Privacy Office
U.S. Department of Homeland Security
Washington, DC 20528

PAPER ABSTRACT : "THE PRIVACY VALUE"

The following abstract is offered for inclusion in the program of the Fourth Workshop on the Economics of Information Security, hosted by the Kennedy School of Government, Harvard University, June 2nd and 3rd 2005.

About the Privacy Office of the U.S. Department of Homeland Security: The DHS Privacy Office is the first enterprise-level privacy office in the federal government, led by Nuala O'Connor Kelly, the first statutorily-mandated Chief Privacy Officer. The Privacy Office is organized along several verticals: Legal, International, Disclosure, Compliance and Technology.

This paper is part of an ongoing program of outreach and collaboration, continuing the integration of privacy protection in all discussions of the appropriate use of information and the role of government for business and society.

THE UNSEEN LOSS

The defining characteristic of the Information Economy is the unique agility and speed with which corporate and government organizations can define and redefine the services they offer. Accompanying this new capability is a new pressure to leapfrog ahead at a pace that rarely allows the opportunity to examine the minutia of each step forward.

In an attention-driven marketplace, the most treasured asset is the relationship between the organization and the individual (the individual employee, customer or citizen). The keystone of this relationship is the individual's trust that the organization will use the individual's personal information appropriately. "Appropriate Use" generally refers to actual use that furthers an articulated, legitimate purpose, which was communicated prior to the collection of the personal information. Trust is created when the individual first shares personal information and lasts for the life of the information.

An organization, corporate or government, remains successful as long as it can sustain the trust relationship with the individuals it serves. Trust is embodied in the personal information and is won or lost each time that information is used.

The more services the organization develops and the more "personal" and interactive those services become, the greater the threat to this trust. If the threat is realized, the organization faces an iceberg of damage. The small incident above the surface is actually driven by a much larger systemic failure underneath.

Unfortunately, most corporate enterprises and government agencies follow conventional organization structures which suffer from a blind spot between the management of business, technology and security. Without a clear sense of what personal information is absolutely needed and how it will directly advance an important purpose, the organization risks collecting more data than it will use and using the information it collects in ways it may not fully acknowledge.

In order to see into this blind spot, the organization must change the way it manages its operations. A new framework is needed that can identify personal information (and thus locate the core of individual trust) and oversee the consistency of use from the point of original collection through all phases of integrated uses including the final disposition.

Privacy is the discipline that provides this much needed framework. An integrated privacy office would ensure that the crucial relationship between the organization and the individual is maintained as the corporate enterprise or government agency races ahead to build new and improve personalized online services.

Some organizations approach privacy in this way, however, most either ignore privacy completely or treat it as a cost. This last 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 its core asset (personal information) without the ability to avoid or overcome those challenges.

THE COST OF TREATING PRIVACY AS A BARRIER

Too many organizations view privacy as an expense subtracting from the bottom line and as a barrier to safety and security. Many view privacy narrowly and as an artificial restriction placed on freely-given information. The term "Privacy" is equated with "secrecy" and the belief is that the individual's sole point of control is a "right of first refusal". Once the "secret" is known, it becomes a "good" in the new information economy. From this perspective, the lesser and later the investment in privacy the better.

These organizations seek additional uses of more personal information but cannot see the accompanying risks. They lack an enterprise view into the gap between the management areas they do understand (service development, technology and security) and are totally unprepared when an event does occur. The greater the avoidance, the more damaging the consequences.

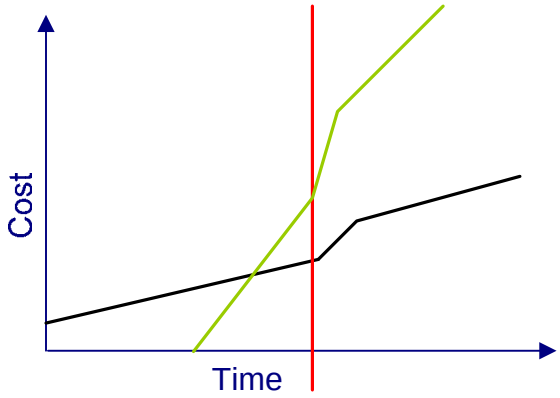
THREE SCENARIOS

The following three cost models show the relationship between the initial investment in a privacy program to the recovery and long term costs should an event occur (red line). Each of these models shows a base-line approach (black line) and an extreme approach (green line). These models show the success of a high initial privacy investment and the danger of a last minute reaction.

THE WORST-CASE SCENARIO

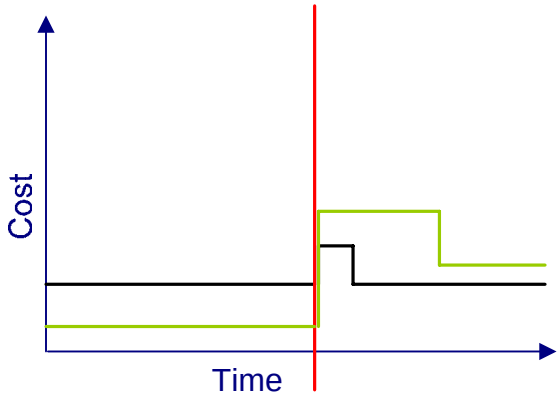
In the worst-case scenario, the base line organization (black line) invest very little in privacy protection early on. The crisis hits and the response is dramatic. Costs accelerate and stay higher over the long term. In the extreme version of this scenario (green line), the organization only invests 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.



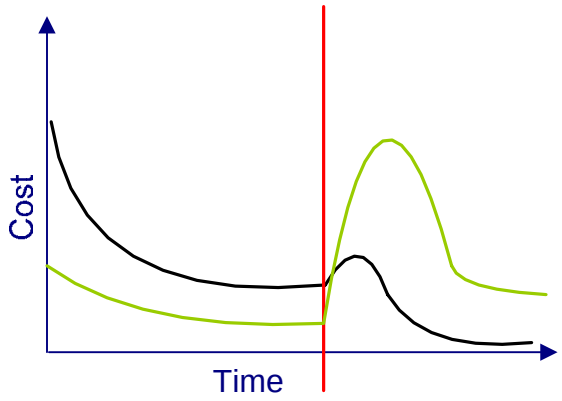
THE MEDIOCRE SCENARIO

Less extreme than the worst-case scenario, the mediocre approach shows an even investment in privacy protection over time. When the 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. However, the extreme version of this approach invests too little 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 SITUATION

Ideally, costs should decrease over time. In this diagram, the black line represents the well-planned approach that incorporates privacy into the original system design. The green line represents a similar attempt, but one that is not fully committed. Even though the black line shows a higher initial cost, going forward, the difference between the black and green lines shows a higher recovery cost and a higher long term cost after the threat.



SIGNIFICANCE

The severity of the cost differential between the best and worst-case scenarios is driven by the extent to which the organization incorporates privacy protection into its business system design.

If privacy protections are properly built into the operations from the start, at the initial design stage, then there is a lower recovery cost during 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.

Privacy provides the organization with a unique a view into what information it is using, how it is using it and how that use compares with the original purpose (or expectation). Without the clarity privacy delivers, an organization will not understand the risk or consequences 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 limits the cost of responding to a crisis and also limits the post-crisis long term costs.

THE PRIVACY VALUE

The most visible gain of a properly-integrated privacy program is the resilience of the organization to a crisis. The less dramatic but more meaningful measure is the ability of the organization to avoid the crisis completely and to consistently and reliably increase trust and reduce cost.

In the information economy, trust is the cornerstone of success. This is as true for government agencies as it is for commercial enterprises. An organization that understands the value of trust and the embodiment of that trust in the use of personal information will easily see the value of integrating privacy protection within its management and leadership structures.

An organization that operationalizes privacy protection faces less risk, incurs less cost, retains more individual trust, uses more information to build more services and is in the best position to be propelled by the information economy.