Trustmark Schemes Struggle to Protect Privacy (2008)

Chris Connolly, Galexia[1]

[1] Chris Connolly is a Director of Galexia, an independent consultancy specialising in privacy and electronic commerce. Research assistance for this article was provided by Amy Vierboom. <http://www.galexia.com.au>.

Web: www.galexia.com **Ph:** +612 9660 1111 **Fax:** +612 9660 7611
Post: Suite 95 Jones Bay Wharf, 26-32 Pirrama Road, Pyrmont NSW 2009, Australia

Document Control

Version

1.0

Date

26 September 2008

Source

The latest version of this article is available from
http://www.galexia.com/public/research/assets/trustmarks_struggle_20080926/

Copyright

Contents

1. Introduction

July 2008 was a landmark month in the history of privacy trustmarks – the seals that appear on some websites to provide a level of assurance about privacy protection. The largest and most successful trustmark – TRUSTe with over 2000 members – changed its status from 'non-profit' to 'for profit'. And the second largest trustmark – BBB Online Privacy with over 700 members – closed its doors for good, abandoning a scheme that it had run for over eight years.

Can the remaining trustmark schemes play a legitimate role in protecting privacy? This article examines the track-record of trustmarks to date and assesses their current relevance as a privacy protection tool.

1.1. The role of trustmarks

The basic premise of privacy trustmarks is that end users are supposed to have confidence in web sites displaying the trustmark seal, as it presumably indicates that the site adheres to good privacy standards.[2] In practice, although trustmark seals all appear similar, the level of privacy protection varies a great deal. Some seals are backed by detailed standards and independent audits. Other seals are provided with no requirements or checks (other than payment). Some seals include a free dispute resolution service for complaints, other seals have no complaints mechanism or charge consumers for lodging complaints.

The trustmark sector is completely unregulated and there are no published standards or even basic guidelines for running a trustmark service. There are some emerging trustmark associations, such as the Asia-Pacific Trustmark Alliance,[3] but these are still at the formative stage.

It is difficult to see how privacy can be protected by trustmarks in an environment where many of the seals are worthless. However, some argue that the legitimate trustmark schemes can still provide a level of privacy protection, and trustmarks are often held out as either an alternative or a complement to privacy legislation.

This article examines both legitimate and non-legitimate privacy trustmarks, and finds that there are serious consumer issues for both categories. Trustmarks have struggled to provide even basic privacy protection to date, and with the demise of BBB Online Privacy and the change in status of TRUSTe, it is difficult to be optimistic about the future.

1.2. The current trustmark 'market'

The privacy trustmark market has changed significantly. The newly for-profit TRUSTe dominates with its high profile, large member base and reported annual revenue of $5 million USD. A handful of other privacy trustmarks still exist, but they are mostly small issue-specific trustmarks such as Privo (catering for children's sites) and ESRB (catering for computer games). There are also a number of low standard trustmarks catering to the cheap end of the market at around $15-150 a year for membership – these trustmarks should not be taken seriously.

This Article includes brief analysis of the following privacy trustmark schemes:

Scheme	Coverage	Members[4]	Notes	Cost (USD)
BBB Online Privacy https://www.bbbonline.org/privacy/	Generic privacy seal for websites.	Approx 700	Closed in July 2008.	Was based on revenue ($200-$7000)
Consumer Guard http://www.consumer-guard.com/	Generic privacy seal for websites.	Not available	Low standard, affordable web seal – limited information available.	$125 per year

[2] Curtin M, *A Failure to Communicate: When a Privacy Seal Doesn't Help*, Interhack Corporation, 25 August 2000, <http://www.interhack.net/pubs/truste-web-bug/>.

[3] <http://www.ataportal.net/>

[4] Membership estimates are from Penn J, *Privacy Seals: Opt In Or Opt Out?*, Forrester Research Inc., 3 October 2006, <http://www.truste.org/pdf/privacy_seals_opt_in_or_opt_out.pdf>. However, estimates for most schemes are optimistic and appear to include numerous expired seals – see for example the discussion concerning PrivacyBot below.

Scheme	Coverage	Members[4]	Notes	Cost (USD)
ESRB http://www.esrb.org/privacy/index.jsp	Specific privacy seal for entertainment software (games) websites. US only.	Approx 50	Large number of sites covered as many members have multiple game sites.	Based on revenue ($200 to $40,000)
Guardian http://www.guardianecommerce.net/	Generic privacy seal for websites.	Approx 500	A basic business verification site with additional low privacy standards.	$15.99 per year.
PrivacyBot http://www.privacybot.com/	Generic privacy seal for websites.	Approx 300	Low standard, affordable web seal with limited functionality.	$100 per year
Privo http://www.privo.com/	Specific privacy seal for children's websites. US only.	Approx 50	Limited to children's sites – focus on verification of parental consent	Not available
TRUSTe http://www.truste.com/	Generic privacy seal for websites plus range of specific seals for email, children's sites etc.	Approx 2400	Highest profile scheme – changed from non-profit to for-profit in 2008.	Based on revenue ($500 to $25,000)
Trust Guard http://www.trust-guard.com/	Generic privacy seal for websites.	Not available – possibly 100-200	Low standard, affordable web seal with limited functionality.	$197 per year
Verified Privacy WBK Certified Seal http://www.websiteboosterkit.com/	Generic privacy seal for websites.	Not available	No checks or standards – sold as a package with the Website Booster Kit.	$49 one-time fee

This article does not provide detailed coverage of all privacy trustmark schemes. For example, it does not cover generic website trustmark schemes that focus on business verification or consumer protection. Some of these schemes do briefly mention privacy, but it is not their focus (e.g. TrustSG in Singapore[5]). Also, this article does not cover the small number of privacy trustmarks that operate in non-English speaking jurisdictions (e.g. the PrivacyMark in Japan[6]).

2. Standards

The most important test for privacy protection in the trustmarks environment is the underlying standards or requirements that are applied by each scheme. Perhaps expectations here should be realistic – what standard should a consumer expect in a market where a business can buy a legitimate looking privacy seal for $15.99 a year?

Indeed, the privacy standards are appallingly low for trustmarks. Attempts to impose higher standards (during the early stages of trustmark development) appeared to fail on commercial grounds. For example, TRUSTe originally had three privacy seals, indicating whether the collection and disclosure of personal information occurred using a colour scheme.

[5] <http://www.trustsg.org.sg/index.html>

[6] <http://privacymark.org/index.html>

This was quickly dropped in favour of a single seal:

> TRUSTe's original idea was to allow a website to display one of three icons, indicating whether its privacy policy was good, ok, or bad. There turned out to be problems with this - strangely enough, no site wanted to post an icon saying that their privacy sucked - and the icons looked too similar anyway. So they went with one icon, a 'badge' that every member site posts. All the badge means is that the site *has* a privacy policy, and that, as far as TRUSTe knows, they haven't violated it.[7]

More recently, TRUSTe indicated that commercial considerations still had an impact on TRUSTe's privacy standards:

> Ms. Maier [CEO] said that TRUSTe would not attract companies into its program if it required them to get the affirmative consent of every user for any use of personal data. [8]

As TRUSTe is the largest remaining trustmark scheme, it is important to examine the privacy standards they apply to members. When a consumer visits a website and clicks on the TRUSTe logo they are taken to a verification page, which makes the following claims:

> The TRUSTe program is consistent with government and industry guidelines concerning the use of your personal information. These standards include the Organization for Economic Cooperation and Development (OECD) *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, the Federal Trade Commission and Department of Commerce's *Fair Information Practices*, the *California Online Privacy Protection Act*, and the *CAN-SPAM Act*.

This sounds very impressive, but is it true?

The first standard mentioned in the claim is the OECD Guidelines. In fact, these OECD Guidelines contain several principles that do not appear anywhere in the TRUSTe standards for a generic seal.[9] These include:

— **OECD Collection Limitation Principle**
There should be limits to the collection of personal data and any such data should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.

— **OECD Data Quality Principle**
Personal data should be relevant to the purposes for which they are to be used, and, to the extent necessary for those purposes, should be accurate, complete and kept up-to-date.

[7] Slashdot, *TRUSTe Decides Its Own Fate Today*, 8 November 1999, <http://yro.slashdot.org/article.pl?sid=99/11/05/1021214>.

[8] Hansell S, *Will the Profit Motive Undermine Trust in Truste*, 15 July 2008, <http://bits.blogs.nytimes.com/2008/07/15/will-profit-motive-undermine-trust-in-truste/>.

[9] <http://www.truste.org/requirements.php>

This is not the first Article to assess TRUSTe's privacy standards against the OECD Guidelines, and they have been found wanting by two Data Protection Commissioners:

> Another, and more troubling problem, relates to the actual privacy standards set by the seal programs. Different seals mean different things. Some are not seals of assurance at all, and do not require adherence to a specified privacy policy. This office [the Information and Privacy Commissioner Ontario] and Australia's federal Data Protection Commissioner conducted a joint study comparing the privacy criteria of the three most popular seals – TRUSTe, BBBOnLine and WebTrust – against the OECD Guidelines. In our opinion, none of these seal programs, at the time of our review, fully met the standards of the OECD Guidelines. The common deficits were no requirement to: 1) limit collection; 2) ensure that data was relevant to the purposes; 3) provide information to the data subject in a reasonable time and manner, without excessive charge, and in an intelligible manner; and 4) provide reasons for any denial of access.[10]

The claim of 'consistency' with the OECD Guidelines is a strong one. The complete absence of two of the OECD Principles is not mentioned on the TRUSTe site.

TRUSTe's privacy standards for their most common seal (the 'basic' privacy seal with over 2000 members) are in fact lower than any privacy law, binding agreement or international privacy standard. Indeed, the TRUSTe standards have to be strengthened (by the inclusion of extra access and correction rights) for organisations wishing to receive the TRUSTe EU Safe Harbour Privacy Seal – a program that includes around 15% of TRUSTe members.

Unfortunately, despite this low bar, TRUSTe has the highest privacy standards of any of the generic privacy trustmark schemes available, now that the BBB Online Privacy Seal program has closed.

The low privacy standards in the trustmark market are further eroded when the trustmark disclaimers are taken into account. For example, the Trust Guard disclaimer states:

> Trust Guard is a website verification company. We take great care in our verification process and strive to offer accurate, reliable information to consumers. If a Trust Guard Verified company changes its information without informing Trust Guard, we cannot be held responsible.[11]

The Guardian eCommerce disclaimer states:

> A Web site's participation in the Safe Site Approval and Privacy Seal Program does not guarantee consumers are protected in terms of privacy and security. While seal program participants have met our strict code of ethics and our site requirements, this does not guarantee a Web site's compliance now or in the future.[12]

Some trustmark schemes make very little attempt to impose privacy standards. For example, the Trust Guard Privacy Verified seal looks impressive to consumers, but to qualify you only have to include a brief three paragraph privacy policy.

---

[10] Ann Cavoukian, *Should the OECD Guidelines Apply to Personal Data Online?* A Report to the 22nd International Conference of Data Protection Commissioners (Venice, Italy), September 2000, <https://ospace.scholarsportal.info/bitstream/1873/6935/1/10301025.pdf>. See also: The Office of the Information and Privacy Commissioner Ontario and The Office of the Federal Privacy Commissioner of Australia, *Web Seals: A Review of Online Privacy Programs*, September 2000, <http://www.privacy.gov.au/publications/seals.html>.

[11] <http://www.truste.org/about/press_release/09_06_07.php>

[12] <http://www.guardianecommerce.net/guardlegal.htm>

Trust Guard also promises that 'As soon as you place your Multi-Seal order, we'll begin the verification process, send you your Seals, and set up your Certificate within one business day; updating any outstanding issues on your Certificate as they are verified. This allows you to start receiving benefits to your website right away!' The cost of the privacy seal is either $197 per year or about $130 per year as part of a multi-seal package deal. Readers may wish to make their own determination of the level of privacy protection provided by Trust Guard at these prices when combined with their 24 hour approval process.

The low level of privacy standards have resulted in great disappointment for many users. A typical expression of this disappointment comes from a complainant:

> The [TRUSTe seal] was like a warm fuzzy blanket that made me feel more comfortable visiting the site in question, and I never paid more heed to it than that. This warm fuzzy blanket, though, turned out to be crawling with bedbugs and full of holes.[13]

3. Enforcement

The most significant criticism of trustmarks is that in practice they have proved to be virtually worthless in the face of major privacy breaches. Their privacy standards are low to begin with, but even these rules are simply not enforced against large, paying members.

It is very difficult to gather overall data on enforcement. Most schemes do not publish any data on breaches, complaints or revocations. The only published figure available is on TRUSTe and that is limited to a brief fact sheet that says there were 3 terminations in the 2007 financial year.[14] Other data can be compiled by reviewing media stories and TRUSTe's 'watchdog advisories'.[15]

From this information it is clear that enforcement action is rare. The following table sets out the known enforcement action by TRUSTe following major privacy incidents. Data and examples for other trustmark schemes are simply not available:

Site	Privacy Breach	Response
Geocities (1998)	GeoCities settled with the Federal Trade Commission over allegations that it misled its users about what it did with their personal data.[16] FTC demanded that GeoCities display a clear privacy policy and get consent from parents before information is taken from children[17] TRUSTe had certified GeoCities as compliant.	TRUSTe declined to revoke GeoCities' trustmark despite the FTC investigation and charges.[18]
AOL (1999)	AOL provided member details to telemarketers. Privacy advocates complained that this breached the privacy policy certified by TRUSTe.[19]	AOL and TRUSTe claimed that the certification only applies to aol.com, not to members.aol.com. No action was therefore taken.

[13] Mansour S, *TRUSTe covering for Facebook*, December 2007, <http://stevenmansour.com/writings/2007/december/24/truste_covering_facebook>.

[14] <http://www.truste.org/about/fact_sheet.php>

[15] <https://www.truste.org/consumers/watchdog_advisories.php>

[16] Federal Trade Commission of America, *Internet Site Agrees to Settle FTC Charges of Deceptively Collecting Personal Information in Agency's First Internet Privacy Case*, 13 August 1998, <http://www.ftc.gov/opa/1998/08/geocitie.shtm>.

[17] Computergram International, *Dyson Believes A Test Case Would Prove Truste's Mettle*, 27 October 1998, <http://findarticles.com/p/articles/mi_m0CGN/is_3525/ai_53140062/pg_1?tag=artBody;col1>.

[18] Regoli N, *Indecent Exposures in an Electronic Regime*, 9 February 2002, Federal Communications Law Journal, <http://www.law.indiana.edu/fclj/pubs/v54/no2/Regoli.pdf>.

Site	Privacy Breach	Response
Hotmail (1999)	A security flaw in Hotmail exposed personal information for a short period. [20] Hotmail was a TRUSTe member.[21]	TRUSTe and Microsoft issued a strange, joint press release indicating that the Hotmail security issue had been cleared by an audit. Details and the identity of the auditors were not made public.[22] No action was taken against Hotmail.
Microsoft Global UID (1999)	A software bug (acknowledged by Microsoft) transferred Hardware IDs to Microsoft regardless of whether users chose to send this information or not. Microsoft was a TRUSTe member.	TRUSTe claimed that the software download was outside their jurisdiction as it did not involve personal information supplied to the website licenced by TRUSTe.[23] TRUSTe took no action. The decision was widely condemned as there were significant references to downloaded software in the Microsoft website privacy policy.
Real Networks (1999)	RealNetworks' RealJukebox software was found to be surreptitiously gathering data about the music-listening habits of its users and passing it on to the company. RealNetworks was a TRUSTe member.	TRUSTe declined to investigate RealNetworks because 'RealJukebox is music-listening software that works via the Internet, but only indirectly through a Web site visit.'[24] Privacy and consumer groups condemned the decision: 'The TRUSTe seal featured on the Real-Networks site created in consumers natural expectations of a certain level of professionalism, honesty, and privacy from the company. When they didn't get it, RealNetworks customers were extremely vocal about their displeasure.'[25]
Deja News (1999)	Deja News' practice of logging IP addresses in conjunction with the site's mail-to feature allowed Deja News to collect personal information in breach of their privacy policy. Deja News was a TRUSTe member.[26]	TRUSTe eventually issued a statement suggesting that they had 'specified certain clarifying language to be included in the privacy statement'. But Deja News, independent of TRUSTe, had already dropped the practice. No other action was taken against Deja News.
Batteries .com (2003)	A Web site licensed by TRUSTe, batteries.com, stated in its privacy policy that it would not share consumer information with third parties, yet consumers received spam that could be traced back to an email leak by batteries.com.[27]	TRUSTe required batteries.com staff to undergo privacy training. They also had to update their privacy policy and send apologies to customers. TRUSTe stated: 'This benefits both batteries.com and the marketplace more than if TRUSTe had simply revoked its right to post the TRUSTe seal'.
Choicepoint (2005)	Choicepoint inadvertently sold personal records to criminals involved in an identity theft scheme..[28] This compromised the personal information of 163,000 people – Choicepoint settled with the FTC for a $15 million USD fine.	TRUSTe was silent during this entire incident. Notably, at the end of 2005 TRUSTe did acknowledge the kind assistance of Choicepoint in formulating the TRUSTe Security Guidelines 2.0.[29]

---

[19] Smith R, *Online Profiling from a Consumer's Perspective*, 8 November 1999, <http://www.cdt.org/privacy/FTC/profiling/russsmith.htm>.

[20] Lettice J, *MS-commissioned secret audit clears MS over Hotmail holes*, The Register, 5 October 1999, <http://www.theregister.co.uk/1999/10/05/mscommissioned_secret_audit_clears_ms/>.

[21] TRUSTe, *Hotmail Advisory*, 9 September 1999, <https://www.truste.org/consumers/watchdog_advisories/0999_microsoft.php>.

[22] TRUSTe, *Hotmail Resolution*, 4 October 1999, <https://www.truste.org/consumers/watchdog_advisories/1099_microsoft.php>.

[23] TRUSTe, *Microsoft UserId Investigation Results*, March 1999, <https://www.truste.org/consumers/watchdog_advisories/0399_microsoft.php>.

[24] Oakes C, TRUSTe Declines Real Probe, Wired, 11 September 1999, <http://www.wired.com/science/discoveries/news/1999/11/32388>.

[25] Levine D, *Personal Information Privacy – What Rights do you have to your data?*, Know Your Rights, Vol 8, Issue 4, April 2000, <http://www.smartcomputing.com/editorial/article.asp?article=articles/archive/g0804/18g04/18g04.asp&guid=>.

[26] TRUSTe, *IP Logging:Watchdog # 1847 – Deja Statement of Finding Investigation Results*, April 1999, <https://www.truste.org/consumers/watchdog_advisories/0499_dejanews.php>.

[27] TRUSTe, *A Case Study in Enforcement: batteries.com*, 2003, <https://www.truste.org/pdf/Enforcement_Case_Study.pdf>.

[28] Singel R, *More on Choicepoint*, Secondary Screening, February 2005, <http://www.secondaryscreening.net/static/archives/2005/02/>.

[29] TRUSTe, *Security Guidelines*, November 2005, <http://www.truste.org/pdf/SecurityGuidelines.pdf>.

Site	Privacy Breach	Response
Gratis (2005)	Gratis Internet, parent company of FreeiPods.com, offered free iPods for users who agree to try out various subscription offers. In 2005 Gratis sold the data it gathered on 7.2 million consumers to an email advertising firm.[30] The owners of Gratis were investigated and sued. Gratis was a TRUSTe member.	When asked by Wired News in 2004 how third-party spammers got hold of Gratis members' e-mail addresses, TRUSTe said it could not find a problem with Gratis' practices - 'The results of our investigation indicate that Gratis Internet did not violate their privacy policy.' [31]TRUSTe terminated Gratis on 9 February 2005,[32] but provided no reasons, stating that: details of violations are subject to confidentiality. On 11 February 2005 TRUSTe issued a strange press release that TRUSTe and Gratis would 'work together for the benefit of consumers to ensure Gratis websites are in compliance with the TRUSTe program requirements'.[33] Shortly after this press release (exact date unknown) the TRUSTe website was amended to say that 'Gratis has failed to finalize the required changes … and has not been recertified into the TRUSTe Web Privacy Seal Program'.[34]
AOL (2006)	AOL released the log of 3 month's worth of searches by 650,000 users, for open download by researchers. Names were replaced by a unique user number, resulting in many users being clearly identified, in breach of the AOL privacy policy. Several senior AOL staff were sacked over the incident.[35]	Although AOL was a TRUSTe member during this period, TRUSTe made no public comment about the incident and took no action against AOL. In 2007 TRUSTe honoured AOL as one of three 'Most Trusted Companies for Privacy'.[36]
Facebook Beacon (2007)	Beacon was developed by Facebook so advertisers could reach new audiences. When a Facebook user buys something a small frame would pop up giving the user an option to share that information with friends. This window would only appear for a few seconds and if the user missed it the data would be posted in the user's news feed. Facebook was a TRUSTe member.	After public outcry Facebook changed the way Beacon operates. Users also complained to TRUSTe.[37] TRUSTe remained silent throughout the incident. Some time after Beacon had been reformed, TRUSTe and Facebook issued a joint press release: 'TRUSTe and Facebook Announce Disclosure Enhancements for New Web sites that Implement Beacon… TRUSTe Continues to Lead Development of Online Privacy Standards'.[38]

[30] Kahney L, *FreeiPods.com Sold Private Data – Despite Promising Not to*, 16 March 2006, <http://cultofmac.com/freeipodscom-sold-private-data-despite-promising-not-to/248>.

[31] Kahney L, *FreeiPods.com Sold Private Data – Despite Promising Not to*, 16 March 2006, <http://cultofmac.com/freeipodscom-sold-private-data-despite-promising-not-to/248>.

[32] TRUSTe, *TRUSTe Revokes Seals From FreeiPods*, 9 February 2005, <http://www.truste.org/about/press_release/02_09_05.php>.

[33] TRUSTe, *TRUSTe and FreeiPods.com agree to work together to ensure Customer Privacy*, 11 February 2005, <http://www.truste.org/about/press_release/02_11_05.php>.

[34] TRUSTe, *TRUSTe Watchdog Advisories*, accessed August 2008, <https://www.truste.org/consumers/watchdog_advisories.php>.

[35] Arrington M, *AOL Proudly Releases Massive Amounts of Private Data*, TechCrunch, 6 August 2006, <http://www.techcrunch.com/2006/08/06/aol-proudly-releases-massive-amounts-of-user-search-data/>.

[36] Marketwire, *TRUSTe and Ponemon Institute Name HP, Intuit and AOL the Top Three Most Trusted Companies of 2007 for Privacy*, 30 January 2008, <http://money.aol.com/news/articles/qp/pr/_a/truste-and-ponemon-institute-name-hp/rfid65588526>.

[37] Karmens R, *A Letter to TRUSTe Regarding Facebook*, Binary Freedom, 26 November 2007, <http://www.binaryfreedom.info/node/262>.

[38] TRUSTe, *TRUSTe and Facebook Announce Disclosure Enhancements and Model Privacy Policy Language for New Web sites that Implement Beacon*, 14 December 2007, <http://www.truste.org/about/press_release/12_14_07.php>.

Site	Privacy Breach	Response
Facebook account closure (2007)	Numerous Facebook members have concerns that they cannot close their Facebook account, because there is no mechanism to do so on the Facebook site. Several prominent consumers have complained about this to TRUSTe. [39]	TRUSTe advised complainants that 'Facebook is not violating its privacy policy or TRUSTe's program requirements'[40] In another complaint, they called Facebook's account deletion process 'inconvenient,' but said Facebook was 'being responsive to us, and they currently meet our requirements.'[41] Facebook was able to delete user details for one member, but only after his complaint appeared on television in the UK.[42]

TRUSTe has defended itself against this type of criticism, stating: 'As for enforcing standards our goal is to resolve privacy issues, offer incentives to change business practices, and fix problems when they inevitably occur, not in kicking out websites'.[43] TRUSTe also points to its success in terminating Gratis:

> Consumer generated Watchdog complaints have resulted in severe sanctions against licensees, including TRUSTe's public termination of Gratis Internet - a company that the New York Attorney General has sued subsequent to TRUSTe's actions.[44]

In fact, Gratis Internet is the only major company that appears to have been terminated by TRUSTe. And the investigation and subsequent law suit by the New York Attorney General were launched well before TRUSTe took any action at all. Gratis retained its membership of TRUSTe for many months after TRUSTe was first informed that they had sold millions of email addresses to a marketing company.

This defence looks a bit thin when TRUSTe can only point to one effective enforcement action in more than 11 years – against a company who was already being taken to court by regulators. As one commentator noted: 'I cannot find a good reason to advise a consumer with a privacy complaint against a TRUSTe seal holder to bother filing a complaint with TRUSTe'.[45]

Other trustmark schemes have had even less success at enforcement, or have published no information on enforcement at all. [46]

---

[39] See for example: Aspan M, *On Facebook, leaving is hard to do*, International Herald Tribune, 11 February 2008, <http://www.iht.com/articles/2008/02/11/business/11facebook.php>, and, Mansour S, *TRUSTe covering for Facebook*, December 2007, <http://stevenmansour.com/writings/2007/december/24/truste_covering_facebook>.

[40] Mansour S, *TRUSTe covering for Facebook*, December 2007, <http://stevenmansour.com/writings/2007/december/24/truste_covering_facebook>.

[41] Aspan M, *On Facebook, leaving is hard to do*, International Herald Tribune, 11 February 2008, <http://www.iht.com/articles/2008/02/11/business/11facebook.php>.

[42] McGarr S, *Facebook's European Privacy Problem*, MaGarr Solicitors, 20 January 2008, <http://www.mcgarrsolicitors.ie/2008/01/20/facebooks-european-privacy-problem/>.

[43] Hansell S, *Will the Profit Motive Undermine Trust in Truste?*, 15 July 2008, <http://bits.blogs.nytimes.com/2008/07/15/will-profit-motive-undermine-trust-in-truste/>.

[44] TRUSTe, *TRUSTe Certifications and Online Trust*, 25 September 2006, <http://blog.truste.org/?m=200609>.

[45] Gellman R, *TRUSTe fails to justify its role as privacy arbiter*, Privacy Law and Policy Reporter Volume 7 No. 6, December 2000, <http://www.austlii.edu.au/au/journals/PLPR/2000/53.html>.

[46] Gellman R, *TRUSTe fails to justify its role as privacy arbiter*, Privacy Law and Policy Reporter Volume 7 No. 6, December 2000, <http://www.austlii.edu.au/au/journals/PLPR/2000/53.html>.

4. Transience

Consumer confidence in trustmarks has also been shaken by their transient nature. More trustmark schemes have disappeared than have survived, and it is difficult for consumers to invest their trust in this form of privacy protection:

> Trustmarks can fade. Some trustmarks continue to exist, but the organizations that stand behind them and attempt to provide 'heft' to the mark itself have long since evaporated. In this case, the mark remains but its meaning fades… While the programs may have closed, the trustmarks remain on some sites.[47]

The most significant demise has been the withdrawal of the BBB Online Privacy Seal service. At its peak this service had accredited over 700 websites. New applications ended in 2007 and the complete service (including managing complaints for existing accredited sites) ceased on 1 July 2008.[48] Many sites still display the seal. BBB Online does provide a generic Reliability Seal. However, the privacy standards required under this service are significantly lower than those required under the Privacy Seal.

In Australia, the high profile privacy trustmark 'eTick' was established in 2001. It suffered a financial collapse in 2002 and was withdrawn.[49] It remains the only high profile example of a privacy web seal in Australia. Despite the withdrawal of eTick in 2002, both eBay Australia[50] and eBay India[51] still display their eTick logos in 2008, including links from their help pages.

The web privacy seal graveyard includes other prominent examples such as controlscan, enshrine, web trader, trust UK and safetrade.[52]

5. Timing issues

The level of protection offered by a web trustmark depends on the time of a transaction and/or the time of making a complaint. Protection will only be available for the period where the organisation is certified. There may also be other time limits on lodging a complaint.

---

[47] Leading Edge Forum, *Transparency and Assurance: Putting a Measure on Digital Trust*, published in Digital Trust series, Volume 7, 2008, <http://www.csc.com/aboutus/leadingedgeforum/knowledgelibrary/uploads/LEF_2008DigitalTrustVol7.pdf>.

[48] Better Business Bureau (BBBOnLine), *BBBOnLine Privacy Seal*, 2003, <http://www.bbbonline.org/privacy/>.

[49] Greenblat E, *eTick sacks CEO, reviews finances*, Sydney Morning Herald, 24 August 2002, <http://www.smh.com.au/cgi-bin/common/printArticle.pl?path=/articles/2002/04/24/1019441256300.html>.

[50] eBay, *Privacy Central*, accessed 10 September 2008, <http://pages.ebay.in/help/welcome/privacy_overview.html>.

[51] eBay, *Internet Standards Certification*, accessed 10 September 2008, <http://pages.ebay.com.au/help/community/certification.html>.

[52] Rao V, Cerpa N, Jamieson R, *A Comparison of Online Electronic Commerce Assurance Service Providers in Australia*, 14th Bled Electronic Commerce Convention, June 25-26 2001, <http://ecom.fov.uni-mb.si/proceedings.nsf/Proceedings/FC446171B839BEE3C\1256E9F003123C8/$File/33_Rao.pdf>.

The biggest timing problem is the volatile nature of membership of trustmark schemes. Memberships often lapse for non-payment. Typically these are quickly renewed but consumers lose their rights (or become confused about their rights) during the intervening period.[53] In the Gratis case (discussed above) the membership status of the company changed almost daily as TRUSTe issued multiple press releases and clarifications.[54] Privacy legislation is far more static by contrast.

Timing issues were also a concern in the GeoCities case, where it appeared that TRUSTe maintained the certification of GeoCities even as they were negotiating a substantial privacy law settlement with the Federal Trade Commission:

> In June 1998, the FTC announced - to everyone's surprise - that it and GeoCities had come to a settlement regarding violations of consumer privacy. Everyone was surprised because this was the first anyone had heard of it. Where was TRUSTe? Caught flat-footed, TRUSTe scrambled for a few days, then made its own announcement. It pointed out that GeoCities had begun the alleged privacy violations before applying to become a member (in April) and being accepted (in May). Therefore, TRUSTe claimed, the violations were technically not under the scope of their investigation. But turn that around and put it another way - it was able to become a TRUSTe member even while under investigation by the FTC, and TRUSTe said nothing. [55]

If trustmark schemes will not provide basic information and warnings to consumers because of 'timing issues' their value as a privacy protection is significantly diminished.

TRUSTe isn't the only trustmark scheme that has allowed timing issues to become a barrier to privacy protection. PrivacyBot offers a 'provisional' trustmark – a seal that looks exactly the same to the consumer as the regular PrivacyBot seal:

> Use our 6 Step Wizard to create a Privacy Policy in about 10 minutes. Your Privacy Policy & Trustmark will be delivered promptly online. Display the Trustmark today on a provisional basis.[56]

A consumer who provided personal information to the site during this 'provisional' period receives no protection and cannot use the PrivacyBot complaints service if any problems occur prior to full certification. Provisional periods can be as long as six months. This odd approach displays the high value that trustmarks place on business convenience, and the low value placed on privacy protection.

Also, consumers may lose some rights under trustmark schemes if they don't complain quickly. Consumers lose their rights under the Guardian privacy seal if they don't complain of a breach within 25 days of the original transaction.[57] This compares poorly with the time periods used in general privacy and consumer protection law. It also compares poorly with best practice advice for consumers from Privacy Commissioners – for example the Australian Privacy Commissioner encourages people to complain within 12 months of becoming aware of a the breach (not the date of the original transaction).[58]

---

[53] See for example the consumer discussion regarding a lapse in membership of the online retail giant newegg: <http://digg.com/security/Newegg.com_pulling_a_fast_one_>. Also, see the debate regarding the membership of me.dium <http://blogme.dium.com/content/2008/04/just-the-facts-maam/>.

[54] Kahney L, *FreeiPods.com Sold Private Data – Despite Promising Not to*, 16 March 2006, <http://cultofmac.com/freeipodscom-sold-private-data-despite-promising-not-to/248>.

[55] Slashdot, *TRUSTe Decides Its Own Fate Today*, 8 November 1999, <http://yro.slashdot.org/article.pl?sid=99/11/05/1021214>.

[56] <http://www.privacybot.com/>

[57] <http://www.guardianecommerce.net/guardlegal.htm>

[58] <http://www.privacy.gov.au/privacy_rights/complaints/index.html>

6. Trustmark scams

In addition to the many concerns regarding legitimate trustmarks, there are numerous instances of trustmarks being used in online scams. The most common example is that a site will claim to be certified and display the seal on their website or on their privacy policy. This is now so common that the major trustmark schemes publish lists of known fake sites. The TRUSTe list of known fakes includes 125 entries.[59]

Where trustmark certifications have expired, there appears to be little that can be done to have the seal removed. Unless the consumer clicks on the seal to check, they will not know that the seal is worthless. This appears to be a widespread problem with some of the small trustmark schemes. For example, the majority of PrivacyBot seals examined during research for this article had expired.

PrivacyBot also does not publish a registry of current members or a list of fake sites, making it almost impossible to check a claim in a privacy policy if they do not display the seal properly (as the seal is supposed to include a deep link to the registry entry).

For example, a Google search for 'we have registered with privacybot.com' or 'privacybot trustmark' on 10 September 2008 returned 22 relevant results. These are the standard words used in PrivacyBot privacy policies. Of the 22 sites, 13 had expired, 5 provided no links to a registry entry (making it impossible to check their status) and one still had a 'provisional' status, five months after their application.

Despite all 22 sites claiming that they were members of PrivacyBot, only 3 sites were able to be confirmed as active members of PrivacyBot. If a consumer had believed the privacy policy and not checked the status themselves, their chance of privacy protection was a dismal 13%.

Search Rank	Site	Status
1	http://www.iso9000simplified.com/	Provisional
2	http://sitestats.com/privacy/policy.php	Expired
3	http://www.heartof.com/privacy.php	Expired
4	http://sitestats.com/privacy/policy.php	Expired
5	http://www.e-file-tax-returns.org/privacy.html	Active
6	http://www.tricktape.com/privacystatement.aspx	Expired
7	http://www.activewin.com/terms/privacy.shtml	No registry link
8	http://www.onlinecomputerservicenetwork.com/privacy.html	Expired
9	http://www.usemybank.com/	Active
10	http://www.quantumbooks.com/	No registry link
11	http://www.ugogrl.com/	Expired
12	http://www.3crm.com/help.php?section=business	Expired
13	http://www.computerservicenetwork.org/	Expired
14	http://www.audaciousarts.com/privacy.html	Expired
15	http://www.cst-consulting.com/privacy.htm	No registry link
16	http://www.thetascongroup.com/privacy_policy.html	No registry link
17	http://www.wtiq.com/privacy/policy.php	Expired
18	http://www.pcpro.co.uk/html/Privacy_Policy.html	No registry link
19	http://www.addressender.com/index.php	Expired
20	http://mardirect.com/privacy.htm	Expired
21	http://truevine.net/privacypolicy1.html	Expired

[59] <http://www.truste.org/consumers/web_seal_violators.php>

Search Rank	Site	Status
22	http://free.1040now.net/	Active

There are numerous other trustmark products which are unlikely to deliver any privacy protection and are, in reality, scams. For example, the Verified Privacy WBK Certified Seal is sold as part of the Website Booster Kit.[60] It costs just $49 and the site claims to have sold over 40,000 kits. For a one-off payment you can use the seal forever without any checks or other requirements. The kit does include a template privacy policy, but the text for the 3-point privacy policy is just clumsily copied from the Trust Guard site with one or two words changed (although at point 2 it still accidentally mentions Trust Guard).[61]

In addition to the prevalence of fake, useless and expired trustmarks displayed on websites, other scams have been reported. The TRUSTe name and domain were used as part of an escrow payment scam.[62] Both TRUSTe[63] and BBB Online[64] have also been targets of sophisticated phishing scams. In some cases even the verification pages have been recreated by fraudsters.[65]

Although these scams are not the fault of the trustmark schemes, they still have a negative impact on the usefulness of trustmarks as a privacy protection:

> One can't help but wonder whether verification services like TRUSTe may at some point cause more problems than they solve. If the appearance of an official looking seal on a website lulls the user into a false sense of security, then what good is it? [66]

7. Coverage

The limited coverage of privacy trustmarks has been a major concern for consumers. Despite the grand sounding names, such as privacy seal, certified privacy seal or verified privacy seal, most trustmarks only cover a very small area of an organisation's activity.

For example, the TRUSTe privacy seal states:

> The privacy statement and practices of www.XYZ.com have been reviewed by TRUSTe for compliance with our strict program requirements.

The BBB Online Privacy Seal stated:

> The seal does not reflect the past practices or policies of any particular seal participant, or practices pertaining to information collected other than online.

---

[60] <http://www.websiteboosterkit.com/tool3.html>

[61] <http://www.websiteboosterkit.com/verifiedprivacy.html>

[62] *Scam using TRUSTe.org?*, 12-13 December 2007, <http://www.fraudwatchers.org/forums/archive/index.php/t-12447.html>.

[63] Wagstaff J, *TRUSTe's Own Phishing Hole*, Loose Wire Blog, 10 November 2004, <http://www.loosewireblog.com/2004/11/trustes_own_phi.html>.

[64] Currie E, *Better Business Bureau – Don't Fall for the Bbb Internet Scam*, 16 August 2007, <http://www.articlesbase.com/internet-articles/better-business-bureau-dont-fall-for-the-bbb-internet-scam-199591.html>.

[65] Ong GM, *Latest, Coolest Gizmos at a Malware Near You*, 2 July 2007, <http://www.avertlabs.com/research/blog/index.php/2007/07/02/latest-coolest-gizmos-at-a-malware-near-you/>.

[66] Wagstaff J, *TRUSTe's Own Phishing Hole*, Loose Wire Blog, 10 November 2004, <http://www.loosewireblog.com/2004/11/trustes_own_phi.html>.

These restrictions have been strictly and severely enforced in practice.

In the Microsoft Global UID case, TRUSTe stated that its seal covered only Microsoft's website – not its software – and that the data Microsoft gathered was not transmitted to Microsoft's website.[67] But consumer groups argued that Microsoft's privacy page (prominently displaying the TRUSTe seal) also discussed online registration of software products, and noted that the 'personal profile' from their software registration appears on the website and is editable from the website. That page appeared to claim that registration *was* covered by the TRUSTe certification.[68]

Similar arguments were used to justify the lack of action in the RealNetworks case and the AOL case.

In the RealNetworks case TRUSTe claimed that the 'music-listening software works via the Internet, but only indirectly through a Web site visit'.

In the AOL case TRUSTe claimed that the seal only covers 'www.aol.com' and not 'members.aol.com.'. This means that if you visit www.aol.com (which is covered by the seal) and you decide to join you are sent to members.aol.com which is not covered by the TRUSTe seal, and you lose your protection.[69]

These three decisions are questionable. Taken together they are one of the chief causes of TRUSTe's poor reputation.[70] The AOL decision is particularly galling, and makes TRUSTe look like they were happy for AOL to lure people into paying for a service based on a privacy promise that is then withdrawn once the money is handed over.

8. Independence

There have been numerous concerns expressed about the independence of trustmark schemes, as their revenue comes from fees paid by members and sponsorship (typically from large members).[71]

Trustmark schemes deny that sponsorship or membership fees have any influence on decisions, but this defence is weakened by the poor enforcement history of trustmark schemes when faced with significant privacy breaches by their members.

In particular TRUSTe has failed to take action in a number of high profile cases involving its biggest ('premier') sponsors – Microsoft and AOL. It is unclear why TRUSTe accepts sponsorship from organisations that it is supposed to certify and regulate.[72]

---

[67] Tedeschi B, *E-Commerce Report; Some online sellers are hiring prominent auditors to verify their privacy policies and increase trust*, The New York Times, 18 September 2000, <http://query.nytimes.com/gst/fullpage.html?res=9501E2DF163BF93BA2575AC0A9669C8B63&sec=&spon=&pagewanted=all>.

[68] Slashdot, *TRUSTe Decides Its Own Fate Today*, 8 November 1999, <http://yro.slashdot.org/article.pl?sid=99/11/05/1021214>.

[69] Smith R, *Online Profiling from a Consumer's Perspective*, 8 November 1999, <http://www.cdt.org/privacy/FTC/profiling/russsmith.htm>.

[70] Clark T, *TRUSTe clears Microsoft on technicality*, CNET News, 22 March 1999, <http://news.cnet.com/2100-1023-223374.html>.

[71] Rotenberg M, Hoofnagle C, *In the Matter of Microsoft Consent Order*, Electronic Privacy Information Center, 9 September 2002, <http://epic.org/privacy/consumer/microsoft/ordercomments.html>.

[72] Molander J, *Trust For Sale: TRUSTe Certifies the Web's Dreck*, 25 September 2006, <http://www.thoughtshapers.com/index.php/weblog/archive/trust-for-sale-truste-certifies-the-webs-dreck-direct-revenue-siteadvisor/>.

Although data on enforcement is not available for most schemes other than TRUSTe, there was some limited analysis of the BBB Online Privacy Seal in 2000. This analysis expressed concern about the small number of enforcements, and highlighted a case where BBB Online appeared to change a decision following a threat by the member to withdraw from the scheme:

> The appearance here is that eBay threatened to drop BBB Online so BBB gave in to eBay's demands. Vacating a decision may be appropriate sometimes, but withdrawing it from public view once posted is a terrible precedent. It undermines the integrity of BBB's reporting system.[73]

There have also been questions about industry links with the trustmark schemes. For example, the Board of TRUSTe has included Directors from members who have been involved in significant cases, such as Microsoft, Real and AOL. It has also included Directors from Doubleclick, and conversely the Chair of TRUSTe sat on a privacy advisory board for Doubleclick, despite their membership of TRUSTe at the time.[74] The perception of bias in these situations is high, and TRUSTe makes very little attempt to appear independent.

TRUSTe has also published *joint* press releases with industry members under investigation – such as Microsoft, Geocities, RealNetworks and Facebook. To an observer of privacy regulation this behaviour is unprecedented, and provides little confidence in the independence of TRUSTe.

On July 15 2008 TRUSTe changed its status from non-profit to for-profit and accepted investment (from Accel – part-owners of Facebook).[75] The current Board of Directors for TRUSTe is being reformed and consists only of their new investors. Depending on the makeup of the new Board, this may reduce perceptions of conflict of interest, although it does raise some perception issues regarding Facebook (a TRUSTe member).

Obviously this is a recent change, but the majority of TRUSTe members still retain the standard (old) TRUSTe wording in their privacy policies:

> XYZ is a licensee of the TRUSTe Web Privacy Seal Program. TRUSTe is an independent, non-profit organization whose mission is to build user's trust and confidence…

This misleading information should be corrected.

A very small number of sites have changed their description of TRUSTe since the change in status. For example, AOL now describes TRUSTe as 'an independent organization whose mission is to advance privacy and trust in the networked world'.[76] If organisations are going to tell consumers that TRUSTe is 'independent' then greater care should be taken regarding independence and conflicts of interest. AOL remains a premier sponsor of TRUSTe – this is not disclosed in the AOL privacy policy.

Possibly the low point of TRUSTe's approach to independence occurred on 30 May 2008, when they issued a press release titled 'Does Google Care About Privacy and Trust?'.

It was a critique of Google's failure to provide a link to its privacy policy on the Google home page, and by TRUSTe standards was very strongly worded:

---

[73] Gellman R, *Online privacy dispute resolution: BBBOnline*, Privacy Law and Policy Reporter Volume 7 No. 7, December 2000, <http://www.austlii.edu.au/au/journals/PLPR/2000/62.html>.

[74] Raven K, *TRUSTe, DoubleClick, Privacy, and a Possible Conflict of Interest*, 30 May 2000, <http://www.fitug.de/debate/0005/msg00703.html>.

[75] Bonanos P, *Accel invests in former non-profit TrustE*, Tech Confidential , 15 July 2008, <http://www.thedeal.com/techconfidential/vc-ratings/vc-ratings/accel-invests-in-former-nonpro.php>.

[76] <http://about.aol.com/aolnetwork/aol_pp>

> It is inevitable that [Google] draw fire regarding their lagging privacy commitment… If Google applied today for the TRUSTe privacy seal of approval, we would require them to post a link on their homepage. All TRUSTe certified search engines AOL, Yahoo, Microsoft and Lycos follow this practice… As one of the most pervasive collectors of internet data and information of all types, Google should step up to meet best practices as have the 1500 companies who proudly display the TRUSTe seal.[77]

This attack on Google comes from an organisation which has never once in 11 years issued a criticism of an existing TRUSTe member stronger than a mild 'concern'. But of course, Google is not a member. Indeed, if Google were to join TRUSTe (including their many affiliate sites such as Flickr and YouTube) it would provide hundreds of thousands of dollars in new revenue for TRUSTe. The attack on Google's 'lagging privacy commitment' contrasts with glowing press releases issued by TRUSTe regarding members such as Microsoft[78] and Facebook.[79]

The TRUSTe attack on Google was, clearly, a serious mistake. It adds fuel to the perception that TRUSTe is biased towards organisations that pay large membership fees and provide corporate sponsorship to TRUSTe. The complete lack of objectivity in their contrasting media releases on competitors Google and Microsoft is in stark contrast to the independence and professionalism required of regulators.

9. Penetration

Trustmark schemes have not been successful in penetrating the market. Just 7 out of the global top 50 visited websites have any form of trustmark. This is made up of 7 sites with TRUSTe seals (3 of those are Microsoft brands).[80]

One emerging criticism of trustmarks is that the proportion of legitimate, privacy-friendly websites with trustmarks is diminishing, while the number of scam sites or privacy intrusive websites carrying trustmarks is increasing. There is a risk of guilt by association for legitimate sites, as some commentators have started to warn consumers that a trustmark may actually indicate a higher risk than the absence of a trustmark.

A major cause of this issue is the large number of scam, fake, expired and useless seals that now appear online (discussed above).

A more pressing issue is the number of privacy-intrusive sites who have been certified by TRUSTe – the last high-profile generic privacy trustmark scheme still operating. TRUSTe has listed all of the following sites as certified in recent years, either as part of the privacy seal program or the trusted download program. These organisations are all well known to privacy, security and consumer advocates, as they have been subject to numerous privacy and security breaches, FTC investigations and ongoing consumer campaigns[81]:

Website	Issues

[77] TRUSTe, *Does Google Care about Privacy and Trust*, 30 May 2008, <http://blog.truste.org/?p=85>.

[78] TRUSTe, *IE8: Browsing 'In Private' Features Take User Privacy to Center Stage*, 25 August 2008, <http://blog.truste.org/?p=100>.

[79] TRUSTe, *Facebook Helps Keep Your Work, Family, Friends Separate*, 20 March 2008, <http://blog.truste.org/?p=70>.

[80] <http://www.alexa.com/site/ds/top_sites?ts_mode=global&lang=none>, accessed on 29 August 2008.

[81] Edelman B, *Certifications and Site Trustworthiness*, 25 September 2006, <http://www.benedelman.org/news/092506-1.html>.

Website	Issues
coupons.com	Deceptive installation http://blog.truste.org/?p=66
direct-revenue.com	Non-consensual spyware installation, including deceptive installations and installations through security vulnerabilities. http://www.benedelman.org/spyware/nyag-dr/
eZula.com	Adware / malware http://www.spywareguide.com/product_show.php?id=9
focalex.com	Spyware http://www.spywareremove.com/removeFocalex.html
freecreditreport.com	Consumer protection warnings http://www.ehow.com/how_4502163_cancel-freecreditreportcom-account.html
freeipods.com (Gratis Internet)	Spam seller http://cultofmac.com/freeipodscom-sold-private-data-despite-promising-not-to/248
funwebproducts.com	Malware - sends a record of every websearch made, with the user's IP address http://www.spywareinfoforum.com/index.php?showtopic=15652
Idownload (e.g. smartshopper)	Deceptive practices http://www.edbott.com/weblog/?p=496 Malware http://www.411-spyware.com/remove-smartshopper
maxmoolah.com	Spam seller http://www.siteadvisor.com/
Relevant Knowledge (provisional)	Tracking / adware http://www.411-spyware.com/remove-relevantknowledge
webhancer.com	Installs tracking software without informed consent http://www.siteadvisor.com/
wowpapers.com (Hotbar)	Spyware / adware http://www.spywareinfoforum.com/lofiversion/index.php/t50584.html
yourgiftcards.com	Spam seller http://bbs.spamgourmet.com/viewtopic.php?start=75&t=81

Note that TRUSTe has defended the appearance of many of these sites on its list of sealholders, claiming that they were listed in error:

> FunWebProducts, was, by an error in our database listed on our customer list, but it has never been certified, and has never displayed any seals or reference to TRUSTe to consumers.[82]

In total, more than a dozen such errors have been claimed by TRUSTe.[83] Many of the sites were listed in error for over 12 months.[84]

[82] TRUSTe, *TRUSTe Certifications and Online Trust*, 25 September 2006, <http://blog.truste.org/?m=200609>.

[83] Porter W, *TRUSTe Answers The Challenge and Asks Mr. Edelman To Do The Same…*, 2 October 2006, <http://www.revenews.com/wayneporter/truste-answers-the-challenge-and-asks-mr-edelman-to-do-the-same/>.

[84] Edelman B, *Certifications and Site Trustworthiness*, 25 September 2006, <http://www.benedelman.org/news/092506-1.html>.

10. Consumer understanding

TRUSTe's own research on factors that are most likely to increase privacy trust shows that a web seal scores 9% (ranked 7th).[85] But after more than 10 years of operation, the actual level of privacy protection provided by a trustmark is still poorly understood by consumers:

> The presence of so many trustmarks almost guarantees misunderstandings, misuse and misappropriation of claims of digital trust. The desire to invoke digital trust for online enterprises, combined with the business opportunities that await those who provide emblems of trust (trustmarks), has led to hundreds of trust claims and marks. While the urge to represent and measure trust in the digital enterprise is admirable, not all trustmarks deliver digital trust.[86]

The operators of trustmark schemes have been aware for many years that consumers do not understand the full limitations of the seals (e.g. low standards, limited coverage), yet little has been done to combat this misunderstanding. For example, the CPAs who ran the WebTrust seal conducted their own empirical research on consumer understanding in 2000. They found:

> 22% incorrectly indicated that 'customers are absolutely protected against fraud.' This result is cause for concern. If 22% of consumers believe that WebTrust absolutely protects against fraud, CPAs could be exposed to legal action. Another question revealed that 59% of study participants thought that the CPA 'approved the business practices'. [87]

Some trustmark schemes add to this consumer confusion by making broad (and incorrect) claims that their privacy standards are consistent with privacy laws. One scheme really confuses consumers by publishing a list of 'safe links' on its website. These are not certified members of the trustmark program, they are just links that appear to generate click-through advertising revenue.[88]

There is a concern that consumers may be misled into revealing more information than they would reveal to other sites:

> Considering that the vast majority of the public may be unaware of this misrepresentation and believes in the illusion of safety created by the placement of a trustmark on a Web site, this misplaced trust may lower users' personal guards, leading them to reveal more information than they would in situations without the appearance of the privacy-ensuring mechanisms. These user perceptions may ultimately result in a situation more detrimental to users than the absence of privacy policies or trustmarks altogether. [89]

The most famous study of consumer understanding of trustmarks was conducted in 2003. It asked consumers to assess the privacy protection offered by three real privacy seals (TRUSTe, BBB Online and CPA WebTrust) plus one phoney privacy seal (Web Shield). Web Shield was created from standard clip art. Sadly, the fake seal was recognised by 15% of consumers as a legitimate trustmark seal, only slightly below TRUSTe (42%) and BBB (29%) and well above WebTrust (8%):

---

[85] TRUSTe, *2007 Most Trusted Companies for Privacy Award*, summary prepared by Ponemon Institute, 29 January 2008, <http://www.truste.org/pdf/2007_Most_Trusted_Companies_Award.pdf>.

[86] CSC Consulting, *Transparency and Assurance: Putting a Measure on Digital Trust*, 2008, <http://www.csc.com/aboutus/leadingedgeforum/knowledgelibrary/uploads/LEF_2008DigitalTrustVol7.pdf>.

[87] Portz K, Strong J, Busta B, Schneider K, *Do Consumers Understand What WebTrust Means?*, October 2000, <http://www.nysscpa.org/cpajournal/2000/1000/features/f104600a.htm>.

[88] <http://www.guardianecommerce.net/guardlinks.htm>

[89] Regoli N, *Indecent Exposures in an Electronic Regime*, 9 February 2002, Federal Communications Law Journal, at page 370, <http://www.law.indiana.edu/fclj/pubs/v54/no2/Regoli.pdf>.

This finding suggests that any official-looking graphic placed on a website has an equal chance of persuading the consumer that the site is trustworthy, regardless of any relation between that graphic and the actual web assurance seals.[90]

11. Government and Trustmark Schemes

There has been some minimal overlap between government regulation of privacy and trustmark schemes, although to date this has been restricted to a few instances in the United States.

For example, several trustmark schemes, including TRUSTe, are approved complaints resolution bodies for the purposes of the EU Safe Harbour regime. Their actual legal role in the Safe harbour regime is limited to the provision of dispute resolution services.

Similarly, a small number of trustmark schemes, including TRUSTe and Privo, have been approved by the FTC as complaints resolution bodies for the purposes of the Children's Online Privacy Protection Rule (COPPR).[91]

There has been no published analysis by either the EU or the FTC of the effectiveness of these schemes since their approval.

Although this level of Government approval is limited to specific seals (such as the TRUSTe Children's Seal), there is a risk that trustmark schemes may gain broader legitimacy for their generic privacy seals, through this association with Government.

An important development is that trustmark schemes are set to play a role in the *APEC Privacy Framework* 2005.[92] The APEC Privacy Framework is designed to provide a consistent approach to information privacy protection across APEC member economies. A major focus of the APEC work is now the development of Cross Border Privacy Rules (CBPRs).

These Cross Border Privacy Rules will be assessed by an approved accountability agent against a set of common criteria and the accountability agents will vary per jurisdiction – they could be Privacy Commissioners or trust-mark scheme operators. If an organisation's CBPRs are assessed as compliant they will be added to a public directory of compliant organisations.[93]

Under this system, a decision by an approved trustmark scheme could be considered equal to a decision by a Government regulator such as a Privacy Commissioner:

---

[90] Moores T, *Do Consumers Understand the Role of Privacy Seals in E-Commerce?* Communications of the ACM, Vol. 48, No. 4, pp. 86-91, March 2005.

[91] Children's Online Privacy Protection Rule, 64 Fed. Reg. 59888, 3 November, 1999, <http://www.ftc.gov/os/1999/10/64fr59888.htm>.

[92] More information on the Framework and Principles is available at: <http://www.apec.org/content/apec/apec_groups/committees/committee_on_trade/electronic_commerce.html>.

[93] Asia-Pacific Economic Cooperation, *The Cross-Border Privacy Rules – Implementation and Operating System*, 2006/SOM3/ECSG/DPM/009, September 2006, <http://www.rsaconference.com/uploadedFiles/2007/us/Conference_Content/ESAF/Cross_Border_Privacy_Rules_Implementation_and_Operation.pdf>.

> Under the agreed framework, a participating economy accepts the assessments made by the designated entity in another participating economy following the choice of approach to CBPRs in that economy (e.g. one economy may have a privacy commissioner it designates to make assessments and another economy may choose to use existing Trustmark bodies, but it would be agreed that a decision by either entity to include an organisation on the list would be accepted).[94]

There is a real concern that this approach in APEC may result in trustmark schemes being seen as an adequate form of privacy protection in the region, or (even worse), equivalent to privacy legislation. TRUSTe already states that it has been chosen as the US Accountability Agent for the 2008/2009 APEC Pathfinder project (similar to a pilot project).[95]

The use of trustmark schemes has not been legitimised in this way elsewhere. Indeed, the OECD recommendations on cross-border privacy enforcement exclude commercial organisations such as TRUSTe:

> 'Privacy Enforcement Authority' means any public body, as determined by each Member country, that is responsible for enforcing Laws Protecting Privacy, and that has powers to conduct investigations or pursue enforcement proceedings.[96]

There are other limitations on the potential use of trustmarks as a complement to privacy legislation at the regional level. In practice trustmark schemes are effectively restrained to domestic companies. For example, trustmark scheme information in Japan and Vietnam is largely available only in local languages. In Japan the list of trust-mark members is not available in English and the trustmark logo itself is written in Japanese characters. [97]

12. Conclusion

This article has examined the track-record of English-language trustmarks to date. Clearly this record is poor. With the demise of the BBB Online Privacy Seal there is now a strong focus on TRUSTe – the only remaining large-scale privacy trustmark.

However, the reputation of TRUSTe is low, and it is difficult to see what relevance TRUSTe now has a privacy protection tool:

> It's long been apparent to many in the privacy and security community that TRUSTe was not to be trusted, that their standards were worthless, and that their true sympathies and interests lay with the very companies they were supposed to be policing. TRUSTe was never more than a cleverly run public relations front for privacy abusive online companies. [98]

TRUSTe has already been described by one of its founding organisations (the Electronic Frontiers Foundation) as a failed experiment:

---

[94] Crompton M, *The APEC Privacy Framework - Creating Trust in developing Cross-Border Privacy Rules: A Progress Report*, 2007, <http://www.iispartners.com/apec8march.pdf>.

[95] Rotman D, Phillips J, Kurtz C, Tomaszewski, *How to Effectively Transfer Data Overseas*, 2007, <http://www.truste.org/webinars/eu_data_transfer/Website_EU_Presentation.pdf>.

[96] Organisation for Economic Cooperation and Development, *OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy*, 2007, <http://www.oecd.org/dataoecd/43/28/38770483.pdf>.

[97] <http://privacymark.org/application/new/qualification.html>

[98] Howes E., *No Guarantee of Privacy*, 2002, <http://www.spywarewarrior.com/uiuc/priv-pol.htm#no-guarantee>.

> The creation of TRUSTe and its seal program was one such early innovation of EFF. TRUSTe was successful in several areas. ... We now must move out of this awareness-raising mode and into an action mode where real protection can be achieved. Legislation is needed in order to achieve that goal. ... we think it is time to move away from a strict self-regulation approach to protecting privacy online… Our stance has basically been that industry self-regulation would be worth trying, but might or might not be enough. We did the 'proof of concept' ourselves, by launching and spinning off TRUSTe. But TRUSTe was intended to be and is a separate, independent entity, and was created as an experiment. The experiment is in many ways a failure.[99]

It is widely recognised that self-regulation has a legitimate role to play in consumer protection, but that where self-regulation fails, alternative forms of regulation, including legislation should be pursued.[100]

Like many other organisations, EFF now supports privacy legislation, and it is easy to see why. The following table compares privacy trustmarks with privacy legislation:

Issue	Trustmark	Privacy Legislation
Standards	Lowest possible standards on privacy – further lowered by broad disclaimers.	High standards and improving all the time.
Assessment	Some up-front assessment in most schemes and ongoing assessment in a minority of schemes.	Limited assessment – reliance is on complaints.
Enforcement	Poor to non existent.	Patchy, but strong examples in EU (e.g. SWIFT) and Asia-Pacific.[101]
Transience	Serious concern – many trustmarks have disappeared.	Permanent.
Timing issues	Privacy protection depends on timing membership (e.g. Gratis), time of transaction (especially for expired seals due to non payment) and even the time of complaint (e.g. Guardian).	Not time sensitive – lengthy period for complaints, based on knowledge of breach not date of transaction. All organisations covered all of the time.
Scams	Common – more fake trustmark logos in circulation than real ones. Also growing number of phishing scams.	Some limited phishing attacks but not prevalent.
Coverage	Non website privacy breaches are claimed to be outside jurisdiction – very confusing for consumers and only covers a fraction of personal data collected by companies.	Universal coverage of all personal information.
Independence	Major conflicts and perception of conflicts – source of poor reputation for long history of poor enforcement by trustmark schemes against large members.	Independent and impartial. No conflicts of interest.
Penetration	Penetration is miniscule and is falling rapidly (note demise of BBB Online Privacy which had 700 members).	Penetration is universal in jurisdictions with privacy legislation. Strong coverage now in EU and the Asia-Pacific region.
Consumer understanding	Studies show consumers believe trustmark schemes endorse the products and services on offer (not true). Also significant consumer confusion with large number of trustmarks in use.	Privacy regulators do not 'endorse' businesses so no confusion arises.

[99] Slashdot, *TRUSTe Decides Its Own Fate Today*, 8 November 1999, <http://yro.slashdot.org/article.pl?sid=99/11/05/1021214>.

[100] See for example: Braithwaite J, *Responsive Regulation for Australia*, Business regulation and Australia's future, 1993 <http://www.aic.gov.au/publications/lcj/business/chap06.html>.

[101] Connolly C, Lim YF, et al, *Privacy breach sanctions in the Asia-Pacific region*, July 2007, <http://www.galexia.com/public/research/articles/research_articles-art52.html>.

A major problem with the issues identified in this table is that some of the issues are structural – they can not be resolved by improvements in the day-to-day operation of trustmark schemes or by improved governance of trustmark schemes. Issues that are structural and cannot be resolved include transience, timing issues and scams.

Other issues, such as standards, enforcement, coverage, penetration and consumer protection, could not be resolved without significant global investment. It is unlikely that any jurisdiction would invest significant sums in trustmark schemes, rather than directing efforts towards privacy legislation.

Despite these issues, trustmark schemes do have their supporters. TRUSTe in particular is vigorous in defending itself against criticism and stresses that their role is to work with members to achieve gradual improvements. Another common form of support is to point out that 'it's better than nothing'.[102] This may be true in some cases, but there is a question mark over whether the existence of trustmark schemes has hindered or slowed the development of privacy legislation in jurisdictions such as the United States.

In December 2000 Robert Gellman stated that he could not think of a single reason to advise a consumer to make a complaint under a trustmark scheme.[103] In 2008, trustmark schemes appear even less relevant.

[102] Lawrence Öqvist K, *TRUSTe Privacy Seals*, 25 July 2007, <http://mysecuritybox.blogspot.com/2007/07/etrust-privacy-seals.html>.

[103] Gellman R, *TRUSTe fails to justify its role as privacy arbiter*, Privacy Law and Policy Reporter Volume 7 No. 6, December 2000, <http://www.austlii.edu.au/au/journals/PLPR/2000/53.html>.