A Privacy Expectations and Security Assurance Offer System

Jeffrey Hunker
Carnegie Mellon University
Pittsburgh, PA 15213 USA
01 202 257 7778
jhunker@andrew.cmu.edu

ABSTRACT
Consumers accessing web sites for information or to purchase products face limited opportunity to express their privacy preferences, and even less recourse if security violations lead to inadvertent disclosure of privacy sensitive information. A privacy expectations and security assurance offer system is proposed in which on-line organizations with web sites offer consumers, in exchange for a fee, a choice of privacy preferences and information security levels; if privacy is violated under the terms of this privacy expectations and security assurance instrument, consumers will be compensated. The proposed offer system directly links responsibility and accountability for security of privacy information to the on-line organization, and has other benefits. Adoption is problematic, and will require market experimentation.

Categories and Subject Descriptors
K.4.1 [**Computers and Society**]: Public Policy Issues – Privacy, Regulation; K.4.4 [**Computers and Society**]: Electronic Commerce – Security; J.4 [**Social and Behavioral Science**]: Economics; H.4.m [**Information Systems Applications**]: Miscellaneous; J7 [**Computers in other systems**]: Consumer products.

General Terms
Economics, Human Factors, Legal Aspects, Management, Measurement, Security

Keywords: Insurance, privacy, incentives, e-commerce

1. INTRODUCTION
Consumer privacy is a 'red herring,' said Scott McNealy in 1999. 'You have zero privacy anyway. Get over it.' [34] Perhaps no statement better captures the frustration over establishing meaningful privacy mechanisms for information provided by consumers over the Internet.

This paper deals with a special, but important case, of privacy -- where consumers (including, importantly, business customers) access Internet web sites for information or purchases, and organizations ('privacy providers') state or negotiate with consumers the amount, type, and use of information that consumers provide to the organization.

NSPW'07, September 18–21, 2007, North Conway, NH, USA.

In both the social sciences and in the more recently emergent fields of human-computer interaction (and security) (HCI, HCI-SEC) there is a raft of work on privacy in computing. [6,7,8,28,29,31] A central theme of this work is to develop privacy enhancing approaches that are both 'useful and usable.'[28] The proposed system builds on this work. [2,9,10,14,17,25]

2. PRIVACY PROTECTION TODAY
Privacy protection is widely understood as the right of individuals to control the collection, use and dissemination of their personal information that is held by others. [11]

Consumers are concerned about protecting their privacy on the Internet. A recent survey reports that 73% of consumers are either very or somewhat concerned about their privacy on-line. [13]

A wide array of laws, standards, and practices define current privacy protection practices. Their basis is a set of Fair Information Practices, which the FTC notes as

- Notice/Awareness
- Choice/Consent
- Access/Participation
- Integrity/Security, and
- Enforcement/Redress [13]

Many different approaches: The EU relies on comprehensive legislation (the European Commission Directive on Data Protection) that, for example, requires creation of government data protection agencies, registration of data bases with these agencies, and, in some instances, prior approval before personal data processing may begin. [35]

The US, in contrast, uses a sectoral approach that relies on a mix of:

- *Legislation and regulation*, including Gramm-Leach-Bliley (financial services), Health Insurance Portability and Accountability Act (HIPAA) (health care), the CAN-SPAM Act, the Children's On-line Privacy Protection Act, the Fair Credit Reporting Act, and the Electronic Communications Privacy Act. Section 5 of the Federal Trade Commission Act prohibits deceptive or unfair practices, including those related to privacy practices.

  In addition a number of *s*tates (led by California) have enacted laws, inconsistent in their application, that require organizations to disclose any security breach of unencrypted personally identifiable information viewed or acquired by an unauthorized person.
- *Self-Regulation* chiefly involves the posting and implementation of privacy policies on web sites. Survey

work by the FTC and others suggests that most sites (and almost all frequently visited sites) have posted privacy policies. [13] In addition, browsers allow users to configure their preferences for the acceptance and retention of cookies. Using its authority, the FTC has brought a number of cases to enforce the promises of privacy statements.

A number of approaches have been developed to enhance privacy self-regulation. The Platform for Privacy Preferences (P3P) protocol creates user defined privacy preference agents to compare preferences with machine readable privacy statements made by various web sites; it has not been widely adopted. [11] Several on-line privacy seal programs (e.g., TRUSTe) are available, some of which provide a 'safe harbor' signifying compliance with the EU Data Protection standards. VISA and MasterCard have developed the Payment Card Industry Data Security Standard, which member institutions follow to protect credit card transaction information.

Security violations affecting personal privacy information are rife: 'Security' defines mechanisms to provide data confidentiality, integrity, and authentication. In December 2006 the U.S. Privacy Rights Clearinghouse reported that over 100 million records of personally identifiable information had been compromised since February 2005 as a result of security blunders.[37] Typical recent headlines include "Massive security breach at UCLA" (exposing personal details of 800,000 former and current students), "IRS Fails Security Audit, 490 computers missing in 3 years,' 'Lost Disc Puts 2.9 million Georgia residents at risk for ID theft,' 'TJ Maxx Probe Reveals Data Breach Worse Than Originally Thought,' and so on. [3] Some of these privacy related security violations are the result of hacks, some the result of loss of physical media, and some (like the posting by USDA of personal information of farmers) the result of careless policy.

Security violations highlight problems with the current systems for privacy protection:

- There is no natural symmetry between security and privacy. Although a privacy providing organization must have security provisions to ensure privacy, having a privacy policy does not imply security, and having secure infrastructure does not imply privacy. [15] When it comes to violations of security related privacy policy, there is at best only a very weak link between responsibilities for the security of personal privacy related information, and accountability for the lack of security. Typically, the organization responsible for the privacy related security breach suffers embarrassment (if made public), and (sometimes) the costs to offer customers free credit monitoring services. The impact of public embarrassment may be limited; the stock price of TJX Companies (the parent of TJ Maxx) was not noticeably affected by being the source of one of the largest privacy security breaches to date. [27]

Much of the expense associated with stopping fraudulent activity related to credit cards (canceling or reissuing cards, stopping payment, and refunding customers) are absorbed by the issuing banks; the issuing banks working with the (culpable) merchant organization may be penalized with fines by the credit card organizations (VISA, etc) if the merchants they work with are found to be in violation of the Payment Card Industry's data security standards.

Legal redress for privacy related security breaches is difficult. In a recent court case an employee of Brazos Higher Education Service Corporation had stolen a laptop with files related to as many as 550,000 loans. A victim sued Brazos for breach of contract, breach of fiduciary duty, and negligence. Brazos, regulated under the privacy standards of Gramm-Leach-Bliley, was granted a summary judgment in its favor, based on the fact that Brazos had demonstrated a reasonable standard of care (e.g., Brazos had written security policies, risk assessment reports, and 'proper safeguards for its customer's personal information'). [30]

- Consumers face a bad set of choices. There is no standard format for web-posted privacy policies (even in regulated sectors, like those under Gramm-Leach-Bliley), so privacy policies are frequently hard to understand, and even self-contradictory. [8,12] Furthermore, consumers often face a 'take it or leave it' posted privacy policy, with no opportunity for selecting different (higher) desired levels of privacy protection. The take it or leave it approach means that in practice that a consumer who specifies no cookies on their browser is not going to be able to visit many web sites.

More subtly, but important, is the 'race for the bottom' that is a function of the 'market for goodies' in exchange for personal privacy related information.[5] This market for goodies typically takes two forms – either 1) provide us with lots of personal information and we will give you something (e.g., a discount of 1-3%, as in the case of my local supermarket chain) or 2) a pay for tracked performance model ---visit our advertisers, or buy our products, and we'll give you something. This 'market for goodies' caps privacy protections – a consumer can only reduce their privacy protections from the baseline, not increase them. There is little or no market for privacy providing organizations to offer consumers high levels of privacy, or to compete with each other for enhanced privacy rights.[8]

3. PRIVACY EXPECTATIONS AND SECURITY ASSURANCE OFFER SYSTEM

This paper proposes that privacy providing organizations offer to consumers a two step offer (or auction – this will be discussed later in this paper) supplemented by a 'no-brainer' simplification of privacy policy formats. The proposed system would directly tie privacy protection goals (which express desired protection of consumer privacy rights) and security policy (to close vulnerabilities which threaten consumer privacy) with consumer privacy values:

3.1 Privacy expectations and security assurance instrument

When a consumer accesses a web service, and the organization requests information, it would do so in a two step process:

- *First Step: Privacy Rights Expectation Offer:* The policy providing organization would provide a set of privacy offers: 'Here's how we will treat your information as a baseline' and 'here's how we will treat your information

if you pay us 'x,'' and so forth. This sets consumer expectations.

The payment could be presented as an 'annual fee' similar to many credit cards.

- *Second Step: Privacy Rights Security Assurance Offer:* 'If your policy is violated by (describe the conditions) we will pay you z' (or take other actions). This would be augmented by saying 'We will use procedures A, B, C to protect your information,' so the consumer could buy different mechanisms for protecting the data. This would be tied to penalties for violation ('we will pay you z'); if the expectation is 'no release to anyone' and the mechanism purchased is 'baseline protection mechanisms,' then the penalty for information leaking probably should be less than if the mechanism purchased were 'information on isolated systems only, trusted user access.' Thus, expectations could be tied to both assurances and, with more specificity, to mechanisms for implementing assurances.

A 'no-brainer' (and hence not half baked, though perhaps not politically feasible) policy change would augment the effectiveness of the above two step offer system:

- A standardized format for privacy policies would be required; the FTC has already made proposals along this line. A standardized format for privacy policies, much like the food label required by the Nutritional Labeling and Education Act, or the EnergyGuides required by the 1975 Energy Policy and Conservation Act, would allow consumers to quickly assess whether a particular sites privacy policy options satisfy their privacy goals. [12,14]

3.2 Benefits of Proposed Instrument

The proposed system has a number of advantages:

Enhanced consumer privacy choice: Consumers would have a set of choices where, quite literally, 'they could put their money where their mouth is.' The proposed system returns to the consumer some measure of control over their information. Particularly if the price established for limiting widespread consumer information distribution is low, consumers would have an effective tool to limit who gets access to their information (likely price levels for the proposed instrument are discussed later).

Creating a market for privacy preferences, by making explicit a set of choices and valuations for privacy.

Direct incentives for privacy providing organizations to care about the security of personal information: Privacy providing organizations would face consequences for failure to adequately implement their privacy policies. In particular, they would face consequences for failing to have adequate security to protect privacy information – a situation they do not face today.

Better enforcement of privacy policy compliance: Today privacy policy violations are largely in the hands of government enforcement agencies. Under the new system, outside groups (e.g., the trial bar) would have a direct incentive to monitor compliance; as the new system would make compliance easier to track, and also open up avenues for civil actions seeking redress (negligence, breach of contract).

Engendering competition for privacy protection: With a market for privacy preferences emergent under this system, organizations would face pressure to consider privacy provisions as part of their competitive strategy. Banks, for example, might compete for customers by offering better or less expensive privacy options than their competitors – i.e., 'we're not only more secure, we provide a higher expectation of privacy for our consumers.'

More, and more informed, investment in security and risk management: Either voluntarily or mandated by law, organizations would invest some/all of their privacy proceeds in improved security, or do some other risk management calculation. Two factors would help structure this risk management process. Consumers would make their own monetary calculation as to how much privacy meant to them. And the trial bar and public interest groups would serve as compliance watch-dogs – for some because of a possible cut of any proceeds from violations. The net effect would be to provide meaningful economic signals to privacy providing organizations as to appropriate risk management choices.

Promote the emergent market for cyber security insurance: The current market for cyber security insurance is small, and boutique-like.[4] A number of issues slow the maturation of this market (dynamic threat, correlated risk in some instances, complex cyber systems) but a major factor contributing to its boutique status is the way the market for cyber insurance operates today -- as a series of specialized 'one off' transactions, somewhat akin to insuring a pianist's fingers, or, of more economic heft, the market for merchant marine insurance. These insurance markets operate without comprehensive and actuarial sound risk histories, unlike, say, the market for auto insurance. What cyber risk histories do exist are proprietary to the insurer and not pooled (again, unlike auto insurance). The demand for cyber security insurance is driven solely by the internal risk management choices of the customer organization. It is not mandated by law, rarely if ever by other institutions, like financing sources, nor is end-consumer demand a direct impetus. Since cyber security measures of typical risk management tools – degree of risk, return on investment, cost of incidents – is at best highly imperfect, the decision, and hence, demand, to seek cyber security insurance is also likely to imperfectly represent economic reality.

Under the proposed system, both the information available to and the demand for cyber security insurance would increase:

- Privacy providing organizations would now be in a situation where they receive a flow of funds (pay us x for the following level of protection (with the following action to secure privacy taken…)), and a question of how to handle the consequent risk. Under the new system, privacy providing organizations would face the choice of, in essence, self-insuring, or, alternatively, of reinsuring the risk by buying a policy with a 'real' insurance company.
- Risk management decisions would be made with more, though certainly not perfect, information. Consumers would be providing information about 1) their privacy preferences; 2) the amount a consumer is willing to pay for this privacy; and 3) the specific levels or types of security that they desire.

Both more information to shape, and more demand for cyber security insurance are positive developments, if you believe, as

does the author, that more robust risk management techniques are much needed in cyber security.

Lay the foundations for a scoring system for organizational security performance: While performance under the proposed instrument would be private information, legal action due to non-performance would be public. Furthermore, privacy public interest groups and risk aggregators/insurers would have an interest in creating a record of performance/non-performance under the proposed system. Creating a unified record of performance/non-performance could either be voluntary, or mandated under law/regulation. In either event, consumers and insurers would have additional information; if, for example, under a voluntary scoring system a privacy providing organization chooses not to provide data, this in itself is useful (though imperfect) information for consumers.

4. CAN THE PROPOSED SYSTEM WORK?

This is a central question, and three different perspectives bear on answering it: 1) the proposal as a form of insurance; 2) the proposal as a social initiative (like Fair Trade Coffee); and 3) a consideration of the various factors that would impede its adoption (e.g., increased burden of consumer choice).

4.1 A Form of Insurance

Economically the proposed privacy expectations and security assurance offer system is a form of insurance. Consumers face a risk of economic (and other) loss, and pay a premium to have a portion of that loss covered if an uncertain event occurs. Is an insurance vehicle as described viable?

In a well functioning insurance market (e.g., for automobile accidents) the probability of a risk event is understood, as are the extent and amount of covered losses. Neither of these conditions holds for cyber related privacy violations, nor for cyber insecurity generally. This has not prevented cyber security insurance products from being offered [4] but these conditions mean that the market is very inefficient.

Consumers do appear to put a positive value on their on line privacy, though researchers have yet to quantify how much people value their privacy, and to what extent this valuation is dependent on context. [19] Consumers state that they value their privacy, but recent work, examining the privacy tradeoffs that individuals will make to gain access to specific services highlights disparities between stated privacy attitudes and actions. [1,18.23] Only a small fraction of all on-line consumers read posted privacy policies. [12] Recent research concludes that personal beliefs about social values play a role – the less desirable the individual believes about a particular trait, the greater the price a person demands for releasing that information. [19] It is not clear that there has been much work, or any conclusions, drawn about personal privacy valuation in the case that consumers face in on-line situations – where consumers face repeated requests to reveal personal information from different sources (web sites) as they cruise the web. Consumer value of their privacy may be affected by the sense that the information they are being asked to reveal is already known or knowable (either from leaks or data mining), or the mere fact of repeated requests may change consumer privacy preferences. Hence, the literature provides little help in answering 'how much might we expect consumers to pay for an enhanced privacy/security assurance instrument' that would be available at many web sites.

Insight can come from several perspectives. A 'market for goodies' has emerged in which consumers provide additional personal information in exchange discounts or free services (grocery store discount cards are an example). [5] Alternatively, the cost of handling privacy related security breaches provides another perspective. Another set of perspectives is the valuation of mailing lists or even more sensitive information sold to third parties by data aggregators, or the value to criminals of information that allows them to perpetrate identify thefts. To summarize these perspectives:

Table 1. Imputed value of personal privacy violations

Privacy Event	Imputed Privacy Value	Source
Grocery store discounts	~$30-100 per record per year	1-3% discount on $3297 annual expenditure on at home food [36]
Free web service and magazine subscriptions	~$30-200 per record per year	Comparison to market cost for similar services
Cost of security breaches	$90-305 per record	Forrester Research [22,26]; Ponemon Institute [27]
Cost of on-line identity theft	$551 per incident (average) -- $150,000 (full blown)	Surveys [33,20]

These estimates are limited in many ways. Grocery store and other consumer merchandise discounts involve limited data disclosure (many people, arguably, are not overly concerned about who knows the details of their grocery purchases), and stores gain other advantages (customer retention) in addition to the value of the personal information. The per-record cost of security breaches involve many unknowns, plus being subject to scale effects. In both cases, the valuation is negative – 'if you reveal this additional information… 'rather than positive 'if we do not reveal this information…'

Most importantly, these estimates do not capture the devastating financial and emotional losses that can result from a full-blown 'catastrophic' identity theft.

The probability of an inadvertent privacy disclosure is unknown. As a condition of receiving cyber security insurance in other instances, underwriters insist on the policy holder implementing a number of security enhancing measures. How premiums for other cyber security insurance products is a trade secret [AIG-- personal communication].

To summarize, both consumers and privacy providing organizations value personal privacy information, and the valuations for a single voluntary or involuntary disclosure of personal privacy information are in the range of tens or hundreds of dollars for a non-catastrophic disclosure. The probability of a cyber related inadvertent privacy disclosure is unknown, but this has not stopped insurance from being offered in other facets of cyber security. It is reasonable to propose, therefore, that in a functioning market with repeated transactions (consumers visiting multiple sites) the valuation of a privacy expectations/security assurance

instrument would be in the order of a few dollars, with a payout in the event of a security compromise in the range of a few thousand or tens of thousand dollars. This very rough going in estimate of valuation is important, because it suggests that a market for the proposed instrument is feasible.

4.2 A Social Initiative – 'Privacy Choice'

With the 'Fair Trade Coffee' initiative, consumers may pay a little more for their coffee because by doing so they perceive aiding a larger social goal that they deem important.[39] Coffee suppliers respond to this demand, or perhaps also from a shared sense of 'doing the right thing.' However, 'in reality, we do not see companies using their privacy policies as differentiators; nor do we see consumers turning away from companies with privacy-invasive policies in droves.' [8].

The proposed system would highlight that consumers do have a choice in their privacy protections. To view the proposal as a social initiative, one has to look through the lens of social activism. Part of the benefits to some consumers would be that they are advancing the protection of privacy overall, and rewarding companies that provide those protections. Part of the benefits to participating privacy providers are reputational.

What distinguishes a "Privacy Choice" initiative modeled after this proposal from existing initiatives, such as various privacy seal programs, is that underlying the "Privacy Choice" initiative is, arguably, an economically viable insurance market. In this manner the proposed system is not dissimilar to the market for carbon credits.

The history over the last decade of carbon credits (reductions in greenhouse gases) suggests that sometimes markets do not just emerge, they are created, and that social awareness is a factor in their creation. Against the opposition of much of the business community, and, at least implicitly, of some governments, carbon credits trading has evolved from a theoretical idea and a novelty item to being on its way to becoming a functioning and permanent global market. The emergence of this market reflects both economic opportunity and political action. A number of public interest environmental groups and their supporters have advocated the use of carbon credits (for what other financial instrument do purchasers place bumper stickers on their cars?). Economists have supported the idea. Some companies (including European companies, whose governments have not supported carbon trading) have seen the financial and public relations value of creating and selling (and, in lesser amounts, buying) carbon credits. Financial bourses have seized the opportunity for leadership in this emerging market. The prospects (real or prospective) of regulations and laws constraining carbon emissions have bolstered the interest in this economically efficient mechanism.

Similarly, several constituencies would have an interest in promoting the proposed privacy expectations/security assurance system. At least some public interest privacy groups would likely support this proposal, though not all. EPIC, for example, in a recent report, noted that:

> Central to the legal and ethical norms for privacy protection is the recognition that individuals should not be required to negotiate or choose among Fair Information Practices. Such negotiations would invariably disadvantage those who could not purchase sufficient privacy and would lead to a gradual decline in the level of protection available to the general public. [11]

It is noteworthy that not all public interest environmental groups have supported carbon credits trading either.

Some socially aware businesses would be likely early adopters of the proposed system. Businesses whose consumer base captures a wide array of implicit privacy preferences (for example, most mass marketers with significant on-line sales, e.g. some book retailers?) might also realize early adopter competitive advantage from offering 'Privacy Choice.' The trial bar would be an enthusiastic proponent of this system. Also, it is hard to say what role business consumers (suppliers or customers of privacy providing organizations) would play – larger business consumers can privately negotiate privacy provisions individually, but small businesses might find the system of great benefit.

Another impetus for adoption would be that, in the absence of a system such as proposed, regulatory action might prospectively impose liability on privacy providing organizations for security failure inadvertent privacy disclosures. The Massachusetts legislature is considering such legislation. [16]

Therefore, it is likely that initially a thin early adopter market for the proposed instruments would emerge, with considerable price discovery initially. As the market matures, competitive/social pressure – e.g.., 'why aren't you offering 'Privacy Choice' choice?' – would (hopefully) create a fuller, more vibrant adoption of the proposed instrument.

5. ISSUES IMPEDING ADOPTION

A number of factors might impede the adoption of this system, including:

Increased burden of consumer choice: One reviewer noted "Imagine a harassed mother of three now not only having to compare the price of groceries, but the privacy standards and compensation involved." Indeed, usability of the proposed system is an important consideration; consumer choice does impose significant costs.[32}

In its least implementable form, the proposal would present consumers with a myriad of individual multiple choices confusingly presented on each participating web site. It does not have to be that way. The privacy expectations and security assurance offer system could be standardized, with, say, two choices (opt-in or decline), with one or more insurance providers underwriting the risk. Creating an insurance opportunity with clear, understandable, and standardized choices would be in the interests of insurers. Credit card companies could, in alliance with privacy providing organizations, provide standardized sets of coverage – perhaps automatically much like additional insurance coverage accompanies many credit cards. In that case, an on-line purchase made with the appropriate credit card would automatically engender higher levels of protection. Perhaps P3P could be used as a platform for offering the proposed system as well. A simple consumer friendly implementation of the proposal is possible; realization of this potential will depend on insurers, privacy advocacy groups, and financial institutions seizing the potential.

Would the market be perverse? Would the market created generate outcomes that make consumers in particular worse off than today? A market might emerge:

- In which some privacy providing organizations would, in essence, say 'Your baseline is that you have no privacy whatever. Anything you provide to us, including the fact that you have visited this site, will be used in whatever way we want, without restriction. If you want any additional privacy and security, then pay us 'x.';
- Where a 'bet and break' incentive for some ethically challenged users is created: find a weakness in a system, buy the most insurance possible, and then break the system for fun and profit;
- Where the privacy marketplace would in itself disclose sensitive information; the dollar value for a given level of privacy assurance could reveal the importance of the information people wish to protect;
- Where cheating takes place. Privacy providers with obligations under the instrument do not pay as required, or resort to legal obfuscations; other forms of cheating (by consumers or providers) will no doubt be possible.

These are legitimate concerns; it is not clear, until the proposed system is actually implemented, whether these downsides trump the benefits. Some providers offer essentially no privacy now. Cyberspace has an active underworld already; the increased exposure of participating providers might (would) encourage additional security. The proposed system would at least provide additional opportunities for choice in both privacy and security dimensions.

Do the requisite security technologies and policies exist? There are significant technical issues that will need to be addressed. The lack of any effective security metrics makes the measurement of protection levels challenging. Moreover, the proposal would require privacy providers to provide multiple levels of protection. It probably would be easier and cheaper for them simply to protect everything at the highest level, since providers will have to have the technology and practices to do so in any event.

Will apathy and inertia triumph? The proposed system would alter the balance of power (under the new system the consumer has greater control over their data) and so require a shift in the way the market works. There is considerable risk, consequently, that privacy providing organizations would resist adopting this new system, or that consumer would balk at the notion of having to pay for privacy.

Consumers may be apathetic, and, except for a few privacy zealots, unwilling to participate. The likely payments are insufficient to cover the cost of a full-blown identify violation, possibly engendering frustration among those 'covered' under the new system. Privacy providing organizations individually have little or no incentive to change their current stance; if an organization is concerned about protecting privacy, it already has taken the necessary steps.

Most likely therefore the new market will not emerge as a result of the summation of individual uncoordinated action by privacy providing organizations or consumers. Instead, a new market will be created, an act of will, by some combination of insurance providers, socially aware privacy providers, and privacy advocate groups. To the consumer the new instruments will have to be simple to understand; to privacy providers the benefits in terms of economic and social return will have to be made apparent. In colloquial terms, people don't buy insurance, they are sold insurance.

6. REFINEMENTS

A modification to the proposed privacy expectations/security assurance would ensure an even more positive consumer benefit.

- An 'opt-out' privacy assurance ceiling/security instrument: Instead of privacy providing organizations stating a baseline privacy and security profile, and offering the choice (with payment) for additional privacy/security, the baseline would be a very high standard, and consumers would be offered inducements to reduce their privacy and/or security options. The ceiling could be porous so that consumers desiring an even higher privacy expectation and security assurance could purchase such an alternative.

The difference between this alternative and the proposed privacy expectations and security assurance offer is simply one of where the baseline is set. Under the proposed system the baseline is assumed to be very low (which generally accords with reality in privacy unregulated sectors in the US); under the modified system the baseline would be much higher. A higher baseline would provide more consumer choice. An 'opt-out' for lower protections would also likely ensure that more consumers would remain with the (higher) baseline. The ability to offer either positive or negative payment flows for privacy and security assurance levels increases the flexibility of the proposed instrument. However, creating a higher baseline would probably require legislation, with the attendant political difficulties (read infeasibility).

There are a number of choices as to the specific structuring of the proposed privacy expectation/security assurance instrument which will need to be made. These include:

- Administratively managed offer/response or auction?: A system where privacy providing organizations state 'here are your choices' is closer to the existing system ('here is our privacy policy') and may initially be the most effective initial market mechanism. There is a degree of consumer education that will have to take place in the early stages of the proposed market, and an administrative offer/response system lets both consumers and privacy providing organizations explore the options and the emergent pricing. However, there is much to be said for auctions – auctions are of increasing interest to economists as efficient mechanisms for capturing preferences, risk aversion, and other information.[24] An open question for discussion (in the authors mind) is how an efficient auction would be structured.
- Term of the privacy expectations and security assurance instrument: The first component (privacy expectations) presumably could be altered at any time, although it might merit some thought as to whether a 'claw-back' provision is technically or administratively feasible ('I agreed before that you could reveal my personal privacy information, but now I don't agree to that, and want you to retrieve and protect this information under a new

privacy preference). The second component (security assurance) is an insurance instrument requiring a time period. Pro-rating the insurance component if consumers wish to change their choice of instrument ('we'll pay back x% of your premium) is a logical choice.

7. CONCLUSION

The proposed privacy expectations and security assurance offer system would augment or supplant existing privacy protection measures, and help to link security and privacy protection responsibility to organizational accountability. As an explicitly half-baked idea, obviously there are a number of questions and issues regarding the structure and feasibility of this proposal. In summary, however, the proposed instrument would provide numerous benefits while circumventing some of the political barriers that stand in the way of increased privacy choice for (in particular) US consumers.

8. REFERENCES

[1] Acquisti, A., and Grossklogs, J. 2003. Losses, Gains, and Hyperbolic Discounting: An Experimental Approach to Information Security Attitudes and Behavior. Proceedings of the 2nd International Workshop on Economics and Information Security. www.cpppe.umd.edu/rhsmith3/agenda.htm

[2] Adams, Anne and Sasse, Martina Angela 2001. Privacy in Multimedia Communications: Protecting Users, not just data. In HCI Conference, Ann Blandford, Jean Vanderdonckt, and Philip D. Gray. 2001. People and Computers XV interactions without frontiers: joint proceedings of HCI 2001 and IHM 2001. BCS conference series. London: Springer.

[3] Analysts: TJ Maxx case may cost over $1B. The Boston Globe. April 12, 2007. www.boston.com/business/personalfinance/articles/2007/04/12/analysts_tjx_case_may_cost_over_1B

[4] Baer, Walter S. and Parkinson, Andrew 2007. Cyberinsurance in IT Security Management. IEEE Security and Privacy Volume 5 Issue 3 (May-June 2007) pp. 50-56. DOI=10.1109/MSP.2007.57.

[5] Chang, A, Kannan, P.K., Whinston, A.1998. Goodies' in Exchange for Consumer Information on the Internet: The Economics and Issues. In Proceedings of the Thirty-First Hawaii International Conference on System Sciences Vol. 4. (Hawaii, USA January 6-9 1998). IEEE, 533-542.

[6] Cranor. L.F. 2003. P3P: making privacy policies more useful. IEEE Security and Privacy. Vol. 1 Issue 6 (November-December 2003). 50-55. DOI=10.1109.MSECP.2003.1253568.

[7] Cranor, L.F. and Garfinkel, S. 2004. Secure or Usable? IEEE Security and Privacy. Vol. 15. Issue 5. (September-October 2004). 16-18. DOI=10.1109/MSP.2004.69

[8] Cranor, L.F. 2005. Giving notice: why privacy policies and security breach notifications aren't enough. IEEE Communications Vol. 43 Issue 8 (August 2005) 18-19.

[9] Dubauskas, Natasha 2005. Business Compliance to Changing Privacy Protections. In Proceedings of the 38th Hawaii International Conference on System Sciences.(Hawaii, USA). IEEE, 2005.

[10] Earp, J.P., Anton, A.I., Aiman-Smith, L., and Stufflebeam, W.H. 2005. Examining Internet Privacy Policies Within the Context of User Privacy Values. IEEE Transactions on Engineering Management. Vol. 52, Issue 2 (May 2005).

[11] Electronic Privacy Information Center (EPIC) 2000. Pretty Poor Privacy: An Assessment of P3P and Internet Privacy. June 2000. 2. www.epic.org/reports/prettypoorprivacy.html

[12] Federal Trade Commission, Commissioner Sheila Anthony no date. The Case for Standardization of Privacy Policy Formats. www.ftc.gov/speeches/anthony/standardppf.shtm

[13] Federal Trade Commission 2000. Privacy OnLine: Fair Information Practices in the Electronic Marketplace; A Report to Congress. Federal Trade Commission, May 2000. 2.

[14] Federal Trade Commission no date. Staff Report: Enhancing Consumer Privacy OnLine. www.ftc.gov/reports/privacy/Privacy4.shtm.

[15] Ghosh, Anup 2002. Maintaining Privacy in an OnLine World. IT Professional. Vol. 4, Issue 5 (September- October 2002), 24-28.

[16] Greenemeier, Larry 2007. Massachusetts bill would make businesses pay for poor data security. Information Week. February 22, 2007. www.informationweek.com/story/showArticle.jhtml?articleID=197008143

[17] Hagel, John, and Rayport, Jeffrey 1997. The Coming Battle for Customer Information. Harvard Business Review (January-February 1997) 53-65.

[18] Hann, I.H. et al. 2003. Overcoming OnLine Information Privacy Concerns: A Comparison of Privacy Policies, Convenience, and Promotions.. Working Paper (September 2003). Marshall School of Business, University of Southern California.

[19] Huberman, Bernard, Adan, Etan, and Ane, Leslie 2005. Valuating Privacy. IEEE Security and Privacy Vol. 3, Issue 5 (September-October 2005) 22-25.

[20] ID theft nets 85000 pounds a head: study. The Channel Register, January 19, 2007. www.theregister.co.uk/2007/01/19/id_theft_nets_85000a_head/

[21] Karat, Claire-Marie, Brodie, Carolyn, and Karat, John 2006. Usable privacy and security for personal information management. Communications of the ACM Vol. 49 Issue 1 (January 2006) 56-57. DOI=http://doi.acm.org/10.1145/1107458.1107491

[22] Kark, Khalid 2007. Calculating the Cost of a Security Breach. Forrester Research, April 10, 2007.

[23] Kleinberg, J., Papadimitrou, C.H., and Raghaven, P. 2001.On the Value of Private Information. In Proceedings of the 85h Conference on Theoretical Aspects of Rationality and Knowledge (TARK-2001*)*, J. van Bertherm, ed. Morgan Kaufman, 2001. 249-257.

[24] Klemperer, Paul 1999. Auction Theory: A Guide to the Literature, Chapter 1: A Survey of Auction Theory. Journal of Economic Surveys, Vol. 13(3) (July 1999) 227-286. www.nuf.ox.ac.uk/users/llemper/VirtualBook/survey.pdf

[25] Laudon, K.C 1996. Markets and Privacy. Communications of the ACM. Vol. 39, No. 9. 992-1004.

[26] Leyden, John 2005. US banks lose $50bn to phantom fraudsters. The Channel Register, September 16, 2005. www.channelregister.co.uk/2005/09/16/gartner_phantom_fraud/

[27] Leyden, John,, 2007. How much do security breaches cost anyway?, The Channel Register, April 12, 2007. www.channelregister.co.uk/2007/04/12/breach_cost_estimate/

[28] Olson, Gary and Olson, Judith 2003. Human-computer interaction: psychological aspects of the human use of computing. Annual Review of Psychology Volume 54 (Annual 2003) 491.

[29] Palen, Leysia and Dourish, Paul 2003. Unpacking 'Privacy' for a Networked World. Conference on Human Factors in Computing Systems, Proceedings of the SIGCHI Conference on Human Factors in Computing Systems. ACM Press New York, NY. 129-136.

[30] Rasch, Mark 2006. Strict liability for security breaches?, Channel Register, February 22, 2006. www.channelregister.co.uk/2006/02/22/data_breach_liability/

[31] Sasse, M.A., Brostoff, S. and Weirich, D. 2001. Transforming the 'Weakest Link' – A Human/Computer Interaraction Approach to Usable and Effective Security. BT Technology Journal Volume 19 Number 3 (July 2001) 122-131. DOI=10.1023/A:1011902718709

[32] Schwartz, B 2005. The Paradox of Choice. Harper Collins.

[33] Smith, Marcia S. 2005. Identity Theft: The Internet Connection. Congressional Research Service. The Library of Congress. CRS Report RS22082 (March 16, 2005) 2.

[34] Sprenger, Polly 1999. Sun on Privacy:'Get Over It' Wired. January 26 1999. http://www.wired.com/politics/law/news/1999/01/17538.

[35] U.S. Department of Commerce 2007. Safe Harbor Overview. www.export.gov/safeharbor/sh_overview.html

[36] U.S. Department of Commerce Bureau of Labor Statistics 2006. Consumer Expenditures in 2005, Report 998. US Department of Labor. www.bls.gov/cex/csxann05.pdf

[37] U.S. Privacy Rights Clearinghouse 2007. www.privacyrights.org. See also SC Magazine 2006. A dubious milestone – Privacy Rights Clearinghouse reports exposed record No 100 million. December 14, 2006.

[38] Varian, Hal 1996. Economic Aspects of Personal Privacy. White Paper, 1996. www.sims.berkeley.edu/~hal/Papers/privacy.html

[39] What is Fair Trade Coffee All About. http://globalexchange.org/campaigns/fairtrade/coffee/background.html