Privacy White Lists - Don't be Fooled (2009)

Chris Connolly, Galexia[1]

[1] Chris Connolly is a Director of Galexia, an independent consultancy specialising in privacy and electronic commerce. <http://www.galexia.com>.

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

2 June 2009

Source

The latest version of this article is available from
http://www.galexia.com/public/research/assets/privacy_white_lists_2009/

Copyright

Contents

1. Introduction

Privacy 'white lists' are published by trustmark schemes to help identify which organisations have been certified as compliant members of their scheme. If an organisation is on the list a consumer may have an increased level of confidence that they will be covered by the rules of the trustmark scheme, including privacy protection and dispute resolution. Consumers can also use the white lists to check that the use of the trustmark is valid, as a significant proportion of trustmarks that appear on websites are often fake or expired.

There is a trend towards the global expansion of white-lists and there is a proposal to develop an APEC white-list of organisations that comply with the APEC Privacy Framework *Cross Border Privacy Rules*.[2]

This article summarises a Galexia study of white lists published by trustmark schemes. (Surprisingly, not all trustmark schemes publish white lists). The study only examined white lists where the trustmark operators claim that organisations on the lists have passed strict verification of privacy protection standards. Also, the study only examined white lists that have some form of Government backing, oversight or approval. Only six white lists are published that meet all of these criteria, and the Galexia study excluded one white list (ESRB) because it was limited to one very specific type of product (computer games).[3]

This resulted in a study of 5 white lists ranging from 9 to 340 members. Where the published white list was larger than 300 entries Galexia studied 50% of the members on the list. For all other white lists Galexia studied every entry on the list.

The study included the 'Government oversight' criteria as Galexia considers there are risks for consumers where Governments lend credibility to trustmark schemes and white lists - without adequate quality control and regulation in place.

Overall the study found that privacy white lists contained an alarming proportion of inaccurate and out of date information. Depending on the trustmark scheme administering the white-list, between 22% and 73% of information is inaccurate or out of date.

2. White Lists in the Study

2.1. Mexico – the AMIPCI Trust Mark

In Mexico a generic e-commerce trustmark is in operation that includes some privacy requirements. The trustmark is administered by AMIPCI (Mexican Internet Association) with some Government funding and support. There are approximately 278 members and information is available in Spanish and English.[4]

[2] <http://www.apec.org/apec/apec_groups/committee_on_trade/electronic_commerce.html>

[3] <http://www.esrb.org/privacy/>

[4] <http://www.sellosdeconfianza.org.mx/lisneg.php>

The AMIPCI rules state that all certified members must:

> Comply with the provisions of the guidelines or principles on privacy of APEC information, also known as Asia-Pacific Economic Cooperation (APEC).

The Galexia study made the following findings:

Issue	Test	Non-Compliance %
No working seal	A working seal does not appear on the organisation's web site	5%
Membership has expired	The membership is not current	5%
Privacy policy not available	The organisation's privacy policy is not available	17%
Overall non-compliance	Cumulative total	23%

A cumulative total for each table has been included so that organisations are only counted as non-compliant once, even though they may be non-compliant across several categories.

The Galexia study of the AMIPCI trustmark also tested whether the claim that organisations comply with the APEC Privacy Framework is valid, as this is the privacy standard required by AMIPCI. The APEC Privacy Framework contains nine high-level Principles and it is quite complex to test a privacy policy against all of them. However, *Principle 2: Notice* is relevant to website privacy policies and does contain an item that is easy to check – item (e) regarding notice of access and correction rights and processes:

> **APEC Privacy Framework Principle 2: Notice**
>
> Personal information controllers should provide clear and easily accessible statements about their practices and policies with respect to personal information that should include:
>
> …
>
> (e) the choices and mean the personal information controller offers individuals for limiting the use and disclosure of, and for accessing and correcting their personal information.

Some sites have a privacy policy, but 68 of the AMIPCI trustmark sites (30%) did not comply with the one APEC Privacy Principle that Galexia was able to check (Principle 2 Notice regarding access rights). Many of the privacy policies are only one paragraph long and it is difficult to understand how they can have been certified by AMIPCI as compliant with the APEC Privacy Framework. While the APEC standard is weak, it cannot be complied with in a one paragraph privacy policy. A more thorough examination of AMIPCI members is likely reveal an even lower level of compliance.

AMIPCI Strengths

— The AMIPCI white list is available to the public;

— Data is relatively up-to-date (although a few seals had expired, no expiry was more than three months old);

— Information is available in multiple languages;

— A deep verification link is provided wherever the seal appears; and

— Privacy standards are published (although only in the form of a link to APEC).

AMIPCI Weaknesses

— Many of the privacy policies were very short (one paragraph only); and

— AMIPCI overstates compliance with the APEC Privacy Framework.

2.2. Singapore – CommerceNet

The Singapore Government promotes a generic e-commerce trustmark known as TrustSG. It is provided by multiple organisations, the largest of which is CommerceNet Singapore. It is a generic ecommerce seal with short privacy requirements. There are approximately 340 members.[5]

TrustSG is an initiative of the National Trust Council (NTC). The council is industry led with support from the Government through the Infocomm Development Authority of Singapore (IDA).

When a consumer clicks on the trustmark a verification page appears with the following statement:

> This member has been awarded the TrustSg seal as it adheres to the Code of Practice set by CommerceNet Singapore Ltd to promote good e-business practices.

To save time, the Galexia study examined the first 168 organisations on the CommerceNet white list (50% of the total). The Galexia study did not examine the remaining smaller provider of TrustSG seals in Singapore.

The Galexia study made the following findings:

Issue	Test	Non-Compliance %
No working seal	A working seal does not appear on the organisation's web site	45%
Membership has expired	The membership is not current	14%
Privacy policy not available	The organisation's privacy policy is not available	26%
Overall non-compliance	Cumulative total	54%

It was difficult to study the CommerceNet white list as it is out-of-date. The list was visited on numerous occasions between February and April 2009 and it was clear that the expiry dates listed on the site were not being updated or maintained. At the time of completion of this article (14 April 2009) the CommerceNet white list describes ALL members as 'expired'.[6]

This is a good example of the problems consumers may have when relying upon out of date white lists. For the purposes of the study Galexia visited each site and clicked on the seal (where available). The expiry date was checked by analysing the verification page, rather than relying on the white list.

[5] <http://www.cnsg.com.sg/>

[6] <http://www.trustsg.com.sg/for_merchants/cnsg_b2c.html>

CommerceNet Strengths

— The CommerceNet white list is available to the public;

— The privacy seal is 'self-served' (served from CommerceNet's domain) and is considered current best practice;

— A deep verification link is provided wherever the seal appears; and

— The privacy standards are published.

CommerceNet Weaknesses

— The entire white list is out of date (it shows that all seals have expired);

— A very high proportion of sites were not displaying the seal at all.

2.3. Thailand

The Thailand Department of Business Development (part of the Ministry of Commerce) runs a generic ecommerce seal with one privacy provision (sites must have a privacy policy). It has around 22 members and information is available in English and Thai.[7]

The Galexia study made the following findings:

Issue	Test	Non-Compliance %
No working seal	A working seal does not appear on the organisation's web site	18%
Membership has expired	The membership is not current	36%
Privacy policy not available	The organisation's privacy policy is not available	18%
Overall non-compliance	Cumulative total	73%

Department of Business Development Strengths

— The Department of Business Development white list is available to the public;

— Information is available in multiple languages;

— A deep verification link is provided wherever the seal appears; and

— Privacy standards are published.

[7] <http://www.trustmarkthai.com>

Department of Business Development Weaknesses

— The privacy standards are very low – only requiring publication of a privacy policy; and

— A high proportion of seals had expired.

2.4. USA – Privo

Privo's Privacy Assurance Program is a specific privacy seal with particular focus on children's privacy requirements. Privo has 9 members.[8] A white list is not published, although there is a page of company logos for sites accompanied by the following text:

> Click on any of the logos below to check out our newest PrivoLock–enabled websites or Privo certified sites!

Privo was approved as a trustmark scheme for compliance with the Children's Online Privacy Protection Rule (COPPR) in 2004. Privo highlights this FTC approval on their front page and numerous other pages of their website:

> Privo is the first and only infomediary service to be recognized by the Federal Trade Commission (FTC). As an FTC designated Safe Harbor, it is our responsibility to ensure compliance with current federal and proposed state privacy laws. Privo is an FTC-approved, neutral third-party service provider.

Does the FTC approval mean that consumers can rely on sites that claim to be Privo members, or rely on the list of approved sites on the Privo website? Privo only has nine members and even with this small number there is minimal compliance and poor quality control.

The Galexia study made the following findings:

Issue	Test	Non-Compliance %
No working seal	A working seal does not appear on the organisation's web site	44%
Membership has expired	The membership is not current	44%
Privacy policy not available	The organisation's privacy policy is not available	0%
Overall non-compliance	Cumulative total	55%

In addition, Privo does not publish any information at all regarding their standards for approving a website, and they provide no information (or even contact details) regarding reporting breaches and dispute resolution.

[8] <http://www.privo.com/kids_sites.htm>

Privo Strengths

— A deep verification link is provided wherever the seal appears (although some links were broken or contained basic errors).

Privo Weaknesses

— No privacy standards are published;

— The white list is a series of company logos rather than organisation names or URLs; and

— Privo overstates the significance of their FTC approval considering the lack of information on concerning privacy standards and dispute resolution on their website.

2.5. USA – TRUSTe Children's Privacy Seal

TRUSTe offers a Children's Privacy Seal – a specific privacy seal with special children's privacy requirements. It has approximately 41 members (although this includes multiple sites belonging to a single organisation such as Disney).[9]

TRUSTe (like Privo) is approved as a trustmark scheme for compliance with the Children's Online Privacy Protection Rule (COPPR), and they highlight this Government approval on their web site:

> The Federal Trade Commission has approved TRUSTe as a COPPA Safe Harbor program. The TRUSTe Children's Seal certifies that your business is compliant with the COPPA Rule – letting parents know that their kids' information is safe.[10]

However, this Government approval does not mean that privacy protection is assured – TRUSTe has the same issues with broken and missing seals and expired members as other trustmark schemes.

The Galexia study made the following findings:

Issue	Test	Non-Compliance %
No working seal	A working seal does not appear on the organisation's web site	22%
Membership has expired	The membership is not current	n/a
Privacy policy not available	The organisation's privacy policy is not available	0%
Overall non-compliance	Cumulative total	22%

The TRUSTe white list does not publish expiry dates, so the Galexia study assumes all working seals are current.

[9] <http://www.truste.com/>

[10] <https://www.truste.org/businesses/childrens_privacy_seal.php>

The Galexia study also examined whether member sites still describe TRUSTe as non-profit, as this is an ongoing concern with TRUSTe.

On 15 July 2008 TRUSTe changed its status from non-profit to for-profit and accepted investment from Accel – part-owners and Directors of Facebook. Nearly a year after the change 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…

The Galexia study found that 29 out of the 51 sites still claim that TRUSTe is non-profit. This misleading information should be corrected.

TRUSTe Strengths

— The TRUSTe white list is available to the public;

— A deep verification link is provided wherever the seal appears;

— Privacy standards are published; and

— All sites had published privacy policies.

TRUSTe Weaknesses

— No expiry dates are published;

— A high proportion of links were broken (although sites could still be located through searches); and

— A large number of sites still incorrectly claim that TRUSTe is non-profit.

3. Summary of findings

Overall the study found that privacy white lists contained a surprising and alarmingly high proportion of inaccurate and out-of-date information. Depending on the trustmark scheme administering the white-list, between 22% and 73% of information is inaccurate or out of date. If a consumer relied on the white lists they would face the risk that they would receive no privacy protection from the trustmark scheme as the organisation's membership had expired. Similarly the enormous number of missing or broken seals means that consumers are unable to verify membership for a large number of organisations.

Compliance Issue	Mexico – AMIPCI	Singapore – CommerceNet	Thailand – DBD	USA – Privo (Children)	USA – TRUSTe (Children)
Number of organisations in the sample	278	168	22	9	41
No working seal	5%	45%	18%	44%	22%
Membership has expired	5%	14%	36%	44%	n/a%
Privacy policy not available	17%	26%	18%	0%	2%
Overall non-compliance	23%	54%	73%	55%	22%

This finding raises concerns about the use of white lists as a privacy protection mechanism and adds to more general concerns regarding privacy trustmarks and self regulation.

It is also alarming that all of the white lists examined in this article received Government approval. The two US white lists were both accredited by the Federal Trade Commission (FTC) and the other lists receive Government funding and high-level endorsement. There are risks for consumers in having Governments lend this type of credibility to trustmark schemes and white lists without adequate quality control and regulation in place.