The Digital Persona and Trust Bank: A Privacy Management Framework
Sree Nilakanta & Kevin Scheibe

Abstract
Information privacy and protection in the United States is a source of great debate in both the academy and industry. Technological advancements in areas such as data warehousing allow aggregation of data across seemingly unrelated sources to create detailed profiles of individuals making privacy pundits cry foul. This tension begs the question, who owns secondary or transactional information of individuals. Currently ownership is with the organization. In this paper we develop a framework that shifts the ownership to the individual. We show how this shift benefits not only the individual but also the organization. We introduce a Trust Bank, an organization acting as an agent for consumers, and describe the benefits of allowing the consumer control their Digital Persona, the electronically aggregated profile created by transactional processes.

1. Introduction
Contemporary businesses are distinguished by their ability to alter industry structures and adopt competitive strategies that span conventional industry boundaries because they have become increasingly savvy at exploiting proprietary data about their customers. Supermarkets enter retail banking, banks become insurance providers, and logistics firms become customer support providers. In each case, these firms know a great deal about their customers’ preferences, transactions, and purchase behaviors and apply sophisticated data warehousing and data mining technologies to manage the customer. The central focus of this paradigm shift is digitized personal information. The more detailed and shared the personal information, the better the value the customer may receive from businesses. Informational price is the price of privacy and becomes the basis for an informational capitalism.

Consumer privacy in contemporary society is an endangered concept. The public majority believes they have lost control over how their personal information is collected and used by companies. Several studies have found that consumers are wary of privacy issues and feel disempowered to control their privacy rights (Claburn 2004; PrivacyKnowledgeBase 2004). The advent of the Internet, electronic commerce, and mobile devices has further contributed to
the erosion of personal control of privacy. Privacy Knowledge Base, a private organization that monitors and disseminates information on privacy related matters, concludes, based on the results of over 200 surveys over the last decade, that (a) privacy is an ongoing issue of significant importance to the consumer, (b) a majority of consumers are pragmatic in their view of privacy and the need to share private information with companies with appropriate balance of risk and return, and (c) consumers will demand appropriate laws and regulations to stem the erosion of their privacy rights should the need be perceived, as in health and financial information (PrivacyKnowledgeBase 2004).

The tension between personal control of privacy and desirable benefits of service requiring release of control is the motivation of the framework presented in this paper. We present a framework that allows individuals to maintain control and receive direct benefit of their information and allows companies potentially greater informational access for value added service and products. This paper is organized as follows. Section two defines and discusses privacy, data collection, FIP, and regulation. Section three explains the digital persona (DP) and trust bank (TB) framework and discusses implications. Finally, the conclusions and discussion of future direction are presented.

2. Background

2.1. Privacy

Nearly forty years ago Alan Weston published the seminal work on privacy and freedom in our society (Westin 1967), and with technological advancements, such as the Internet, e-commerce, and data warehousing, the fundamental issues of privacy and the need for disclosure presented in his work increase in significance. Weston defines privacy as,
the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others. Viewed in terms of the relation of the individual to social participation, privacy is the voluntary and temporary withdrawal of a person from the general society through physical or psychological means, either in a state of solitude or small-group intimacy or, when among larger groups, in a condition of anonymity or reserve. The individual’s desire for privacy is never absolute, since participation in society is an equally powerful desire. Thus each individual is continually engaged in a personal adjustment process in which he balances the desire for privacy with the desire for disclosure and communication of himself to others, in light of the environmental conditions and social norms set by the society in which he lives. The individual does so in the face of pressures from the curiosity of others and from the processes of surveillance that every society sets in order to enforce its social norms (Westin 1967).

Privacy is the control of information. Privacy is not absolute, but must be relinquished to some degree to participate in society. In modern society a balance between disclosure and privacy is required by every participant (Westin 1967).

Privacy is the amount of control that an individual can exert over the type of information and its release to others. Researchers have formulated multiple aspects of information privacy to cover physical privacy, social privacy, decisional privacy, and personal privacy. Prosser’s [1960] legal definitions of intrusion, disclosure, falsification, and appropriation relate to these four types of privacy issues. Bellman et al. (2003) in their study uses the four dimensions of information privacy developed by Smith, Milberg, and Burke (1996) to encompass the dimensions of collection, unauthorized secondary use, improper access, and errors. Technological advances and
enhanced ease of data collection have resulted in explosive growth of consumer data gathered by companies. The public feels that increased data collection is intrusive, unreasonable, and excessive. When a company uses consumer data for purposes other than its intended purpose, the secondary use becomes unauthorized. Collection dimensions reflect this. Lapses in security and integrity of the data collected may also lead to improper access and use. Errors can exist in the data because of problems with source or transformation. All of these factors can result in violation of privacy rights of the consumer and can cause irreparable harm.

A literature review of information privacy and the US and European data privacy approaches suggests that there are distinct differences between the two regions. The primary differences are the condition of limited access to identifiable information about individuals and the regulatory and managerial perspectives about privacy. And there are no rules regarding the collection, use, and sharing of personal data that currently spans all sectors of the economy. In contrast, in Europe the data subjects have much greater rights to their data. Few American databases of consumer information have been designed with this concept in mind, although some could perhaps fulfill the European requirements (Smith 2001). The Organization for Economic Co-operation and Development Guidelines on the Protection of Privacy and Trans-border Data Flows (OECD 2004) are one of the best known information privacy practice norms and are the bases for many European privacy legislations.

The recent spate of privacy acts like the Health Insurance Portability and Accountability Act (HIPAA) of 1996, the Gramm-Leach-Bliley Act of 1999, and Sarbanes-Oxley act seems to have changed the way organizations handle the personal information privacy issue. A recent financial privacy act passed by the California Legislature may give consumers even stronger privacy protections than afforded by the federal Gramm-Leach-Bliley Act. Among many other
noteworthy provisions, these privacy acts require the organizations to monitor business partner compliance and force them to inform the consumer about privacy policies (DeMuro and Grant 2001, Puclik 2003).

The OECD privacy guidelines stipulate eight core principles to manage privacy issues. These are collection limitation, data quality, purpose specification, use limitation, security safeguards, openness, individual participation, and accountability. Among the eight core principles, the individual participation principle allowing users to control their personal data and hence their privacy is core to ensuring a balanced and pragmatic approach to consumer privacy.

Self regulation and enforcement affect both the consumer and firm. The following matrix illustrates this framework. Privacy laws and regulations enacted by government bodies bind firms to certain norms of behavior. Similar regulations, often in the form of common laws govern consumers. Self regulation among consumers and firms differ to the extent that standards become de facto for firms whereas among consumers it is often affected by the community to which they belong. For example, journalists by and large adopt the notion that they should not reveal a rape victim’s identity even though it is a public record during a trial. Bennet (Bennet 1992) notes that data protection issues arise because of the complicated relationship between the individual and those with power to manipulate the personal data.

In order to understand the multi-faceted problems of privacy, Bennet (1992)suggests that we explore it from three dimensions, namely, humanistic, political, and instrumental. His basic premise is that privacy is fundamentally a data protection issue.

“On one level, therefore, the increase in the number and complexity of policies that we expect the modern welfare state to administer has meant a quantitative increase in the amount of information collected from individuals… On a qualitative level, there has
also been a change in the nature of the information collected. As programs have become increasingly refined, more sensitive and discriminating information on the financial, employment, health, and educations histories of a citizen has been required.” (Bennet 1992)

Protection or promotion of one’s dignity, individuality, integrity, or private personality amounts to defining the basic attributes of humanism. Westin (1967) argued that privacy is a set of four interrelated values, namely, protecting personal autonomy, providing a sense of emotional release, promoting self-evaluation and creativity, and limiting and protecting communication. While Westin aggregated privacy issues under these four major tenets, Flaherty (Flaherty 1989) enumerated thirteen different factors for consideration. They are, the right to individual autonomy; the right to be left alone; the right to a private life; the right to control information about oneself; the right to limit accessibility; the right to exclusive control of access to private realms; the right to minimize intrusiveness; the right to expect confidentiality; the right to enjoy solitude; the right to enjoy intimacy; the right to enjoy anonymity; the right to enjoy reserve; and the right to secrecy.

Information is the currency of the post-industrial economy (Bell 1973). It is transitory and contextual and has value to someone at a particular time. Information technology (IT) can enhance value of information through its management, control, and use. In this regard we see that as the number and complexity of policies increase there is a tendency to increase collection of personal data (Bennet 1992). Transactions with agencies such as motor vehicle departments, the IRS, etc., lead to the collection of administrative records. Crime data, credit reports, and the like give rise to the collection and retention of intelligence on the individual. Census, surveys, and similar data are gathered as statistical demographic data on individuals. Regulatory
requirements, national security concerns, and providing government services often give rise to the above type of data collection. In addition, commercial transactions also generate a growing repository of personal data.

Personalization systems that collect data on consumer demographics and behavior have become common business practice. Companies collect these information either directly from the consumer as part of the transactions or from third parties. Cranor (Cranor 2003) identified four types of systems of personalization. Recommender systems collect explicit and implicit data yielding behavior patterns and preference profiles. Task or session based personalization have been used in recommending products and services that appear similar. User and system initiated personalization focus on user involvement. Finally, prediction based personalization rely on purchase groups where the groups could be other consumers or product groups fitting a profile. Cranor also identified several risks associated with these personalization schemes including receiving unsolicited offers, discriminated on price and other demographics, victimized due to illegal disclosures of private data, be subjected to legal subpoena, and placed on surveillance. Different solutions may be discussed to reduce these risks, but perhaps the best approach is to yield control of the collection and use of personal data to the user. We agree with Cranor that “users should be able to control what information is stored in their profile, the purpose for which it will be used, and the conditions (if any) under which it might be disclosed. They should also be able to control when and if personalization takes place.” Accomplishing the above objective is a non-trivial task because the consumer’s digital persona is a complex labyrinth of both structured and unstructured transaction data resulting from their interaction with a wide range of companies and agencies. Clarke (Clarke 1994) defines digital persona as a model of an individual's public personality based on and maintained by transactions, and is intended for use as a proxy for the
individual. This digital persona exists unbeknownst to most individuals who do not even know that extent of data exchange among organizations is increasing, whether at the level of cohort groups or individual consumers.

2.2. Fair Information Practice

In 1997 the Federal Trade Commission (FTC) drafted the fair information practice (FIP) principles as a set of guidelines to protect the consumer and business. FIP are comprised of five principles. **Notice/Awareness** is the disclosure from a company or organization to the individual about what and how information is collected and used. **Choice/Consent** gives the individual power to allow or disallow the use of information collected about them. **Access/Participation** means that the individual should be able to inexpensively access information collected about them and contest inaccuracies. **Integrity/Security** states that the data collected should be accurate and secure. Organizations are expected to take “reasonable steps” to ensure integrity and security. **Enforcement/Redress** is the teeth in the bite of the fair information practice principles. Without a vehicle for appropriate recourse for misuse of information, no incentive for compliance exits (FTC 1998). Culnan (Culnan and Bies 2003) describes a set of global principles, fair information practices, which were developed to balance consumer privacy concerns with an organization's need to use personal information. She suggests three alternatives for implementing fair information practices with particular attention to the Internet: government regulation, industry self-regulation, and technological solutions. These solutions are also central in the privacy framework proposed by (Head and Yuan 2001). In their framework, a privacy protector coordinates appropriate actions prescribed by the above solutions with the privacy subject (consumer), privacy violator, and information collector (agency). Essentially, there are three
ways to enforce/encourage FIP participation – the market, the government, or some mixture of both.

2.3. Regulation

At one extreme is pure market regulation, where financial motivation is the impetus for FIP compliance. Organizations that had strong privacy protection policies would attract customers with that interest. Ideally, if a company violated the privacy of an individual, that person would no longer do business with the company. There would be a loss of revenue constituting a penalty. If enough people reacted similarly, then the company has incentive to change its practices. A key component of the effectiveness of a pure market approach to regulation is the disclosure of the information usage practices of a firm. It is here that the pure market approach fails. Consumers rarely know all the details of how a firm will use information about them, and with this approach, there is little incentive for a firm to release any more information than is absolutely necessary for its own profit.

The other extreme is pure government or enforcement regulation, where a governing body determines privacy rules and recourse. If a firm violates the privacy of an individual then it can expect some form of legal retribution. The failure of this approach lies in the high costs associated with maintaining and enforcing the necessary laws. Moreover, it can be argued that since government does not intimately know the business of the firms, then the rules established will either fall short or beyond the actual needed level of protection. This too will add to the overall cost of pure enforcement regulations.

Somewhere in the middle of these two extremes lies self-regulation. The effectiveness of self-regulation is primarily dependent upon the participation organizations. However, the form of self-regulation is similar to government regulation in that it is comprised of three components of
separation of power. They are legislation, enforcement, and adjudication. Legislation refers to who made the rules and what they are. Enforcement is how the rules will be enforced and who will start that process. Adjudication pertains to determining whether or not a company has actually violated those rules (Swire 1997). Self-regulation is most effective when market pressure is combined with government enforcement (Boulding 2000). Market pressure will encourage firms to proactively adopt privacy measures to attract customers, and government enforcement will deter firms from violating privacy rules. Furthermore, since companies know their business and can integrate measures appropriate for their interests as well as their customer’s, then government will not need to intervene at the level required for pure enforcement. The question is is it working? Some studies have shown that it is not (Reidenberg 1999; Culnan 2000; Hancock 2000). One reason for this apparent failure is insufficient motivation for compliance either on by market or enforcement. To that effect, some argue for stronger laws (Schwartz 1999) such as those in Europe (Reidenberg 1999; Boyarski, Fishman et al. 2001), some suggest better market incentives (Hancock 2000; Porcelli, Selby et al. 2002), and others believe the market is still driving companies to self-regulate (Hemphill 2000). While the reasons for non-compliance of FIP may differ, the theme of lack of motivation to comply is the same.

3. Digital Persona and Trust Bank

Clarke (Clarke 1994) defines DP as a model of an individual's public personality based on and maintained by transactions or secondary information, and is intended for use as a proxy for the individual. This DP exists unbeknownst to most individuals who do not even know that extent of data exchange among organizations is increasing, whether at the level of cohort groups or individual consumers. Currently, information brokers sell the secondary information with no
direct monetary benefits to the individual to which the information is about. Moreover, they have no direct control of who buys and sells the information about them. The only control they may exercise is opting out.

3.1. Monitoring and Controlling Privacy

Flaherty (Flaherty 1989) conducted comprehensive studies of data protection laws in Europe and United States and argues that as a primary vehicle to ensure privacy data protection laws imply several opportunities. Flaherty’s empirical and functional approach suggests the following:

- A constant review, updating, and adaptation of the law
- A continuing sensitivity to, and an expertise in, new technologies and application
- A separate, institutionalized policy instrument with a permanent, relatively small, dedicated, administratively expert, and technically competent staff whose responsibilities for licensing or registration are minimized
- A single privacy advocate at the head of the agency who knows exactly when to use the carrot and when to use the stick, and who is not concerned with balancing data protection with other administrative and political values
- A supportive public opinion and legislature

Dynamics of policy formation do not end in promulgating privacy laws but it establishes legacies related to statutes, politics, technologies, and international trade norms. Success of data protection and hence privacy would depend on these legacies. Statutory frameworks define some of the implementation norms such as organizational leadership, resource allocation decisions, etc. Public opinion and legislative actions affect politics of privacy. Post September 11 changes in public opinion and legislative interventions (e.g., the Patriot Act) clearly show an increase in
demand to centralize and improve efficient use of administrative resources and proprietary personal information. Popular outrage and media attention to examine the sanctity of these policies have been few implying the need to develop sustainable policies to support data protection laws. Computer matching of records and computer profiling based on user behavior patterns are legacies of advanced technological developments. The privacy implications are enormous. Moreover, businesses find that competitive success and even survival today depends on their ability to exploit fully the proprietary personal data collected through transactions. A digital persona is not only useful for the government to presage the criminal or terrorist behavior of an individual or group but also fruitful for the business to hone in on the individual and collective preferences of the consumer. The advent of the Internet and World Wide Web blew away the notion of a bounded data bank. Because the data protection statutes have become insensitive to differing organizational and technological contexts, the Council of Europe developed a more refined series of recommendations for data protection in a variety of fields such as social security, direct marketing, medicine, and scientific research. It is clear that the emerging interdependence of both the problems and solutions would significantly affect the statutory, political, and technological contexts of data protection policies. A direct result of these developments is the trans-border data migration regulations that apply to a growing list of countries. In addition, the cultural differences and their concomitant attitudes towards privacy and intellectual property rights make it impossible to determine the global success of any policy. Nevertheless, privacy is becoming a universal concept and has to be addressed by governments, businesses, and consumers.

Farber (Farber 2004), citing Garter group analyst Hunter, states that in order to establish trusted relationship with customers, firms would want to adopt a privacy management
framework that comprises three parts. Following Flaherty (Flaherty 1989), the framework yields a policy architecture akin to the statutory framework, a compliance architecture similar to the political dimension, and a technology architecture comparable to the technology dimension.

Policy frameworks that define privacy vis-à-vis data protection and within the contexts of the four statutory, political, technological, and international dimensions provide a basis for defining the privacy trust bank. The statutory dimension enables us to define business financial risk of maintaining private proprietary data. At this dimension we can also develop measures of the value of privacy and exchange premium for personal data in the secondary market. Because valuation and maintenance come into focus here, organizational and control aspects can be addressed as well.

The political dimension contributes to the regulatory and enforcement factors. Because the good intents of bureaucracies, governments, and other data collection agencies result in excessive surveillance and monitoring of individuals, strong data protection standards and transparencies of process are essential. Political support for transparency has normally waned during periods of strife and instability and often results in more secrecy and increased lack of trust. Because public opinion can be affected, a trust bank should be designed to withstand the loss of resultant transparency.

Perhaps the most significant dimension is technology. The extraordinary variety of technology, its immense integrative capability, and the capture and dispersion of personal data in almost every walk of life is astounding. Capability exists today to cast a net as wide as possible to pull in every element of a person’s life and reconstruct not only a replay of their life but predict potential behavior. Adequate protective measures must therefore be available to safeguard the trust bank. Because the technology exists and will be used, as recent revelations of
computer matching of travel records show, a trust bank must provide safe harbor provisions for the consumer.

Grossman (Grossman 2000) describes the notion of providing privacy through circles of trust. Circles of trust, where each circle of trust is made up of local names, given meaning by their context and used only for a limited number of reasons, are designed to grow together. The circles start at the local level, giving a sense of vouching, and continue to grow in reach and credibility while doing away with the need to have a global identifier. After all, the basis of the idea is that it is your local circle of friends that credibly vouch for you and therefore any trust must begin at the local level. Privacy and trust building are essentially a social activity. Camp (Camp 2003) argues that Privacy is both operational (in the sharing of data) and internal (based on user perception of privacy). Any design for trust in any digital environment requires an understanding of not only the technical nuances of security but also the human subtleties of trust perception.

(Jarecki, Lincoln et al. 2003) proposes a mechanism that provides cryptographic filters on the mining of personal data, enabling efficient mining of previously-negotiated properties, but preventing any other uses of the protected personal data. Their approach does not rely on complete trust in the analysts to use the data appropriately, nor does it rely on incorruptible escrow agents. Instead, they propose conditional data escrow where the data generators, not the analysts, hold the keys to the data, but analysts can verify that the prenegotiated queries are enabled. Their solution relies on verifiable, anonymous, and deterministic commitments which play the role of tags that mark encrypted entries in the analyst's database. The database owner cannot learn anything from the encrypted entries, or even verify his guess of the plaintext on which these entries are based. On the other hand, the verifiable and deterministic property
ensures that the entries are marked with consistent tags, so that the database manager learns when the number of entries required to enable some query reaches the pre-negotiated threshold.

Ownership of information implies direct control and benefit of the use of the information. Information is an asset that persists. The ownership of the asset is with the individual, but that does not allow them to destroy it. They have the authority or ability to decide how it may be put to use and will receive direct benefit from that use, whether monetary or otherwise. In the same way that Americans exercise freedom within the constructs of the constitution and society, the DP also must exist with constructs. Therefore, one cannot simply erase information about themselves, or destroy their DP, because by doing so, trust is violated.

3.2. Trust Bank

A TB is a repository of DPs. Because most individuals either lack the technical ability or willingness to maintain their own persona, the TB acts as an agent for them. In a fashion similar to a credit agency storing information about individual’s credit rating, a TB stores all transactional information about consumers. However, a major difference is that the TB operates for the benefit of the individual and not the organization, although the organization will also benefit. The consumer can interact with the TB to determine how much information they want to disclose and to whom those disclosures may occur. This may be accomplished through a few different ways. One is to allow an individual to log into their account and select preferences much like the customizable news readers. This would occur through a series of categorical check boxes. For individuals not as technically savvy, this could occur through a telephone conversation with a TB service representative or a mailing. Individuals may alter their trust preferences at any time, and the TB should make timely reports to individuals about who is requesting what information about them. The TB should be funded solely by the individual
members, whether through annual fees, or percentages of income generated by the secondary information transactions. This funding mechanism is similar to voluntary consumer reporting organizations, and thus maintains independence from outside interference or influence.

Once preferences are stored in the TB, then interactions with organizations may transpire. If an organization has established trust with TB then they may lease information about individuals for a fee/discount that directly benefits the individual. If an organization violates trust, then their trust level may be decreased, thereby incurring a market penalty. Periodic audits and customer feedback ensure trustworthiness of participants. The information contained within the TB is subject to laws and regulations affecting privacy.

3.3. Individual Control of Digital Persona

We propose transferring the locus of control of personal data from organizations to the individual. Firms would have access to all of these data and more through negotiated exchange of personal data from the consumer. Furthermore, the economic benefit of post transaction data rests primarily with the consumer. To accomplish this we separate the economic benefit of transactions into two stages. In the first stage economic benefit goes to the primary parties involved in the transaction (e.g., revenue from sale of goods or services), namely the vendor. Subsequent benefits derived from utilizing the transaction data should go to the consumer. Firms have realized that information about consumers and their purchase behavior is as valuable as revenue generated from transactions, and have proceeded to collect and use consumer data. Transferring the locus of control of the data to the consumer, the economic benefit of trading this data to interested parties can reside with the consumer, and firms gain greater benefit because they will have access to more reliable competitor and affiliate data (Murthi and Sarkar 2003). A primary market currently exists composed of consumers or customers and vendors or suppliers.
Secondary markets result because information about primary market participants has value. Secondary markets are then pure information. Who owns this information? Complete ownership of the secondary market does not currently exist. Bits and pieces are owned by different organizations. Intermediaries are used to bring together disparate information, and producers of the information (consumers) have no say in its control or use. An open and free market place of information can be created when this data resides with the consumer. Consumers and their holistic DP can come together to form the information market place. Transaction economics and free market economic theories suggest that this is a far superior alternative than oligopolistic nature of current secondary market structure (Rust, Kannan et al. 2002).

4. Summary

By transferring control of secondary information to the individual and housing the DP in a TB, organizations can gain greater access to data across multiple sources, and individuals can receive direct benefit to the secondary information market. This will allow organizations to enter different market segments or industries or gather information to better serve customers and increase current market shares. TBs improve accuracy, relevance and currency, and do not necessarily require their participants to be technically savvy. Organizations need not retain detailed customer information because they can access relevant data through the TB. With the framework proposed here, neither organization nor individual suffer for the prosperity of the other.
References


