ACC 626

PRIVACY SEALS: WHAT IS THEIR VALUE AND CAN ACCOUNTANTS OFFER THEM COMPETITIVELY?

Aruj Kumar
ACC 626 Section 1
Prepared for: M. Datardina
Table of Contents

Abstract........................................................................................................................................1
1.0 Introduction..............................................................................................................................2

2.0 Privacy Seals Today & WebTrust.............................................................................................2
  2.1 TRUSTe..................................................................................................................................3
  2.2 Better Business Bureau...........................................................................................................3
  2.3 WebTrust...............................................................................................................................3

3.0 Value of Privacy Seals.............................................................................................................4
  3.1 Studies in favour of Privacy Seals..........................................................................................4
  3.2 Studies against Privacy Seals...............................................................................................5
  3.3 Other studies.........................................................................................................................6

4.0 What does this mean for Executives and Decision Makers?....................................................7

5.0 Privacy Trends.........................................................................................................................7

6.0 Automated Privacy Certification versus Manual Certification................................................8
  6.1 TRUSTe Certification Process...............................................................................................8
  6.2 WebTrust Certification Process...........................................................................................9
  6.3 Key Differences....................................................................................................................9
  6.4 How Can Privacy Seals Offered by CA’s become Competitive?............................................10

7.0 Conclusion...............................................................................................................................10

Annotated Bibliography..................................................................................................................12

Additional Works Used................................................................................................................22
ABSTRACT

Privacy seals represent some level of third-party assurance over a specific privacy policy or practice. The current market for seals in business to consumer e-commerce is dominated by TRUSTe, a primarily automated and relatively simple to obtain seal. On the other hand, seals that require audit style procedures for certification, such as WebTrust (offered by accountants), have not been picked up in the market. Numerous studies have been conducted attempting to determine the value of seals. Several claim privacy seals are beneficial while an equal number of studies claim they are not. In other words, it is unclear whether privacy seals add value, so their adoption appears to be contingent on a low price and an unobtrusive certification process. While a desire for higher levels of assurance over the use and storage of private information may be realized in the future, the current environment demands that WebTrust change its form and cost in order for Chartered Accountants (CA’s) to offer a competitive seal in the market. This paper recommends that the WebTrust adopts much less costly minimum standards and continuous monitoring software similar to what is used by TRUSTe. WebTrust would need to advertise to consumers as well as businesses in order to be successful.
1.0 Introduction

The rapid growth of electronic commerce and information technology has led to the proliferation of online services and products. The range of online offerings can vary from shoes to insurance and everything in between. What most of these services have in common, however, is that in order to access or purchase them, there must be some level of personal identification. Whether it is a mailing address or payment information, some level of privacy is forgone as a price for the convenience and efficiency afforded by electronic transactions.

How then can consumers weigh the costs associated with the loss of privacy against the benefits of e-commerce? Certainly there is a natural process in place that limits the privacy exposure of users in that websites that blatantly misuse private information should lose customers until they are no longer a viable operation. Yet there is a fine line between abuse of private information and distasteful privacy practices. In theory, consumers would be more comfortable with an online purchase if there was some way to ensure that their private information was not being abused and even perhaps pay a premium for greater degrees of care over their private information. This is where privacy seals come in. A privacy seal is a visible logo or symbol on a website that signifies some level of third-party assurance over some specific privacy practice or policy. Note that there is no universal framework over what level of assurance a third party privacy seal provides. This means some privacy seals could have more rigorous compliance requirements while others may be relatively lenient.

This paper examines the effectiveness of privacy seals from a number of views. It examines how privacy seals affect consumer decision making. It looks at consumer confidence and how privacy assurance can influence price paid. It attempts to come to a conclusion on whether privacy seals offer a material value proposition and whether it is something for executives and decision makers to consider. This paper is also intended to provide some insight for the Chartered Accountant (CA) profession and whether or not offering privacy seals and privacy assurance can be turned into a feasible or even significant revenue base for CAs.

2.0 Privacy Seals Today & WebTrust

In order to provide some context for the discussion on privacy seals, the reader should be aware of the current market for them. The vast majority of privacy seals involve a primarily automated process. Quick examinations of advertised fees show that they are priced well below what could be performed through a traditional audit assurance process. The market leader in privacy seals is TRUSTe. Other competitors include the BBB Accreditation (formerly BBBOnline). There are also privacy seals for specific products and services such as EuroPriSe in Europe for IT products and services. There have been significant changes in the privacy seal landscape over the last 10 years or so.
2.1 TRUSTe

TRUSTe was established in 1997. According to its website, it has grown to include over 4000 web properties and its logo can be found on the websites of top companies like Apple and AT&T. They also purport a 90% renewal rate and that their mark has been proven to “increase e-commerce conversion rates, average order size, form completion rates, customer engagement, and more.” TRUSTe has a very large market share that continues to grow.

2.2 Better Business Bureau Accreditation (BBB)

The Better Business Bureau used to have an online privacy seal called BBBOnline which was similar to TRUSTe, but it was discontinued as a separate product and rather added as a component of their general BBB accreditation. The BBBOnline seal was established in 1999 but was discontinued because it was losing ground as a standalone product. As of today, the website for the BBBOnline seal no longer exists and privacy requirements can be found on the website for general BBB accreditation. The accreditation now is used by many for purposes other than its privacy certification.

2.3 WebTrust

WebTrust is a key learning tool when considering the role of Chartered Accountants in the privacy seal market. It is widely regarded as a failure by many, at least in a business to consumer assurance context. The seal was launched in 1997 as a joint effort between the Canadian Institute of Chartered Accountants (CICA) and the American Institute of Certified Public Accountants (AICPA). It was originally meant to capitalize on the booming e-commerce industry. The seal is still offered today, but it has a very limited market share due to the cost and effort involved. The form of the procedures involved in attaining the seal is very similar to that of traditional audit, including signing off on a written opinion. WebTrust is primarily offered in the United States, while only six firms offer the service in Canada. Although WebTrust is an example of a privacy seal offered by public accountants, it is not an example of a competitive one. A part of this paper seeks to determine why this is the case and what needs to change.

There is somewhat of a polarization in the privacy seal market today. Popular seals continue to grow in market share while less popular seals retain a flat or even decreasing market share. This suggests that there is some value in using familiar or widespread seals.

---

3.0 Value of Privacy Seals

Key to every decision involving the use of privacy seals is assessing the value they can provide to the company or website that displays them. Their value proposition is motivated by everything from what price they should be offered at to where and when they should be displayed. Numerous studies have been conducted in an attempt to empirically attest to their value or lack thereof and these will be summarized and used to drive the following discussion.

3.1 Studies in favour of Privacy Seals

One study by Chang et al. specifically looks at the effect that the WebTrust seal has on web purchase willingness. It notes that in theory the WebTrust logo should garner higher levels of trust than more generic seals because it is backed by firm reputation. The study uses 320 students from a university in Taiwan and divides the groups based on factors such as risk preference, purchase expectations, purchase experience and purchase intentions. The study establishes three very important conclusions. After controlling for the differences in the groups, a WebTrust seal appears to increase consumer online purchase willingness. It also concludes that WebTrust seals from larger firms are more effective in this goal than seals issued by smaller firms. Finally, it notes what it calls an ordering effect. Consumers are more affected in terms of purchase willingness by the removal of a seal that was once there rather than by the addition of a seal that was not there before.

The study does not offer strong evidence for the effectiveness of privacy seals in that the participants are educated about WebTrust and the firms that issue them before they are surveyed. This is a necessary control to eliminate disparities in participant knowledge. Unfortunately, educating participants about seals likely affects their decision making. In the real world, many consumers will not have knowledge of what a privacy seal actually entails. However, an important implication from this study is that among users that have some degree of brand awareness, seals that are offered by more recognized firms or companies have a more positive effect on consumer purchase willingness.

A second study by Sharon et al. examines the level of trust transference created by third party trust seals or logos. The study used forty undergraduate students from a university in the United States who then solicited participants via email. Through the use of survey questions, a model was constructed that examined six hypotheses. These included the intensity of logo exposure (how many times has the logo been seen before), logo validation (was the logo clicked on), current level of trust in online shopping and

---


disposition to third party certification, among a couple of others. The study used a seven point scale in the survey questions to determine that there is indeed a level of trust transference from a third party seal to the consumer, increasing their level of comfort with a purchase. The variables tested lined up as expected, with the exception of the logo validation hypothesis. This implies that consumers will tend to trust a firm with a seal over a firm without one, whether or not the actual details behind the seal are studied.

### 3.2 Studies against Privacy Seals

A study by Hui et al.\textsuperscript{6} examined the questions of whether privacy statements and privacy seals have value to consumers and whether this affects their willingness to disclose private information. By disguising the study as a marketing survey hosted on a real firm domain name, participants were more likely to disclose information in accordance with their actual preferences. A monetary incentive was included as well. The survey website had three different scenarios. One version of the website was hosted without any privacy assurance, the other with a privacy statement and the third with both a privacy statement and a privacy seal. Note that the TRUSTe seal was used, as it was determined to be more widely recognized than other local seals. The study found that participants who used the version of the website with a privacy statement were willing to disclose much more personal information than the version without any privacy assurance. However, it found that the version of the website that included the privacy seal induced very little disclosure over the version with just a privacy statement. The implication of this study is that users value the existence of a privacy statement and are willing to disclose more information as a result. Users do not, however, value privacy seals as the seals do not appear to induce the disclosure of additional information. Translated into an e-commerce perspective, consumers who are more willing to disclose information are more comfortable with an online purchase and therefore more likely to buy a product or service.

Another study done by Benjamin Edelman\textsuperscript{7} seeks to determine whether a site with third-party certification is actually more trustworthy than a website without such certification. To test this, the problem is restated as follows: “For a certification to cause a consumer to conclude a certified site is more safe than the consumer thought ex ante, the certification must be given to trustworthy sites more often than it is given to untrustworthy sites.” Using software called SiteAdvisor to measure trustworthiness, the study finds that there is an adverse selection problem – sites with trust certificates (specifically TRUSTe) are more than

---

\textsuperscript{6} The information for this study is taken from: Hui et al., 2007. \textit{The Value of Privacy Assurance: An Exploratory Field Experiment}. Retrieved June 27, 2012 from: \url{http://xa.yimg.com/kq/groups/23832221/1275801176/name/%C2%BA%C2%B7%C2%A4%C3%87%C3%92%C3%81%C3%A3%C3%A8%C3%8A%C3%95%C3%82%C3%AC%5B1%5D.pdf}

\textsuperscript{7} The information for this study is taken from: Edelman, Benjamin, 2010. \textit{Adverse selection on online “trust” certification and search results}. Retrieved on June 27, 2012 from: \url{http://www.benedelman.org/publications/advsel-trust-se.pdf}
twice as likely to be untrustworthy. The paper also scrutinizes trust seals by citing numerous studies before it. It notes that seals are issued to companies and websites that are later found to be grossly abusing privacy, citing the example of Gratis Internet in 2004. It also notes that of the many privacy complaints TRUSTe receives, almost none of them result in revocation of the seal. The implication of this study is that privacy seals lack substance and are too easy to obtain. There is theoretically a cost associated with privacy seals as consumers are put off by untrustworthy sites holding or appearing to hold certification. For example, one writer from BrightHub\(^8\) outlines her experience with a website displaying the TRUSTe logo despite not being a TRUSTe member. The logo was not actually a certification but rather displayed in connection with TRUSTe certified software hosted on their website.

3.3 Other Studies

Geographical / Cultural Differences

A study by Babita et al.\(^9\) offers some insight into the idea that the value of privacy seals may vary from country to country. It examines the willingness of consumers from the United States to disclose personal information compared to the willingness of consumers from India to disclose the same information. Using surveys and testing participant interaction with an online firm, the study finds that American participants are more aware of privacy concerns and are less likely to disclose private information than the participants in India. Cultural and geographical differences appear to create a material difference in the willingness of consumers to disclose personal data. The study attempts to explain why this disparity exists. For example, it notes that in India, it is common to post one’s resume online for a job application. The implication of the study is that a privacy seal for a website serving an Indian user base is likely less valuable than a privacy certification on an American website.

Privacy Sensitive Purchases

In a study conducted by Serge et al.\(^10\), it was determined that when consumers purchased privacy-sensitive items, they were willing to pay a premium to purchase them from websites they perceived to have higher privacy standards. The study was conducted in a laboratory setting where prices were controlled and the participants were asked to buy items with their own credit card and billing information. Despite the availability of slightly lower prices for some items, many participants elected to pay a higher


price for increased privacy on sensitive items. The study however was unable to express a meaningful relationship between premium and privacy sensitivity. The study also determined that showing a privacy indicator alongside search results caused more participants to purchase items at a premium from websites with increased privacy.

4.0 What does this mean for Executives and Decision Makers?

The above studies tell us several, sometimes conflicting things. For a decision maker considering a privacy seal for their website, the choice of adopting one depends on the nature of their business, among other things. Businesses involved in the sale of sensitive items benefit more from privacy indicators than business that sell mundane or common items. As illustrated in the studies supporting privacy seals, using a well recognized seal is extremely important as well. The studies opposing privacy seals, on the other hand, claim that they are ineffective and can even have a cost or negative perception attached to them. It may be the case that a simple privacy statement is enough. The decision is not very clear cut. A large company with a well established base of customers well into its operations would likely benefit very little from a privacy seal. Buying into a privacy seal program means that it will probably have to be renewed each year as consumers are far more sensitive to the removal of a seal than its addition. The only thing that seems to be ascertainable from the results of the studies is that the benefit of a privacy seal is not abundantly apparent, and the price paid to acquire one should reflect that fact. This means complex and expensive privacy certifications are likely not worth the cost to businesses until consumers are able to recognize the value behind them.

5.0 Privacy Trends

The world continues to change. It is becoming increasingly difficult to keep information private. With social media and smarter software tracking our behavior on search engines, there is a growing movement towards accountability and stronger privacy controls. As the channels for identity theft and fraud become wider, regulation alone will not likely keep up with the privacy concerns of citizens. This represents a business opportunity for third-party privacy certification entities. The same conditions that drove the creation of WebTrust by accountants years ago still exists today and will likely continue to exist in the future.

For example, privacy reform in the European Union is relatively rigid. In 2012 legislation was introduced to overhaul the EU Directive on Data protection, which includes a clause that states companies storing personal data must be able to explain how and why the data is being held. Companies failing to do so could be fined 2% of revenues, which could translate to billions for much larger firms. Legislation like this could pave the way for more thorough and complex privacy audits, but it could also scare companies from

---

letting anyone have a chance to examine their privacy practices in detail. As privacy needs become more complex, perhaps there will be further value in more thorough privacy certification, but as it stands, the cost-benefit tradeoff for a privacy “audit” is unappealing.

As further examples, India in 2011 introduced more stringent privacy standards requiring companies to disclose to users if their private data is being collected and stored. Mexico, Peru, and Costa Rica are all expected to begin enforcement of stronger privacy legislation in 2012. Singapore is expected the roll out a new framework as well. All of these trends point to a greater desire from the public to protect their private information and to ensure firms are held accountable for the way they use and store private and personally identifiable information.

6.0 Automated Privacy Certification versus Manual Certification

As discussed earlier, the value of privacy seals is not abundantly clear, making it difficult to justify adopting an expensive or thorough privacy certification process. Future trends may change this, but the traditional audit style approach has very little to offer over a simpler, quicker privacy seal that uses mostly automated processes to gain assurance over privacy standards. This section of the paper will examine the certification process and tools used by TRUSTe and compare them to the certification process used by WebTrust. By doing this, it may be possible to see why the WebTrust seal fails to be competitive and what has to be changed in order to turn it around.

6.1 TRUSTe Certification Process

The following is a summary of the certification process as advertised in the 2011 TRUSTe transparency report. It attempts to combine information from the privacy program requirements as well.

Manual evaluation of client practices – This is the primary process by which TRUSTe initially checks to see if a client’s privacy policy meets the minimum requirements of their privacy program requirements. It is done by visiting the client website and through questionnaires. In some cases TRUSTe will use software to scan the client’s website and generate a privacy policy that is in compliance with the minimum requirements for that business.

Client’s own attestation and interviews – Client must attest to their compliance with relevant privacy laws and the minimum requirements set forth by TRUSTe. They must agree to abide by the privacy policy created by TRUSTe if applicable and submit to any dispute resolutions.

---


Monitoring through TRUSTe tools – this is one the key advantages of TRUSTe, it uses proprietary tools to offer continuous monitoring solutions. The primary technologies used here are web crawling and e-mail seeding. Web crawling software tests for the existence of key privacy elements at the point of a transaction (i.e. a privacy policy) and checks that transactions containing sensitive information are sent over an encrypted connection. E-mail seeding is a simple system that submits unique emails to a client’s website and sees what gets sent to the addresses. It checks for unauthorized emails, spam, etc.

Overall, the process is relatively quick. The privacy program requirements are not particularly strict. For example, the requirement for the collection of personally identifiable information (PII) is that it is “reasonably useful for the purpose for which it was collected.”⁴ This by itself is almost meaningless and does not really prevent or preclude the collection of any personally identifiable information, regardless of how sensitive. Essentially TRUSTe checks to see if basic privacy laws are being upheld.

6.2 WebTrust Certification Process¹⁵

The closest comparable offering from WebTrust is the WebTrust Online Privacy engagement, which is bound by the Generally Accepted Privacy Principles (GAPP) issued by the CICA and AICPA. There is no set list of procedures that are performed, but rather the engagement must have the proper amount of work done to reduce the risk that the client is not in compliance with GAPP to an acceptable level. This approach somewhat mirrors a traditional financial audit. Note that a key aspect of the WebTrust seal is that the auditor uses professional judgment when applying procedures. For example, the auditor might determine that certain PII is sensitive enough to require explicit consent for its collection, rather than implicit consent. The seal expires within one year, whereupon the client has 90 days to renew the seal. The follow up would not be as thorough as the initial examination (i.e. a review versus an audit).

6.3 Key Differences

The TRUSTe process is a simpler and quicker way to get a seal on a website. Monitoring and renewal costs are very low and it appears TRUSTe enforces its privacy program requirements primarily through automated tools and responding to the complaints of consumers. The implication of this is that companies with questionable privacy policies have the ability to meet TRUSTe requirements easily, which appears to align with some of the conclusions from the adverse selection study (Edelman) mentioned earlier in this paper.

The choice between TRUSTe and WebTrust can be likened to a public company choosing between two auditors. If both can provide an unqualified opinion, the company will choose the least prying, most

---

flexible, and cheapest auditor. The company only cares about the unqualified opinion, unless it believes that its shareholders value the opinion of one auditor over another. WebTrust is more intrusive and places much greater scrutiny on a company, offering very little marginal value (if any) over TRUSTe.

6.4 How Can Privacy Seals Offered by CA’s become Competitive?

The key to offering a competitive seal is to either demonstrate that a WebTrust seal generates additional value or to change the costs associated with a WebTrust engagement. As consumers get more comfortable with online purchases, it will become increasingly difficult to differentiate one privacy seal over another. It is possible that the environment of e-commerce will change such that consumers become wary of transactions that aren’t thoroughly tested for privacy concerns, but as of now, WebTrust will have to modify its form and cost structure to be successful.

For example, WebTrust could use a minimum requirement style approach similar to what TRUSTe does. Rather than trying to meet a complex set of standards, accountants could perform less costly tests to check for compliance with a framework based around required privacy law. There should also be some minimum client acceptance procedures to avoid dishonest clients. The downside of this approach is that there is an increased chance of certifying an undeserving client, which would consequently damage the reputation of the firm. In addition, the relevant governing bodies should invest in creating automated software (web crawlers and e-mail seeding software) that could be distributed to firms to aid in their certification process. These types of software aren’t necessarily complex and could be updated and rolled out by in-house IT staff at the governing bodies. Once there has been some material change in how the seal is issued, firms must raise brand awareness by continuously advertising WebTrust over channels that reach consumers and businesses, rather than businesses alone.

The ideas mentioned above are steps that could be taken to improve WebTrust. Even then, there is large uncertainty behind whether or not a business to consumer privacy seal issued by CA’s could be successful. It may be the case that the profession must wait for the privacy environment to drastically change before making their move.

7.0 Conclusion

It is questionable as to whether privacy seals add value to an online business. Some studies indicate that they are effective in creating trust as long as they are recognizable while other studies suggest they do nothing to add value. The success of seals like TRUSTe over WebTrust implies that businesses do not completely see the value in privacy seals and are only willing to pay for them if the cost is very low. Costs are kept low through automated procedures and simple program requirements. Audit based assurance seals like WebTrust simply cannot compete due to their much higher cost. While privacy trends are changing and privacy is becoming increasingly important, the current environment demands that WebTrust change is form to become successful. Lower requirements calling for less work, the adoption of
automated monitoring software and a concerted effort towards advertising to consumers is required for WebTrust to become a successful player in the business to consumer privacy seal market.
### Annotated Bibliography

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
<th>Added in the final paper?</th>
</tr>
</thead>
</table>

### Annotation

Cultural differences appear to create a significant difference in the willingness of consumers to disclose personal data. Surveys were given to both Indian and American participants, receiving their rating on several questions designed to test their willingness to disclose personal information and intentions in ensuring and protecting privacy. The study also tested participant interaction with an online firm. It finds that American participants are more aware of privacy concerns and are less likely to disclose private information than the participants in India. This study offers some insight into the idea that the value proposition of privacy seals varies from country to country.
### Annotation

WebTrust assurance seals issued by CPA firms (WebTrust) have a significant impact on web purchase willingness. There was a greater impact if the seals were issued by larger firms, but the study also finds that there is more impact to removing a seal than to adding one that was not there before. 320 students from a university in Taiwan all with computer experience were split into groups and surveyed regarding risk preference and willingness to purchase from a hypothetical company.

### Author Information

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical / website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, database, website, link</th>
<th>Added in the final paper?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Egelman, Serge; Tsai, Janice ; Cranor, Lorrie F.; Acquisti, Alessandro</td>
<td>Timing is Everything? The Effects of Timing and Placement of Online Privacy Indicators</td>
<td>n/a</td>
<td>n/a</td>
<td>2009</td>
<td>n/a</td>
<td>May 26, 2012</td>
<td>Google Scholar / ACM</td>
<td><a href="http://www.guanotronic.c">http://www.guanotronic.c</a></td>
</tr>
<tr>
<td>Author</td>
<td>Title of Article</td>
<td>Periodical/ website</td>
<td>Vol. / No. / Edition</td>
<td>Year published</td>
<td>Pages</td>
<td>Date accessed</td>
<td>Location, data base, website, link</td>
<td>Added in the final paper?</td>
</tr>
<tr>
<td>-----------------</td>
<td>------------------------------------------------------------------------</td>
<td>---------------------</td>
<td>----------------------</td>
<td>----------------</td>
<td>-------</td>
<td>---------------</td>
<td>------------------------------------</td>
<td>--------------------------</td>
</tr>
<tr>
<td>Jiang, Pingjun;</td>
<td>Online Transactions: An Exploratory Study</td>
<td>Marketing</td>
<td></td>
<td></td>
<td>858</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Jones, David B.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><a href="http://journals2.scholarsportal.info.proxy.lib.uwaterlo.ca/details-sfx.xqy?uri=/07426046/v25i0009/839_htcprtio%5Ctaes.xml">http://journals2.scholarsportal.info.proxy.lib.uwaterlo.ca/details-sfx.xqy?uri=/07426046/v25i0009/839_htcprtio\taes.xml</a></td>
</tr>
</tbody>
</table>

**Annotation**

Consumers are indeed provided a level of trust transference from third party certification programs to online e-marketers. However, the degree to which this occurs is positively correlated to a number of factors studied in this paper. Using an online survey, there is a statistically significant relationship between the intensity of logo exposure, disposition to third-party certification, importance of trust factors in online shopping, the current level of trust in online shopping, logo validation and the level of trust transferred to e-marketers.
<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
<th>Added in the final paper?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hui, Kai-Lung; Teo, Hock H.; Lee, Sang-Yong T.</td>
<td>The Value of Privacy Assurance: An Exploratory Field Experiment</td>
<td>MIS Quarterly</td>
<td>31, 1</td>
<td>March 2007</td>
<td>19-33</td>
<td>May 26, 2012</td>
<td>Google Scholar</td>
<td></td>
</tr>
</tbody>
</table>

http://xa.yimg.com/kq/groups/23832221/1275801176/name/%C2%BA%C2%B7%C2%A4%C3%87%C3%92%C3%81%C3%A3%C3%8B%C3%81%C3%A8%C3%8A%C3%92%C3%82%C3%8A%C3%98%C3%83%C3%95%C3%82%C3%AC%5B1%5D.pdf

**Annotation**

The study differs from other studies in that instead of using laboratory testing or surveys, it modifies the content of a real firm's real domain name. The subjects were not informed of the purpose of the study. Under the guise that subject responses would be used to design future products and promotions, the study was done under three different privacy scenarios. The existence of a privacy statement showed marginally significant improvements in information disclosure, while the existence of a privacy statement AND privacy seal showed little improvement over the scenario with only a privacy statement.
<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/ website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
<th>Added in the final paper?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Edelman, Benjamin</td>
<td>Adverse selection on online “trust” certification and search results</td>
<td>Electronic Commerce Research and an Application</td>
<td>n/a</td>
<td>2010</td>
<td>n/a</td>
<td>May 26, 2012</td>
<td>Google Scholar</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td><a href="http://www.benedelman.org/publications/advsel-trust-se.pdf">http://www.benedelman.org/publications/advsel-trust-se.pdf</a></td>
<td></td>
</tr>
<tr>
<td><strong>Annotation</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Because of the lax methods used by trust authorities like TRUSTe, a site using certification is more than twice as likely to be untrustworthy as a site without certification. This is because sites that are bad are pretending to be good and using trust seals to do it. It cites examples from the trust authorities themselves, such as thousands of privacy complaints leading to not a single change in any member privacy policies. It provides examples of untrustworthy sites under investigation that have the TRUSTe seal. The study uses SiteAdvisor to determine whether a site is untrustworthy and comes to the conclusion based on conditional probabilities that sites with a TRUSTe seal are twice as likely to be objectionable to users.</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Cline, Jay</td>
<td>Will the EU Privacy Reform Boost Privacy Seal Adoption?</td>
<td>International association of privacy professionals</td>
<td>n/a</td>
<td>April 13, 2012</td>
<td>n/a</td>
<td>May 26, 2012</td>
<td><a href="https://www.privacyassociation.org/publications/2012_04_12_will_the_eu_privacy_reform_boost_privacy_seal_adoption">https://www.privacyassociation.org/publications/2012_04_12_will_the_eu_privacy_reform_boost_privacy_seal_adoption</a></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Annotation</strong></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>With the new European draft regulation replacing the EU Directive on Data Protection, there has been increased focus on institutionalizing privacy seals as a means to help enforce the new, stricter rules. The article examines the success stories of privacy seals in North American and Japan and wonders what factors will have to be present for privacy seals to</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

16
flourish in Europe. Key success factors are transparency, affordability and credibility, but the article notes that some businesses may have concerns opening their privacy policies to certificate authorities directly controlled by the government. The new penalties for data breaches are quite severe.

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
<th>Added in the final paper?</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pignal, Stanley</td>
<td>New EU Privacy Rules Worry Business</td>
<td>Financial Times</td>
<td>n/a</td>
<td>Jan 22, 2012</td>
<td>n/a</td>
<td>May 26, 2012</td>
<td><a href="http://www.ft.com/cms/s/2/e14f2f3e-44f3-11e1-be2b-00144feabd0c0.html#axzz1w77oG0Ls">http://www.ft.com/cms/s/2/e14f2f3e-44f3-11e1-be2b-00144feabd0c0.html#axzz1w77oG0Ls</a></td>
<td>n/a</td>
</tr>
</tbody>
</table>

### Annotation

The article provides a summary of some key points of Europe’s new privacy regulation. Europe’s new unified privacy laws will enforce strict rules. A company must demonstrate why any personal data retained is necessary (how and why). There is a fine of 2% of revenues for a data breach. There is also a need for explicit consent from people whose data is being processed. There is also a “right to be forgotten” clause which will allow users to have information posted or made public be completely deleted.
There are several resources on the TRUSTe website containing information on their privacy requirements, complaints received, “return on investment” calculations, etc. Of particular interest is the Transparency Report, which outlines TRUSTe’s experiences in 2011 and in previous years, including complaint processing and seal termination. In addition, the site also outlines the privacy requirements for their most common programs.

The BBB offers an online seal which includes its online standards. In addition to its regular business accreditation standards, the privacy standards include very broadly the ideas of respecting privacy, securing sensitive data and honoring customer preferences.

Benbasat, Izak; Dongmin, Kim

Designs for Effective Implementations of Trust Assurance in Internet Stores

Communications of the ACM

53, 2

Feb, 2010

121-126

May 26, 2012


Added in the final paper?
There are three recommendations for improving consumer trust with an internet store. The first is to demonstrate explicit assurances on items consumers closely relate to trustworthiness, such as transmission of data, credit card security, product quality, customer service and the return process. Second, the return process must be made easy as there is a high correlation between trustworthiness and ease of product return. Third, something called the Toulmin model should be used to word assurances. The model says assurances should contain data, a claim and a backing.

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
<th>Added in the final paper?</th>
</tr>
</thead>
</table>

**Annotation**

The articles outlines the problem with trusting seals alone in gaining assurance over privacy, etc. The author describes an experience where she came across a website that included the TRUSTe logo, not the TRUSTe seal, prominently displayed in the bottom right corner. The website was not a listed TRUSTe member and the only reason for the logo was that the spyware packaged with their software is a TRUSTe certified tracking software.

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
<th>Added in the final paper?</th>
</tr>
</thead>
</table>
The report addresses a number of issues, but of relevance here is its discussion of privacy seals. There is a fundamental incentive problem in that companies with strong privacy practices (e.g. Google) have no need for privacy certification whereas marginal companies do. Worsening the problem is the fact that the seal program companies are paid by the people they are certifying. The report says there must be some sort of incentive in place, similar to the one in place in the Land of Schleswig-Holstein in Germany, where public authorities buy privacy compliant products and services wherever possible. The report recommends that the certification authorities have close ties to official regulators but should be self-financing.

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
<th>Added in the final paper?</th>
</tr>
</thead>
</table>
The report includes a section on privacy seals, where it criticizes the poor practices of some of the privacy seal providers. In particular it scorns Trust Guard and its extremely limited requirements for certification. It also criticizes the BBB seal, which can certify a company that sells user data to a third party so long as an opt out option exists. It finds TRUSTe to have stronger requirements but goes on to say that even these are not good enough considering that TRUSTe too can certify an entity that sells user information to a third party on an opt out basis. Most American consumers believe that a website with a privacy policy does not sell data to third parties.

Additional Works Used
