The Privacy Value

PETER E. SAND, J.D., CIPP*

ABSTRACT

One of the defining characteristics of the Information Economy is the agility and speed with which organizations can define and redefine the services they offer. Accompanying this capability is the pressure to leapfrog ahead at a pace that creates challenges for contemplative assessment of the implications of the new services and service models. In an attention-driven marketplace, one of the most treasured assets is the relationship between the organization and the individual. One of the keys to maintaining this close relationship is personalization, both in service and data. The closer the organization can be to an individual, the better. As an organization approaches the data granularity level of an individual, the accuracy of the data and process and the tailoring of the service through mutual expectation and agreement should move to the forefront of organizational concerns. The confluence of these heightened concerns is "privacy." Ignoring privacy until the end of a development process, or worse, ignoring privacy completely, could drive implementation costs so high that an otherwise helpful service will fail, to the potential detriment of the organization itself. The prescription to this dilemma is to bring privacy protective practices into the existing administrative process during the design phase of the IT development process.

OVERVIEW

One of the defining characteristics of the Information Economy is the unique agility and speed with which organizations can define and redefine the services they offer. Accompanying this new capability is a new pressure to leapfrog ahead at a pace that creates challenges for contemplative assessment of the implications of the new services and service models.

The nature of information technology, and more specifically information itself, is the catalyst for this recent acceleration. Shifting the basis of a service from a physical platform to an information platform frees that service and allows the organization to exploit the speed of communication, the reach of social networking, and the agility of data.

---

* Peter E. Sand serves as Director of Privacy Technology in the Privacy Office of the U.S. Department of Homeland Security and can be reached via e-mail at peter@petersand.com.

In an attention-driven marketplace,[1] one of the most treasured assets is the relationship between the organization and the individual. One of the keys to maintaining this close relationship is personalization, both in service and data. The closer the organization can be to an individual, the better.

As an organization approaches the data granularity level of an individual, the accuracy of the data and process and the tailoring of the service through mutual expectation and agreement should move to the forefront of organizational concerns. The title for the confluence of these heightened concerns is "Privacy."

Ignoring privacy until the end of a development process, or worse, ignoring privacy completely, could drive implementation costs so high that an otherwise helpful service will fail, to the potential detriment of the organization itself. The good news is that designing privacy protective practices is relatively easy and can be made part of the existing administrative process that creates the very information technology that would raise the privacy concerns.

This short paper addresses the structural nature of information privacy in the context of information technology-driven services. It delivers one message: successful organizations should identify and resolve all privacy issues at the front-end of any development process.

The discussion begins with a brief overview of information privacy, provides a discussion of the structure of potential costs of ignoring privacy protections, and concludes with a presentation of a framework for integrating privacy into information technology procedures and products to preempt failure costs.

INFORMATION PRIVACY

The term "Privacy" is multifarious and is best understood in specific contexts. Here, "privacy" serves as an overarching label for the appropriate use of personal information.

Personal information is any information that can be used in any way to identify an individual. Appropriate use is any use that is founded in law or sound, legitimate, public policy. The specific meaning of "appropriate" in a particular situation can be guided by agreement amongst the parties to the original contribution of the personal information. These terms are broad and may be seen as over-inclusive (some may consider "personal information" to be limited to direct identifiers such as name, social security number, etc.). Potential

---

[1] See Thomas H. Davenport and John C. Beck, *The Attention Economy: Understanding the New Currency of Business* (Boston: Harvard Business School Press, 2001).

privacy issues exist in data and data usage. In fact, some uses can turn otherwise non-personal information into personal information through an intent to use non-identifying data for the purpose of identifying individuals. Broad definitions at the beginning of a privacy analysis offer the greatest return during the analysis exactly because they are over-inclusive. Terms such as "used in any way that could..." capture the intent aspect of a potential use, which can then guide the specific planning process for any potential impacts on privacy interests that may result.

Privacy protective information systems ensure that the information-driven service:

1. Directly advances articulated legitimate purposes;

2. Clearly discloses expected use prior to implementation;

3. Minimizes the collection, storage, and use of personal information;

4. Provides the opportunity for individuals to access, correct, and seek redress regarding the accuracy of relevant personal information; and

5. Secures personal information against unauthorized and/or unintended use.

These quality control measures recognize that the individual maintains an interest in how their related personal information is used by the organization. These are generally the same principles embodied in the United States' Privacy Act of 1974[2] and in guidelines developed by the Organisation for Economic Co-operation and Development's Working Party on Information Security and Privacy.[3]

An organization that reviews its systems, new or changing, for the above privacy protective criteria will be well positioned to address a

---

[2] See U.S. Dept. of Justice, "Overview of the Privacy Act of 1974, May 2004," http://www.usdoj.gov/04foia/04_7_1.html (accessed November 22, 2005).

[3] See Organisation for Economic Co-operation and Development, "OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data," http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html (accessed February 1, 2006).

privacy issue that might arise. The privacy-aware organization would be well-positioned if it could point to a record of thorough assessment and notification from a standardized process embodying the above principles, demonstrating a well-thought, respectful use of personal information.

Ideally, the organization will preempt a potential privacy critique by using the above measures to design, implement, and operate systems that are successful both in terms of their productive effect on the purpose of the system and their preventive protection of the privacy of information within the system.

The next section of the discussion presents the cost of failing to adequately address privacy protection in system design and operations.

THE COST OF IGNORING PRIVACY

THE UNSEEN LOSS

A potential blind spot exists within the typical organization structure between the internal management of business, technology, and security issues. The management of these discrete functions can become isolated. As the walls around each thicken, the gap between them widens until each is facing different directions with little understanding of the products of the other groups and no awareness of how the position of one group impacts the work of the others.

When a system is developed from a blinded organization, the gaps in understanding and the potential for unintended uses of personal information become part of the system, burying the problems deeper. Ultimately, each use of the system exposes the organization to an increasing degree of risk.

- The disconnected business group blinds the organization by failing to communicate exactly what the purpose and success measure is for the use of information.

- The disconnected technology group blinds the organization by failing to communicate exactly what information the system collects and what the system does with the information.

- The disconnected security group blinds the organization by failing to communicate how it

designates and enforces asset and risk categorization and its overall authorization framework.

The immediate risk to the blinded organization is the development of a system that fails to meet expectations and the direct costs associated with the development of a system that may be quickly abandoned – the greater the investment and reliance, the greater the risk. The organization faces a far greater risk the longer it uses the system built from and embodying this blinded state. The more the organization uses a system that operates outside the organization's understanding and control, the more its resources will be drawn further and further away from the intentions of the organization. Ultimately, the organization may find itself in a position where it is operating in a totally different area of business without any of the safeguards normally accompanying an intentional strategic shift.[4]

The magnitude of the long-term risk presented by a blinded operational system is as broad as the reach of the organization's enterprise-wide communication mechanism, compounded by an order of magnitude defined by the volume and depth of the personal information in use and spread as far as public outcry can reach.

THE COST OF TREATING PRIVACY AS A BARRIER

Too many organizations view privacy as an expense and thus as a barrier to profit, progress, and security. Many view privacy narrowly as an artificial restriction placed on freely given information.[5]

---

[4] In a 1998 action against Geocities for misrepresenting its actual use of collected personal information, "Geocities misled its customers, both children and adults, by not telling the truth about how it was using their personal information" (internal quotations omitted). Federal Trade Commission, "Internet Site Agrees to Settle FTC Charges of Deceptively Collecting Personal Information in Agency's First Internet Privacy Case: Commission Establishes Strong Mechanisms for Protecting Consumers' Privacy Online," http://www.ftc.gov/opa/1998/08/geocitie.htm (accessed February 1, 2006). For an index of Federal Trade Commission Enforcement Actions, see Federal Trade Commission, "Privacy Initiatives: Enforcement," http://www.ftc.gov/privacy/privacyinitiatives/provises_enf.html (accessed February 11, 2006).

[5] "'People are paranoid that computers that know where you are can turn against you' [quoting a panelist]. Social obstacles to location-aware computers mainly surround privacy issues where people are concerned their movements will be tracked by Big Brother." "Panelists unanimously dismissed privacy concerns.... 'The benefits of being able to pinpoint things precisely easily outweigh the negatives,' [quoting a panelist]." Tom Spring, "Location Reigns Supreme with Future PCs: MIT Conference Looks at the Future of Location-Based

Privacy is equated with secrecy, and secrecy equated with a blockade on otherwise productive data. According to this view, stronger privacy protection means less available data, which means less available information-driven services, which means more barriers to progress.

The correlating belief is that once data becomes physically accessible it can be used for any purpose. The theory is that once information is accessible, from whomever, through whatever means, it is no longer "secret" and thus no longer private.

The underlying premise is that the individual's sole point of control over personal information is a right of first refusal. Once the "secret" is known, it becomes a marketable "good" in the new information economy. From this perspective, the lesser and later the investment in privacy, the better.

Organizations that hold this belief rush ahead into new uses of more personal information and miss the accompanying risks. They lack an enterprise-wide view into the gap between the management areas they do understand (service development, technology, and security) and are totally unprepared when a privacy breach occurs. The greater the avoidance, the more damaging the consequences.

As a pragmatic matter, information sharing, specifically between individuals and organizations, is not limited to the simplicity of secrecy/publicity. The expectations of individuals, internal and/or external to an organization, regarding appropriate use, and more often inappropriate use, guide future uses of information regardless of how an organization acquired the data initially.

Organizations should recognize the reality of the expectation model and respond by clarifying internally what data is collected, why, and its uses. This internal awareness should be used to frame the expectations of individuals (internal and external to the organization), prior to collection. The greater the organization's preparation, the greater its protection, hopefully prevention, for potential future privacy complaints and publicized action. The earlier the organization begins preparation, the better.

THREE SCENARIOS

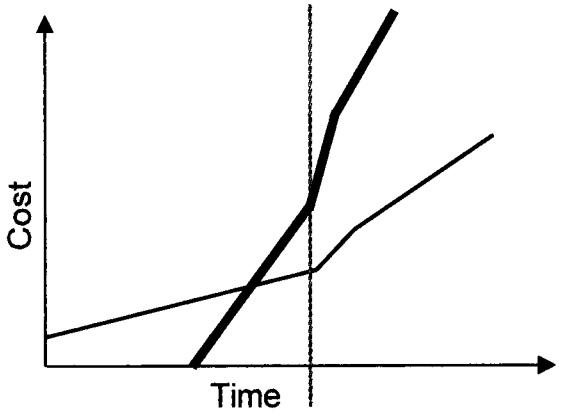
Below are three *descriptive* cost models that show the relationship between early investment in a privacy program to the recovery and long term costs should an event occur (vertical line). Each of these

---

Computing," *PC World.com*, October 1, 2004, http://www.pcworld.com/news/article/0,aid,118031,00.asp.

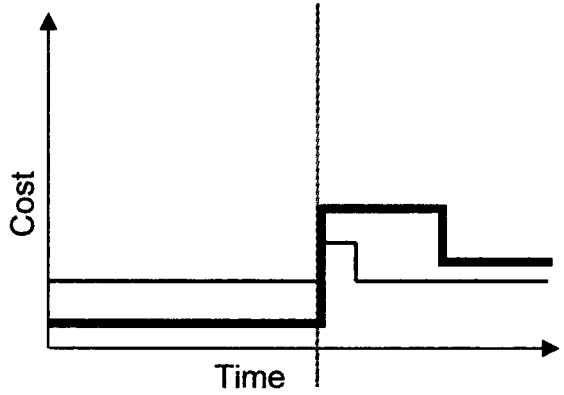
models shows a base-line approach (thin line) and an extreme approach (thick line). These models show the success of a high initial privacy investment and the danger of a last minute /reaction.

THE WORST CASE SCENARIO



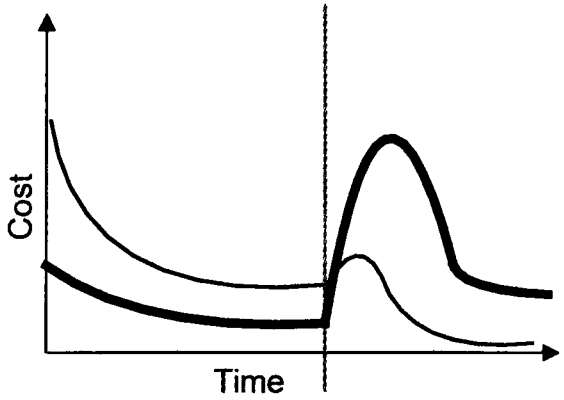
In the worst-case scenario, the base-line organization (thin line) invests very little in privacy protection early on. Crisis hits and the response is dramatic. Costs accelerate and continue to increase over the long term. In the extreme version of this scenario (thick line), the organization only invests when it senses the crisis approaching. The recovery costs are tremendous and because the organization cannot remove the systemic problems that plague its internal operations, costs continue to ramp up as the organization continues to repeat the pattern of rushed solutions. In a severe case, the green line could become so steep, the costs so high, that the business becomes unsustainable.

THE MEDIOCRE SCENARIO



The mediocre approach, less extreme than the worst-case scenario, shows an even investment in privacy protection over time. When crisis hits, there is a modest recovery period, followed by a return to business as usual. The cost base remains constant over time but there are no future cost savings. The extreme version of this approach invests less leading up to the event, has a longer recovery period and spends more over the long term than the baseline organization which invested more upfront.

THE IDEAL SCENARIO



Ideally, costs should decrease over time. In this diagram, the thin line represents the well-planned approach that incorporates privacy into the original system and program design. The thick line represents a similar attempt, one that is only partially committed. The difference

between the thin and thick lines illustrates that a higher initial investment in privacy protection drives a greater cost savings over the long term.

SIGNIFICANCE

The severity of the cost differential between the best and worst-case scenarios is determined by the extent to which the organization incorporates privacy protection into its business and information technology system design. If privacy protections are properly built into the operations from the start, at the initial design stage, there is a lower recovery cost and a much lower overall cost. If privacy protections are addressed only after a crisis occurs, then the resulting costs can be tremendous, even fatal.

Properly integrated privacy protection provides the organization with a unique view into what information it uses, what it does with that information, and how that use compares with the stated purpose (or expectation) of the original collection. Without the clarity that privacy delivers, an organization will not understand the risk or consequences involved, and may be forced to incur great costs in responding to both the immediate and systemic failures under the crisis pressures.

Overall recovery cost is a function of the size of the initial investment in privacy protection. A greater investment in privacy early on, limits the cost of responding to a crisis and also limits the post-crisis long-term costs.

At a minimum, the cost of failing to adequately understand and integrate privacy protection into the organization's operational mechanisms can be defined by the intimately related costs of information security breaches, specifically failures to adequately secure stored personal information.

Personal information is a unique information asset. It holds special value in its role as a touch-point and binding element of the personalized service model of the attention economy. Personal information by its very nature presents a substantial concern for the organization: potentially volatile, outstanding liability. The intimate and persistent connection between personal information and the individual to which it refers creates a bond such that any actions affecting the information also affect the individual.

When an organization loses control over personal information, the individuals tied to that data are immediately affected by the disruptive forces of uncertainty as to who now possesses the personal information, what that unknown person or organization might do with

the personal information, and how those subsequent uses might affect the individual.

The most widely held concern is identity theft, the direct costs associated with the actual theft, and the associated costs involved in clarifying financial records after the fact. When the volume of data lost numbers in the millions of records per security breach,[6] the organization that loses control over personal information potentially faces direct costs associated with repairing the breach and the associated costs involved in the role it may play coordinating with each individual affected by the breach (potentially millions).

PRIVACY FRAMEWORKS

The following overview presents two related frameworks for integrating privacy protections into the use of personal information within systems. The first framework presents a conceptual model for integrating privacy into the technology development and management process. The second framework presents a list of specific questions that will inform a detailed assessment of potential impacts on privacy protections.

THE FULL PRIVACY INTEGRATION

Information technology is a service and as such should be designed in response to a request for new or improved use of information. A well managed and developed system remains closely tied to the original request and seeks to deliver only exactly that capability requested.

The intimate connection between the request and the capability offered as a response becomes more important when the information is personal: when it could be used in any way to identify an individual. This pivot point can arise early in the system design phase when the information is first defined; it can also arrive later as the use of otherwise non-personal information changes and the available data is suddenly used in a way that could identify individuals. Once the

---

[6] The Privacy Rights Clearinghouse maintains a running total of privacy/security breaches since the ChoicePoint announcement that 145,000 individual records containing personal information were mistakenly shared. The Clearinghouse refers to this as the Choicepoint "watershed event." Other events reported include misplaced laptop computers, hacking, lost backup tapes, and insiders, totaling over 51.6 million individual records; *See* Privacy Rights Clearinghouse, "A Chronology of Data Breaches Reported Since the ChoicePoint Incident," http://www.privacyrights.org/ar/ChronDataBreaches.htm (accessed February 1, 2006).

privacy pivot point reaches the individuals associated with the data, suddenly each individual related to the data (at least one individual per record of personal information – potentially millions in total) may have an interest in how that personal information was used, by whom, and how that actual use compares to the individual's expectation at the time of the initial collection.

If an organization is going to face potential responsibility to each person referred to in its data collection, the organization should design rules regarding the handling of that information at the same level of granularity as the data it keeps. The most important element is organizational awareness of the personal information it maintains and the context and strategy for each data set. Awareness requires a process of always knowing what information is collected and used and why, as well as addressing or managing all expectations surrounding that data set.

There is one primary method an organization can use to identify and maintain the level of awareness: a privacy-informed, regularized process for building and maintaining information systems. A habitual practice enables the organization to rely on the integrity of the final result with the assurance that each system successfully passing through a rigid series of quality thresholds will protect both the organization's interests and the organization's potential responsibilities to individual data subjects.

The details of a particular organization's structured development and management process should be formed organically to match the organization's character and values. It is more important that the process be followed consistently and comprehensively than it match an idealized perfect standard. Once institutionalized, the informed practice of privacy protection will improve through use and grow as the organization grows, evolving into a specifically tailored "best practice."

The structured process should devote sufficient attention to thoroughly identifying and addressing all business, technical, and privacy issues early in the process, so that the decisions made on these issues can be built into the system from the start. Early analysis reduces the likelihood of post-development (or worse, post-deployment) changes to or eliminations of the system.

The key component to this structured process is to incorporate privacy evaluations into the life of the process. At each logical stage[7]

[7] System development life cycles typically contain a design stage, a development stage, an implementation stage, an operational stage, and ultimately a review and transition/disposal stage.

a basic privacy assessment should be conducted that explores the relationship of the expected value of the system (the purpose), the information used by the system (the data – with an emphasis on personal information), and the important primary uses of the data to deliver value (the functionality). Provided that the right steps are included in the structured development and management process, and that each step is consistently followed, the organization can confidently rely on its routine operations to deliver a meaningful understanding of what personal information, if any, it uses and why.

In addition to a routine practice of knowing exactly what information is collected and used, it is important to also conduct specific privacy protection inspections. The following section identifies the most important considerations to include in a full privacy review.

PRIVACY IMPACT ASSESSMENT

A thorough privacy analysis includes at least six different, related subjects. Addressing these considerations provides the organization with a comprehensive view of the potential risks it may face by inappropriately using personal information.

1. *Personal Information.* All personal information should be defined in a way that is consistent and meaningful for all decision makers (business, legal, and technical). This expands the organization's awareness of what risks and responsibilities may exist.

2. *Information Use.* All uses of personal information should be clearly articulated and limited to those collections and processes that are absolutely necessary to achieve the purpose of the system and the goals of the organization. A clear understanding of the nature and life span of a particular use of personal information will also identify data retention periods and more specifically, when personal information should be removed from the system. This manages expectations and minimizes exposure to liability.

3. *Individual Authority.* As discussed above, a bond exists between the individual and related personal

information. The organization should consider what rights the individual should have to understand and influence the use of that personal information. This also manages expectations and therefore risk and liability.

4. *Information Sharing and Disclosure.* This is a subset of information use and deals specifically with data transfers. All transfers should be supported by thorough, written understandings regarding how the recipient will use transferred information and how that use compares with the expectations set at the time of the original collection. This is a more focused effort to expand awareness, manage expectations, and minimize risks.

5. *Privacy-Sensitive Technology.* There are certain technologies that raise particularly heightened privacy concerns either through the concern that they intrude deeper into the personal aspect of individual's life or body (biometrics, data mining) or are particularly easy to overlook (RFID). Any use of these special technologies should be further reviewed, articulated and communicated. Like information sharing, this too is a further effort to focus awareness and expectations on those areas where deeper concerns are raised.

6. *Security.* A major part of ensuring appropriate use is preventing inappropriate use. A thorough discussion of privacy protection includes a detailed discussion of how security standards and practices can best assure both the organization and the individual that unintended parties will not misuse the collected personal information.

THE PRIVACY VALUE

Conventional organizational structures account for the three traditional primary information management groups: business,

technology, and security. These primary groups are responsible for defining the foundational data, the specific purposes, uses, functions, and limitations that ought to guide all organizational information practices. Each of these groups is focused on separate aspects of the use of information. Absent a reinforced process of communication, there will be gaps between these different groups and the policies and practices each advocates.

In those organizations that appreciate the value of continuing close coordination and communication regarding the use of information, the potential still exists for a blindness related to the collection and use of personal information.

Privacy is the best lens through which to identify the collection, storage and use of personal information, and the potential accompanying issues and liabilities. A well-integrated approach to privacy protection raises awareness and improves overall organizational strategies regarding how best to use information generally and personal information in particular. An integrated approach to privacy protection can also bring new awareness of the laws, regulations, best practices, and trends that affect the value and responsibilities that accompany the use of personal information.

Some organizations approach privacy with this higher level of awareness. Other organizations either ignore privacy completely or treat it as a cost. The latter group of organizations believe that more personal information will deliver more opportunity for more personalized services and through those services, more growth for the organization itself.

An organization with an absent or under-developed privacy program will continue to face threats against one of its core assets, personal information, without the ability to avoid or overcome those challenges.

The term "privacy" signifies different things in different settings. The information economy and attention marketplace are defined by the fast-paced agility of the new information-driven environment. Both organizations and individuals can benefit from the new advantages information-based services offer.

With this great potential for progress comes an accompanying layer of complexity in managing the use of personal information and the associated expectations regarding how that use will be defined. A fully integrated approach to privacy, and an organizational operational awareness of what privacy means for that specific organization, and the information that organization uses will remove potential blind spots and truly enable the organization to succeed in the modern information-driven environment.