\right) = \lambda\left(\frac{s_b}{S}\right)U\left(s_b, \frac{s_b}{S}\right)$, where $\lambda\left(\frac{s_b}{S}\right)$ is the fraction of the consumer surplus the IMS firms are able to extract. Naturally, $\frac{\partial\lambda\left(\frac{s_b}{S}\right)}{\partial\left(\frac{s_b}{S}\right)} > 0$.

<The game matrix with screening and extraction effects>

	A	B
A	$\lambda(1)U(\bar{S}, 1), \lambda(1)U(\bar{S}, 1)$	$\lambda\left(\frac{s_a}{S}\right)U\left(s_a, \frac{s_a}{S}\right), \lambda\left(\frac{s_b}{S}\right)U\left(s_b, \frac{s_b}{S}\right)$
B	$\lambda\left(\frac{s_b}{S}\right)U\left(s_b, \frac{s_b}{S}\right), \lambda\left(\frac{s_a}{S}\right)U\left(s_a, \frac{s_a}{S}\right)$	$\lambda(1)U(\bar{S}, 1), \lambda(1)U(\bar{S}, 1)$

<Interconnection Nash equilibrium conditions with screening and extraction>

With screening and extraction, the Nash equilibrium conditions become:

$$\begin{cases} \lambda(1)U(\bar{S}, 1) \geq \lambda\left(\frac{s_b}{S}\right)U\left(s_b, \frac{s_b}{S}\right) \\ \lambda(1)U(\bar{S}, 1) \geq \lambda\left(\frac{s_a}{S}\right)U\left(s_a, \frac{s_a}{S}\right) \end{cases}$$

Within each IMS, a theft of identity is possible, resulting in loss L for a customer. That sort of theft happens with probability p_i for IMS_i . In case IMS_i interconnects with IMS_j , the thief who stole a customer's partial identity from IMS_i will have access to services provided by IMS_j , and vice versa. In case of only two IMS-s, denoting p the probability of theft in IMS_1 and q the probability of theft in

IMS₂, the expected value of a loss caused by the partial identity theft is given by $pL + (1-p)qL$.

Assuming L to be directly proportional to the fraction of identity stolen and setting theft probabilities equal across all IMS-s, one gets the following expression for a consumer surplus in case of a specific standard:

$CS\left(s_a, \frac{s_a}{S}\right) = \lambda\left(\frac{s_a}{S}\right)U\left(s_a, \frac{s_a}{S}\right) = \lambda\left(\frac{s_a}{S}\right)U\left(s_a, (p + (1-p)p)\theta\left(\frac{s_a}{S}\right)\right)$ with the game matrix

and Nash equilibria conditions modified accordingly, where $\theta\left(\frac{s_a}{S}\right)$ is an increasing theft loss

function with $\frac{\partial \theta}{\partial \left(\frac{s_a}{S}\right)} \geq 0$.

The maximum risk constraints may be added to the above framework in terms of the loss due to theft function $\theta\left(\frac{s}{S}\right)$. The minimum privacy constraints can be formulated in terms of the maximum amount of one's identity that may be revealed either to all IMS providers lump sum or to each one in particular (in the latter case the scope of the revealed identity information is naturally greater than it is in the former).

The optimal fraction of information services consumed is given by the following consumer maximization problem:

$$\begin{cases} \text{Max } U\left(s, \frac{s}{S}\right) \\ \text{privacy / risk constraints} \end{cases}$$

Assuming the utility function to be

$U = U\left(s_b, \frac{s_b}{S}\right) = \gamma s_b^\alpha - \delta \left(\frac{s_b}{S}\right)^\beta$, where $\alpha \in (0,1)$ and $\beta > 1$, the Nash equilibrium conditions for

interconnection to take place are as follows:

$$\begin{cases} \gamma \bar{S}^\alpha - \delta > \gamma s_a^\alpha - \delta \left(\frac{s_a}{S}\right)^\beta \\ \gamma \bar{S}^\alpha - \delta > \gamma s_b^\alpha - \delta \left(\frac{s_b}{S}\right)^\beta \end{cases} \Leftrightarrow \gamma \bar{S}^\alpha - \delta > \text{Max} \left\{ \gamma s_a^\alpha - \delta \left(\frac{s_a}{S}\right)^\beta, \gamma s_b^\alpha - \delta \left(\frac{s_b}{S}\right)^\beta \right\}$$

Utility function $U(,)$ possesses the following properties:

$$\begin{cases} U(0,0) = 0 \\ U(\bar{S},1) = \gamma\bar{S}^\alpha - \delta \end{cases}$$

Utility function U has the following derivative: $\frac{dU}{ds} = \gamma\alpha s^{\alpha-1} - \beta\delta\left(\frac{s}{\bar{S}}\right)^{\beta-1}$. It can be shown that utility

derived by the consumers from enjoying information services s is increasing up until a certain level (call it level s_0) and then starts decreasing. For certain values of parameters α and β this level can

be computed rather easily. For example, for $\alpha = 0.5$ and $\beta = 1.5$, $\frac{dU}{ds} = \frac{\gamma}{2\sqrt{s}} - \frac{3\delta}{2\bar{S}}\sqrt{s}$. In this case

the utility achieves its maximum at $s_0 = \frac{3\gamma}{4\delta}\bar{S}$, which, provided that $\frac{3\gamma}{4\delta} < 1$, means that the optimal

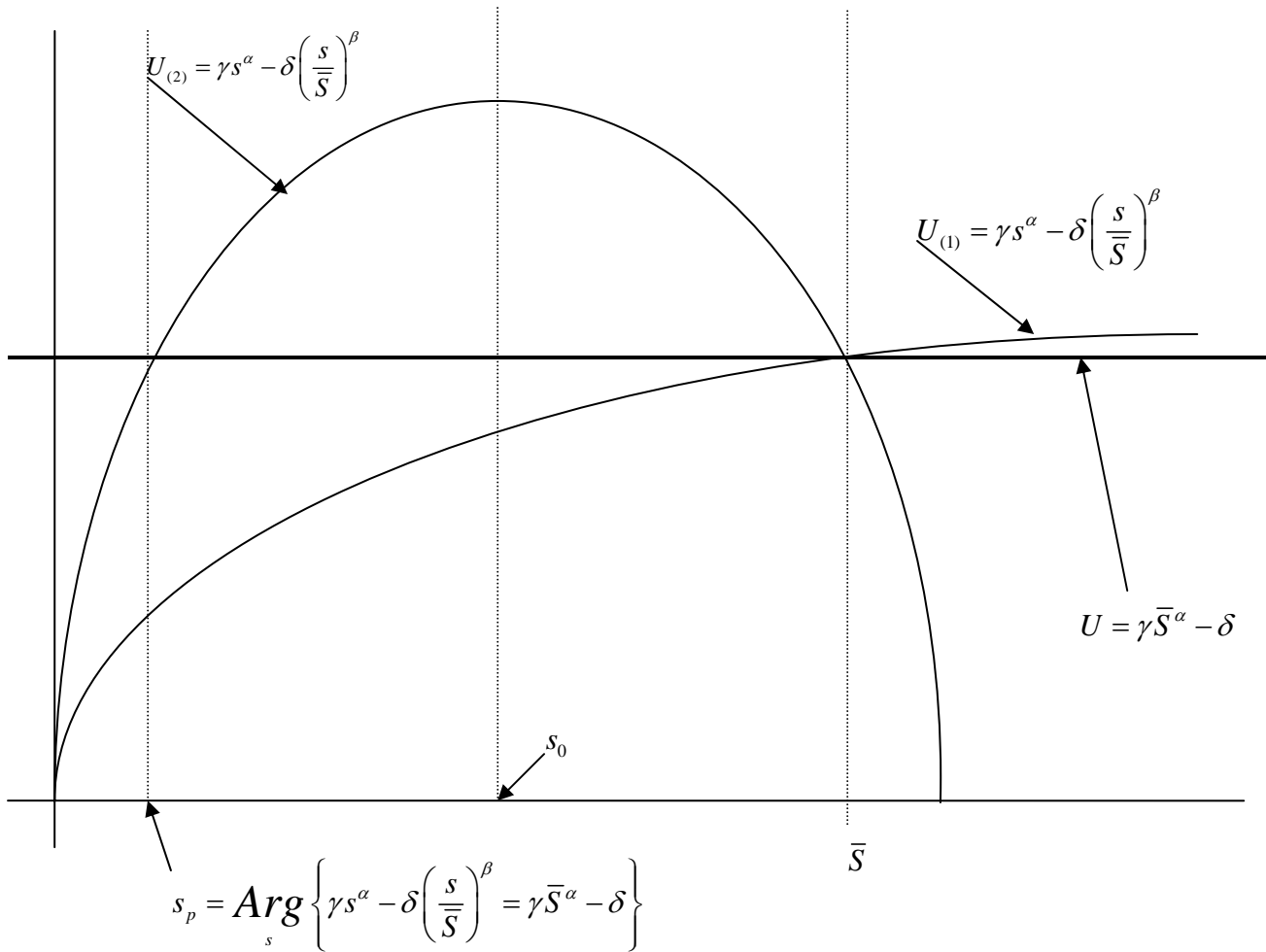
level of services provision for any IMS / consumer group is smaller than \bar{S} , or in other words, there exist conditions under which the centralized IMS structure is not an optimal social choice.

As mentioned before, the game matrix developed above may represent two different settings, namely:

(1) firms extract all consumer surplus, or alternatively, the captive market setting, and (2) the consumer groups belonging to different types of IMS decide whether to let the IMS providers to interconnect. The Nash equilibrium framework is the same in both cases.

Graph 1 below illustrates the incentives faced by any one group of the consumers / IMS provider.

Graph 1: Incentives by one IMS firm / consumer group to interconnect.



By its construction, the utility function is equal to zero when the amount of services consumed is zero and it is equal to $\gamma\bar{S}^\alpha - \delta$ at the maximum available level of services, \bar{S} . The decision to interconnect is being taken for those levels of services for which the incentives to interconnect curve (the horizontal line on Graph 1) lies above the incentives curve to stay with the proprietary IMS structure. The cutoff point is labeled s_p . Consumer groups / IMS firms prefer to stick to the proprietary system if the amount of identity information solicited from them exceeds this cutoff level due to the mounting disutility effects of disclosing identity information.

The following gives general conditions for interconnection to take place:

$$\gamma s^\alpha - \delta \left(\frac{s}{\bar{S}}\right)^\beta < \gamma\bar{S}^\alpha - \delta.$$

The analytical solution for this inequality is rather hard to obtain. However, given the properties of consumers' utility function, namely,

$$\begin{cases} U(0,0) = 0 \\ U(\bar{S},1) = \gamma\bar{S}^\alpha - \beta \end{cases}$$

whenever $s_0 < \bar{S}$ the cutoff level of service provision beyond which a proprietary IMS structure is preferred is below the maximum level of the provision of services, or $s_p < \bar{S}$. The proof of the latter fact is rather intuitive and is not being provided here.

The sufficient condition for interconnection to always be the optimal choice for any one IMS firm / consumer group, the following suffices: $s_0 \geq \bar{S}$. As was mentioned above, in case of $\alpha = 0.5$ and

$\beta = 1.5$ the centralized IMS structure will be always preferred to the proprietary one if $\frac{3\gamma}{4\delta} < 1$, or if the marginal disutility of services is sufficiently small compared to their marginal utility, which makes intuitive sense. This case corresponds to the function denoted $U_{(1)}$ in Graph 1. Once the marginal disutility parameter δ is large enough, the decision to interconnect will depend on the currently consumed level of information services, as illustrated by function $U_{(2)}$. In this case, the IMS firms /

consumer groups will only prefer to interconnect until level s_p of the supplied information services. Beyond that level their choice will be to stay with the proprietary IMS system.

We can thus talk about the minimum “reasonable” level of interconnection required by the users beyond which they prefer subscribing to several alternative IMS providers. The number of these

providers, call it N_s , is roughly equal to $N_s = \text{int}\left(\frac{s_0}{s_p}\right)$.

E. Technology Policy Applications and Work In-Progress

In this study we offered a framework for designing a policy for interconnection between alternative identity management systems (the IMS-s). Also, the primary issue we found while developing this model was that the literature review and theoretical underpinnings on the identity economics can be enhanced to deal with socio-technical and economic aspects of digital identity system in today’s Internet environment. The usefulness of the proposed IMS model is to analyze the economic policy implication of dynamic service interconnections such as in Context-Aware Networks, Ubiquitous Sensor Networks, etc. We believe the scope for such policy stems from the fact that consumers have concerns about privacy, that is, the utility gains from acquiring the many services in exchange for supply of private information (such as e.g. contextual, LBS, etc) can be mitigated or even offset by increases in the disutility of providing this private information. We also conducted studies of characterizing and designing the technical IMS systems for the purpose of developing socially optimal IMS system designs. This study is a useful step on the way of formalizing the identity-related policy design which may help make policy decisions in the area of identity management more educated.

We plan to develop and examine proper case studies using this theoretical framework to deal with various IMS economic issues. This effort has two interrelated goals. First, we want to obtain a picture of how on-line identities are handled in users' organizations with and without technical and policy constraints on identity provision and/or disclosure. With available identity systems and reviewed enabling technologies, we also hope to understand the rationales behind users’ handling of identity, its contextual information and uses of security and privacy enhancement technology. Second, we want to uncover the process of economic decisions that users and organizations make when managing their identities and the dynamic data on those identities.

References

- Akerlof, G. A. (1970). "The Market for Lemons: Quality Uncertainty and the Market Mechanism." Quarterly Journal of Economics **84**(3): 488-500.
- Anderson, R. (2001). Why Information Security is Hard: An Economic Perspective. **2003**.
- Anderson, R. (2002). Security in Open versus Closed Systems: The Dance of Boltzmann, Coase and Moore. Open Source Software: Economics, Law and Policy, Toulouse, France.
- Bechtold, S. (2002). Governance in Namespaces. TPRC 2002 The 30th Research Conference on Information, Communication, and Internet Policy, Alexandria, VA.
- Clarke, R. (1994). "Human Identification in Information Systems: Management Challenges and Public Policy Issues." Information Technology and People **7**(4): 6-37.
- Computer Science and Telecommunications Board, N. R. C. (2002). IDs - Not That Easy: Questions about Nationwide Identity Systems. Washington, DC, National Academy of Sciences.
- Farrell, J. and G. Saloner (1985). "Standardization, Compatibility, and Innovation." RAND Journal of Economics **16**(1): 70-83.
- Feigenbaum, J., M. J. Freedman, et al. (2002). Economic Barriers to the Deployment of Existing Privacy Technology. Berkeley, CA, Workshop on Economics and Information Security: 3.
- Froomkin, M. (2002). The Uneasy Case for National ID Cards as a Means to Enhance Privacy. TPRC 2002: The 30th Research Conference on Information, Communication, and Internet Policy, Washington, DC.
- FTC (1998). Comment of the Staffs of the Bureaus of Economics and Competition of the Federal Trade Commission on Improvement of Technical Management of Internet Names and Addresses. Washington, DC.
- Greenwood, D., D. Combs, et al. (2002). Identity Management: A White Paper. Lexington, KY, National Electronic Commerce Coordinating Council: 68.
- Huston, G. (2002). "ENUM - Mapping the E.164 Number Space into the DNS." The Internet Protocol Journal **5**(2): 13-23.
- Hwang, J. and M. Mueller (2002). The Economics of ENUM Over Cable Broadband Access Networks. Syracuse, NY, The Convergence Center, Syracuse University.
- Rohlf, J. (1974). "A Theory of Interdependent Demand for a Communications Service." Bell Journal of Economics and Management Science **5**(1): 16-37.
- Taylor, L. (1980). Telecommunications Demand: A Survey and Critique. Cambridge, MA, Ballinger.
- Varian, H. (2002). System Reliability and Free Riding. Open Source Software: Economics, Law and Policy, Toulouse, France.
- SSN Report <http://www.ssa.gov/history/reports/ssnreport.html>
- The AAMVA standard <http://www.aamva.org/standards/stdAAMVADLIdStandard2000.asp>