galexia

The US Safe Harbor - Fact or Fiction? (2008)

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.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

2 December 2008

Source

The latest version of this article is available from
http://www.galexia.com/public/research/articles/research_articles-pa07.html

Copyright

Contents

1. Introduction

The US Safe Harbor is an agreement between the European Commission and the United States Department of Commerce that enables organisations to join a Safe Harbor List to demonstrate their compliance with the European Union Data Protection Directive. This allows the transfer of personal data to the US in circumstances where the transfer would otherwise not meet the European adequacy test for privacy protection.

The first public draft of the Safe Harbor Principles was released in November 1998[2], although they were not officially accepted by the EU until 2000.

The Safe Harbor is best described as an uneasy compromise between the comprehensive legislative approach adopted by European nations and the self–regulatory approach preferred by the US. The Safe Harbor Framework has been the subject of ongoing criticism, including two previous reviews (2002 and 2004). Those reviews expressed serious concerns about the effectiveness of the Safe Harbor as a privacy protection mechanism.

After ten years of public debate it is time to examine the Safe Harbor again. This article summarises the findings of a Galexia study regarding the current status of the Safe Harbor Framework. The Galexia study assessed each of the organisations listed on the Safe Harbor List (1,597 entries) against a small subset of key criteria contained in the Safe Harbor Framework Principles.

This study raises concerns that many aspects of the Safe Harbor Framework are not working. Highlights of this study include:

Compliance:

— Although the list contained 1,597 entries, only 1,109 organisations were current members of the Safe Harbor Framework. Many organisations on the list no longer exist or they have failed to renew their certification. The list also includes double entries.

— Only 348 organisations meet even the most basic requirements of the Safe Harbor Framework. Many organisations did not have a public privacy policy, or the policy failed to even mention the Safe Harbor. A large number of organisations failed to comply with Principle 7 – Enforcement and Dispute Resolution, as they did not identify an independent dispute resolution process for consumers.

— 209 organisations selected a dispute resolution provider that was not affordable. These include the American Arbitration Association (AAA) that costs between $120 and $1,200 per hour (with a four-hour minimum charge plus a $950 administration fee), and the Judicial Arbitration Mediation Service (JAMS) that costs $350 to $800 per hour (plus a $275 administration fee). Organisations either failed to disclose these costs or required the consumer to share these costs.

False and/or misleading information:

— 206 organisations claim on their public websites to be members of the Safe Harbor when they are not current members. Many of these false claims have continued for several years.

[2] <http://www.ita.doc.gov/td/ecom/aaron114.html#Safe>

— 36 of these 206 false claimants were also accredited by a third party as being current members of their Safe Harbor trustmark scheme (e.g. the TRUSTe Safe Harbor and BBB Safe Harbor programs), even though these organisations are not current members of the official Safe Harbor.

— 73 organisations claimed to be members of a Privacy Trustmark Scheme (e.g. TRUSTe or the BBB Safe Harbor program) when they are not current members of those schemes, or they claimed to be members of BBB Online Privacy – a scheme that closed 18 months ago and has not accepted any complaints since June.

— 20 organisations displayed a Department of Commerce Safe Harbor 'seal' on their website when they were not actually compliant with the Safe Harbor Framework, including numerous unauthorised seals created using graphics software.

— 24 organisations claimed that they had been certified by the Department of Commerce or certified by the EU – when the Framework is actually based on self-certification.

Overall the study found numerous problems with data accuracy and basic compliance with simple Framework requirements. This study only checked for compliance with one of the seven Safe Harbor Framework Principles (Principle 7 – Enforcement and Dispute Resolution). Galexia did not check the other six principles. Only 348 organisations passed this basic test of compliance with Principle 7.

It is unlikely that many of these 348 organisations would be considered compliant with the more detailed requirements of the other six Safe Harbor Framework Principles. For example, some organisations' privacy policies are only two sentences long.

Overall the study found that the problems identified in previous reviews of the Safe Harbor have not been rectified, and that the number of false claims made by organisations represents a significant privacy risk to consumers.

The Galexia study is part of a broader comparative study of privacy legislation and privacy self-regulation.[3]

2. Previous reviews of the Safe Harbor Framework

It is important to note that the manager of the Safe Harbor Framework – the US Department of Commerce – holds the Safe Harbor Framework in very high regard, and considers it a success. In October 2007 the Department of Commerce claimed that the 'EU view Safe Harbor as a Best Practice and Gold Standard for data protection'.[4]

There is, however, no other evidence available that the EU view the Safe Harbor as a 'gold standard' – the more common view is that the Safe Harbor is a practical compromise. The EU reviewed the Safe Harbor in 2002 and again in 2004. Both studies raised significant concerns.

[3] See also: Connolly C, *Trustmark Schemes Struggle to Protect Privacy*, 26 September 2008, <http://www.galexia.com/public/research/assets/trustmarks_struggle_20080926/> and Connolly C, *Asia-Pacific Region at the Privacy Crossroads*, 25 August 2008, World Data Protection Report, volume 8, number 9, <http://www.galexia.com/public/research/assets/asia_at_privacy_crossroads_20080825/>.

[4] Greer D, *The U.S.-E.U. Safe Harbor Framework*, presentation to the Conference on Cross-Border Data Flows, Data Protection, and Privacy, Washington DC, October 2007, <http://www.SafeHarbor.govtools.us/documents/1A_DOC_Greer.ppt>.

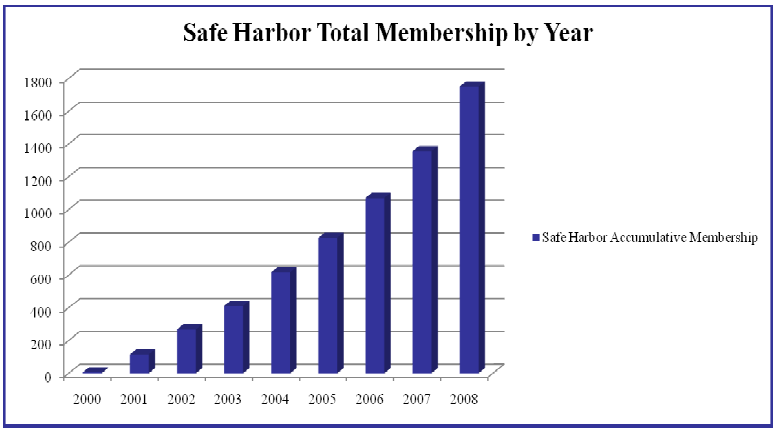
The 2002 review found that 'a substantial number of organisations that have self-certified adherence to the Safe Harbor do not seem to be observing the expected degree of transparency as regards their overall commitment or as regards the contents of their privacy policies. Transparency is a vital feature in self-regulatory systems and it is necessary that organisations improve their practices in this regard.' The 2002 review was also critical of the available dispute resolution mechanisms at that time.[5]

The 2004 review examined 10% of Safe Harbor organisations in detail, resulting in a long list of criticisms, including concerns that a number of companies failed to identify an Alternative Dispute Resolution body. They also raised concerns that 'some alternative recourse mechanisms still fail to comply with applicable Safe Harbor requirements' and 'less than half of organisations post privacy policies that reflect all seven Safe Harbor Principles'.[6]

3. Safe Harbor participants

In October 2008 the Department of Commerce claimed that 'today, nearly 1,700 U.S. organizations [have] certified to Safe Harbor'.[7] The public website for the Safe Harbor states that 'more than 1,500 U.S. companies participate in the Safe Harbor'.[8]

The Department of Commerce also publish the following chart[9] to display total membership:



[5] European Commission, *The application of Commission Decision on the adequate protection of personal data provided by the Safe Harbor Privacy Principles*, 13 February 2002, page 2, <http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/sec-2002-196/sec-2002-196_en.pdf>.

[6] European Commission, *The implementation of Commission Decision on the adequate protection of personal data provided by the Safe Harbor Privacy Principles*, 20 October 2004, <http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/sec-2004-1323_en.pdf>.

[7] Greer D, *The U.S.-E.U. Safe Harbor Framework - Past, Present, & Future*, presentation to the Workshop On International Transfers Of Personal Data, Brussels, 21 October 2008, <http://ec.europa.eu/justice_home/news/information_dossiers/personal_data_workshop/doc/Presentation_Greer.ppt>.

[8] <http://www.export.gov/SafeHarbor/Safe_Harbor_Announcement.asp>

[9] Greer D, *The U.S.-E.U. Safe Harbor Framework - Past, Present, & Future*, presentation to the Workshop On International Transfers Of Personal Data, Brussels, 21 October 2008, <http://ec.europa.eu/justice_home/news/information_dossiers/personal_data_workshop/doc/Presentation_Greer.ppt>.

Although the graph carries the label 'accumulative membership', this is not correct. Galexia downloaded the Safe Harbor list on 17 Oct 2008 and there were 1,597 records (including 19 doubles, triples and the test file).[10] However, 342 of these organisations were listed as 'not current' by the Department of Commerce. A further 136 organisations have failed to renew their certification by the required date and are listed as 'not current' in this study, bringing the total of 'not current' organisations to 478.

Allowing a generous 6 week grace period for renewals only reduces the number of 'not current' organisations by 18. This is because the vast majority of 'not current' organisations have ceased to exist, have left the Safe Harbor permanently, or have failed to renew for 6 months or longer.

Claims that the cumulative membership of the Safe Harbor are approaching 1700, or that 1500 companies 'participate' in the Safe Harbor are simply incorrect. Once doubles, triples and 'not current' organisations are removed, only 1109 organisations remain.

4. Compliant members

The study found that only 348 organisations meet even the most basic requirements of the Safe Harbor Framework. This figure was reached using the following steps:

Membership Requirement	Notes	Number of entries	Number of unique entries removed	Cumulative total
Organisation is listed.	All organisations listed on 17 October 2008.	1597	0	1597
Unique entry	Removes doubles, triples and the test file	19	19	1578
Collects EU personal information	Removes irrelevant organisations who do not collect any EU personal information	7	7	1571
Listed as current by DOC	Removes organisations listed by the Department of Commerce as 'not current'	342	329	1242
Listed as current by certification renewal date	Removes organisations that failed to renew by 17 October 2008.	477	133	1109
Website privacy policy is accessible	Removes organisations who claim to have a website privacy policy, but it is unreachable.	175	57	1052
Privacy policy mentions Safe Harbor	Removes organisations who have a public privacy policy but it does not mention the Safe Harbor at all	218	127	925
Privacy policy complies with the enforcement principle	Removes organisations who have a public privacy policy that does not provide information on the selected dispute resolution provider.	587	279	646
Affordable dispute resolution provider.	Removes organisations who have selected AAA or JAMS as their dispute resolution provider in either their certification record or their public privacy policy.	209	107	539
Verified member of TRUSTe dispute resolution.	Removes organisations who have selected TRUSTe as their dispute resolution provider when they are not current members.	29	11	528
Verified member of TRUSTe privacy program	Removes organisations who claim to be members of the TRUSTe privacy program when they are not current members	30	2	526

[10] On 17 November 2008 there were 1633 records.

Membership Requirement	Notes	Number of entries	Number of unique entries removed	Cumulative total
Verified member of the BBB Safe Harbor program	Removes organisations who claim to be members of the BBB Safe Harbor program when they are not current members.	4	3	523
Dispute resolution provider exists	Removes organisations who have selected BBB Online Privacy as their dispute resolution provider (closed in July 2008)	21	15	508
Privacy program exists	Removes organisations who claim to be members of BBB Online Privacy (closed in July 2008)	31	3	505
No website privacy policy	Removes organisations who require a password or direct contact in order to obtain their privacy policy.	246	151	354
No misleading information	Removes organisations who are using unauthorised Safe Harbor seals or who claim they have been certified by the Department of Commerce or the EU	32	6	348

The 348 organisations that are listed as compliant with these basic Safe Harbor requirements, may not in fact be complaint with all seven of the more detailed Safe Harbor Principles, as this study only assessed compliance with Principle 7.

It is also important to note that although an organisation may be listed here as compliant, it may have restricted the scope of its Safe Harbor membership to a particular category of data. For example 41 of these organisations have restricted the scope of their Safe Harbor membership to human resources data only.

Of the 348 organisations who were found to be compliant in this study, only 54 extended their Safe Harbor membership to all data. This is extremely important. Out of the 1,597 entries on the Safe Harbor list only 54 are compliant with basic Safe Harbor requirements for all categories of data – only 3% of organisations on the list.

5. Detailed Findings

5.1. False claims regarding membership

206 organisations claim to be members of the Safe Harbor when they are not current members. The oldest false claim dates back to June 2003 (i.e. the last date they were actually a member of the Safe Harbor). More than half (112) of the false claims are over twelve months old.[11] There is a significant risk that EU consumers and businesses will be mislead by these claims.

Unfortunately, membership of a third party privacy program does not necessarily lower the incidence of false claims. 26 organisations certified as TRUSTe EU Safe Harbor members are not actually on the current Safe Harbor list. The oldest of these false claims dates back to September 2005, and 11 of these false claims are more than one year old.

[11] Galexia has captured and date-stamped screenshots or files for these 206 false claims.

In most jurisdictions an organisation would face serious consequences for making a false claim of this nature, and even a single breach by a single company would result in regulatory action. In the US there is no indication that this issue has been the subject of any action by authorities, despite the hundreds of false claims over a lengthy period.

5.2. False claims regarding certification

The Safe Harbor is a self-certification scheme, and most organisations reflect this in the text of their privacy policies. However, great care needs to be taken regarding claims that US organisations have been 'certified by the Department of Commerce' or even 'certified by the EU'. There are also some references to the 'Safe Harbor Act' that may mislead consumers, as the Safe Harbor is not a legislative regime.

This study identified a large number of organisation making false claims, using the following words (or similar):

Claim	Location
In the case of the USA, the Safe Harbor Act protects EU citizens and allows transfer of personal data so long as the recipient (Company X) is a certified signatory to the Act.	Company privacy policy
Company X Awarded EU Safe Harbor Certification to Become the First Certified U.S.-based Email Provider.	Company blog
Collection and transfer of this data between Company X Worldwide and its regional offices and/or member firms is allowed through explicit consent as a member and through adherence of Company X Worldwide regional offices to the Safe Harbor Act in Europe.	Company privacy policy
Company X announced today that it has been certified by the U.S. Department of Commerce as compliant with the United States-European Union (EU) Safe Harbor Framework.	Company press release
Company X is certified by the Department of Commerce. We have implemented the Safe Harbor principles and comply with all Safe Harbor principles. Visit http://www.export.gov/SafeHarbor and chose Safe Harbor list to review our certification.	Company privacy policy
Company X today announced that it has received Safe Harbor Certification from the U.S. Department of Commerce…'Receiving our Safe Harbor Certification from the Commerce Department will enhance our capabilities to better serve our European clients'.	Company press release
Company X Joins European Privacy Safe Harbor - Under Safe Harbor, US companies are certified by the EU as providing acceptable privacy protection as defined by the European Commission.	Company press release
We have obtained certification of our compliance with the U.S. Department of Commerce's Safe Harbor program for United States businesses – the so-called EU Safe Harbor.	Company privacy policy
Company X Receives Safe Harbor Certification - US Department of Commerce Certifies Company X 's Data Security - Company X has formalized and documented its data privacy procedures and obtained Safe Harbor Certification from the U.S. Department of Commerce.	Company press release
This Policy is registered and certified with the U.S. Department of Commerce Safe Harbor program.	Company privacy policy
Company X joins a distinguished group of global firms that have met the strict European standard for data privacy protection. The U.S. Department of Commerce and the European Safe Harbor Commission have recently awarded Company X its Safe Harbor certification	Company press release

5.3. The Safe Harbor Certification Mark

The Department of Commerce recently issued a 'Safe Harbor Certification Mark' that can be used by organisations as a 'visual manifestation of the commitment your organization makes when it self-certifies that it will comply with the U.S.-EU Safe Harbor Framework'.[12]

This is a dangerous development and is already resulting in misleading information for consumers. 26 organisations currently display the Certification Mark, but only 13 of these organisations are compliant with the basic Safe Harbor requirements.

The Certification Mark may imply that the site has been endorsed by the Department of Commerce, when the Safe Harbor is merely a self-certification scheme. The Certification Mark is supposed to be preceded by the words 'we self-certify compliance with', although these words do not appear in the graphic itself. One organisation is already using the graphic without the 'self certify' words.

The Certification Mark implies that all information provided to the site will be protected by the Safe Harbor. There is only one logo – rather than separate logos for human resources data, online data, offline data etc. Most organisations restrict the scope of their Safe Harbor membership to 1-2 categories of data.

There is also widespread evidence that organisations have simply made up their own Safe Harbor seals and added them to websites, surveys, emails etc. Consider the following examples:

Organisation	Notes	Logo
Surveygizmo	This site states: 'At the request of customers, here are graphic 'badges' you can place in your survey, email or web page to showcase your compliance.' They are not actually members of the Safe Harbor.	
Delphi Corporation	Their Safe Harbor Policy contains a large Department of Commerce logo without explanation.	
Background Profiles	Their Privacy Notice has an unauthorised Department of Commerce Safe Harbor logo.	
Mind Your Business Inc	This unauthorised Department of Commerce logo is prominently displayed on their home page.	
Acton Inc	This unauthorised Department of Commerce logo appears on their home page next to the words 'Safe Harbor'.	

[12] <http://www.export.gov/SafeHarbor/Safe_Harbor_Instructions.asp>

Organisation	Notes	Logo
Saturn Inc	This Department of Commerce logo appears on their Privacy Policy next to the word 'Associations'. Their entire privacy policy is two lines long.	

In most jurisdictions there are serious repercussions if a company uses a Government coat of arms or logo on their website in a way that implies Government endorsement of the company. There is no indication of such concern in the United States and the Galexia study found that there are actually more unauthorised / misleading seals in use than there are authorised / accurate seals.

5.4. Availability of privacy policies

The entire legal basis of the Safe Harbor relies on a privacy policy being available, so that a comparison can be made between privacy promises and privacy practices. If there is a difference between the promise and the practice, the Federal Trade Commission will have jurisdiction to act using their general consumer protection powers. If no privacy policy is available, the organisations will not be compliant with the US Safe Harbor and there may be no legal basis for enforcement action:

> The FTC has powers to pursue companies which make false or misleading statements in their privacy policies, but it is doubtful whether it would have jurisdiction over those that fail to actually publish the required statements. In those cases … it would be very hard for any kind of enforcement action to proceed in the United States.[13]

The 2004 EU review of the Safe Harbor stressed the importance of privacy policies being available for public review:

> Lack of a public self-statement in itself means that Safe Harbor participants are falling short of what the decision requires. To comply with the Safe Harbor, a company must be subject to enforcement actions by the FTC. The FTC's authority to enforce the Principles upon a given organisation is triggered by such an organisation's public commitment to comply with the Principles. Without such a public commitment, the FTC would not have the authority to enforce the Principles. This basically puts the company that lacks a publicly available privacy policy that fully embraces the Principles in non-compliance.[14]

The Galexia study found that many organisations do not make their privacy policies available. The following table summarises the availability of privacy policies:

Availability	Number of Organisations
Not Available – Contact Required Requires contact with the organisation, often an email address is supplied or the location requires a password.	246

[13] Pedersen A, *US Safe Harbor under fire*, Privacy Law and Business Reporter, issue 75, October 2004, page 10, <http://www.hunton.com/files/tbl_s47Details/FileUpload265/912/Safe_Harbor_Sotto_11.04.pdf>.

[14] EU 2004 review, page 6.

Availability	Number of Organisations
Not Available – Absent The website does not have a privacy policy or access to the privacy policy is permanently broken. In this study access was attempted using both Internet Explorer and Mozilla Firefox. Searches included home pages, contact sections, 'about us', FAQs etc.	175
Available – Findable using search The Department of Commerce self-certification entry was incorrect, but the privacy policy could be found using simple site searches.	208
Available – Accurate link provided Accurately linked or clearly on the home page (includes correcting basic typos).	966

5.5. Content of privacy policies

The quality of the content of privacy policies varies significantly. Major issues identified in this study include:

— Numerous privacy policies are only 1-3 sentences long and contain virtually no information for consumers. The shortest EU Safe Harbor privacy policy simply stated: 'Company X maintains privacy measures that exceed Safe Harbor requirements'.

— Numerous privacy policies simply refer the consumer to the Department of Commerce Safe Harbor website for further details.

— Numerous privacy policies appear to conform to a common 'template' privacy policy that is not complaint with the Safe Harbor Framework. This template has a heading called 'enforcement' or 'dispute resolution' and then has text telling the consumer that if their complaint cannot be resolved with the organisation, they should 'contact your local Data Protection Authority for further information'. There is no other information on independent dispute resolution, and no discussion of the Panel. This template accounts for a significant number of non-compliant sites.

— Numerous privacy policies claim that the organisation is complaint with the Safe Harbor without providing any explanation about what the Safe Harbor is. One example just says 'Customers from the European Union should note that we are in compliance with the Safe Harbor privacy principles.' No further details are provided.

5.6. Participation in privacy programs

The self-certification form asks organisations to 'List any privacy programs in which your organization is a member for Safe Harbor purposes'. This is followed by a box where free text can be entered.

The exact purpose of this part of the self-certification is not clear. There is no requirement to join a privacy program. However, if text is entered here then it is important that the information is accurate. Care needs to be taken not to raise expectations that the 'privacy programs' play any formal role in the Safe Harbor arrangements (there is another box later in the form covering dispute resolution providers – who do play a formal role in the Safe Harbor).

Common entries in this section are TRUSTe (176), BBB (93) and DMA (67).

A range of additional organisations are listed as 'privacy programs in which your organization is a member for Safe Harbor purposes'. However, none of these appear to be programs that cover privacy issues relevant to the Safe Harbor. Some entries are irrelevant or difficult to explain. Many entries appear to confuse privacy compliance with security compliance – and these entries generally indicate a lack of understanding about the Safe Harbor program. Entries include:

Privacy Program	Comments
American Arbitration Association	No relevant privacy program
American Society for Industrial Security (ASIS)	No relevant privacy program
Center for Internet Security	No relevant privacy program
Comodo	Comodo is a firewall provider
European Privacy Officers Network	No relevant privacy program
Gramm-Leach-Bliley Act (GLBA)	GLBA is federal legislation
HIPAA	HIPAA is federal legislation
International Association of Privacy Professionals	No relevant privacy program
International Security Forum	No relevant privacy program
ISO 9001	Not relevant
Privacy Alliance	Inactive
Statement on Auditing Standards No. 70: Service Organizations (SAS 70)	Not relevant
Tulsa Metro Chamber of Commerce	No relevant privacy program.
US Council for International Business (USCIB)	No relevant privacy program
Equifax	?

5.7. Dispute resolution providers

One of the most important compliance requirements in the Safe Harbor is Principle 7 – Enforcement and Dispute Resolution. This requires organisations to select an independent dispute resolution provider – usually indicated in the self-certification entry and/or the public privacy policy.

Compliance with this requirement is confusing, as many organisations select multiple dispute resolution providers or indicate the 'brand' of dispute resolution (e.g. BBB) without clearly indicating which specific BBB program they have selected. There is also enormous inconsistency between the dispute resolution provider selected in the self-certification form, and the provider mentioned in the website privacy policy.

The following table is therefore a very rough summary of the dispute resolution providers selected by organisations:

Dispute Resolution Provider	Number of Organisations	Compliance	Notes
Entry is blank	9	Non compliant	
Entry provides an email address only	2	Non compliant	
AAA	184	Non compliant	The American Arbitration Association (AAA) costs between $120 and $1,200 per hour (with a four-hour minimum charge plus a $950 administration fee).

Dispute Resolution Provider	Number of Organisations	Compliance	Notes
BBB	106	Confusing	The BBB Safe Harbor program is compliant, but it is often unclear whether an organisation is indicating that it is a member of another BBB program (eg the Reliability program), a former BBB program (e.g. the closed Online Privacy program), or whether they just mean a consumer can take their complaint to a generic BBB office.
BBB EU	37	Compliant	This number is likely to be higher as some organisations that have stated 'BBB' will actually belong to the BBB EU program.
BBB Online Privacy	32	Not compliant	This program is closed. This number is likely to be slightly higher as many organisations that have stated 'BBB' will actually belong to the BBB Online Privacy program.
DMA	112	Compliant	
EU DPA Panel	870	Compliant	
JAMS	25	Non compliant	The Judicial Arbitration Mediation Service (JAMS) costs $350 to $800 per hour (plus a $275 administration fee).
TRUSTe (generic)	61	Confusing	The generic TRUSTe program cannot receive complaints regarding offline data, and may therefore not be suitable in all circumstances. This number is likely to be lower as some organisations have only entered 'TRUSTe' on the form without indicating the specific TRUSTe scheme they belong to.
TRUSTe Safe Harbor	110	Compliant	This number is likely to be higher as some organisations have only entered 'TRUSTe' on the form without indicating the specific TRUSTe scheme they belong to.

The key requirements for dispute resolution providers are that they are independent, affordable and they can provide an appropriate range of sanctions.

This study did not include a detailed examination of the independence of the selected dispute resolution providers. However a problem regarding independence was noted in passing. Nearly all members of the TRUSTe program state in their privacy policies that 'TRUSTe is a worldwide, independent, non-profit organization'. This common wording is in fact incorrect and misleading. TRUSTe abandoned its non-profit status in July 2008 and is now a for-profit company. Its major shareholders are venture capital firm Accel – also substantial investors in Facebook. References to TRUSTe being non-profit should be removed immediately. Even the Facebook privacy policy states that TRUSTe is an 'independent, non-profit organization' – many months after the change in status.

Affordability is also a major issue. The Safe Harbor FAQ 11: states that 'the recourse available to individuals must be readily available and affordable'. In all European jurisdictions access to an independent dispute resolution service regarding privacy is free.

Two key Safe Harbor dispute resolution services (selected by 209 Safe Harbor members) are too expensive for ordinary consumers to utilise:

— **The American Arbitration Association (AAA)**
An arbitrator with the AAA charges between $120 and $1,200 per hour (with a four-hour minimum charge). There is also a minimum $925 administration fee for international disputes, that rises depending on the amount of money in dispute. Many privacy complaints will not include a claim for money – in these cases AAA charges a $4,500 administration fee for 'non-monetary amounts'.[15] These fees do not include additional costs such as the hire of a hearing room or telephone conference.

[15] <http://www.adr.org/si.asp?id=5385>

— **The Judicial Arbitration Mediation Service (JAMS)**
JAMS costs $350 to $800 per hour (plus a $275 administration fee). It is also a significant challenge to find detailed fee information regarding JAMS – there is virtually no disclosure of detailed costs on the JAMS website and their panel of neutrals do not publish a fee schedule.

No Safe Harbor member in this study revealed the extent of these costs to consumers in their privacy policy. Some organisations include a clause in their privacy policy requiring the consumer to share these costs.

5.8. Co-operation with the EU DPA Panel

The Safe Harbor enforcement principle requires organisations to identify an independent dispute resolution provider. However, it allows organisations to select an alternative approach – they may agree to cooperate with the dispute resolution Panel established by the EU Data Protection Authorities. Indeed, this approach is required for all human resources data.

Evidence of this 'agreement to cooperate' is essential, as the 2002 and 2004 EU reviews both found that it was necessary for a US organisation to agree to cooperate in order for the EU DPA Panel to gain jurisdiction. It was not sufficient to merely indicate the existence of the Panel or to refer consumers with disputes to individual EU Data Protection Authorities.

The agreement to cooperate with the EU DPA Panel may appear in either the self-certification entry or in the privacy policy. As usual there are considerable problems with data quality regarding this requirement. This includes inconsistency between the entry in the form, and entries on privacy policies. Also, 208 organisations failed to click on a selection in this part of the form, so their entry reads 'select appropriate response' – it is therefore unclear whether these organisations are bound.

Also, most privacy policies do not accurately convey information about the Panel to consumers. There is often no mention at all of the existence of the Panel. Where EU Data Protection Authorities are mentioned at all, the situation is often misdescribed in terms similar to the following:

> If you cannot resolve the issue directly with the Company X Safe Harbor Privacy Contact, you may contact your local data protection authority for further information.[16]

Without a clear indication to consumers that the EU DPA Panel exists as an independent dispute resolution service AND a clear commitment to cooperate with the Panel, organisations are not compliant with the Safe Harbor.

In addition, some privacy policies contain references that would make no sense to a consumer, such as:

> For human resources data we have agreed to cooperate with Data Protection Authorities.

In this example (and similar sites) there is no information about who or where these data protection Authorities are, and what their role is in the case of a dispute.

Overall, the Galexia study found that there was a very low level of compliance with the requirement to identify the EU DPA Panel correctly as the appropriate dispute resolution provider. Only four organisations in the entire study provided contact details for the Panel.

[16] <http://www.rrdonnelley.com/wwwRRD1/PrivacyPolicy.asp>

5.9. Categories of data protected

It is important to note that even if an organisation is compliant with the basic Safe Harbor requirements, they may have limited the scope of their Safe Harbor membership to specific categories of data. This limitation may or may not appear in their published privacy policy, but it is usually recorded in their self-certification entry.

Of the 348 organisations who were found to be compliant in this study, only 54 extended their Safe Harbor membership to all data. Out of the 1,597 entries on the Safe Harbor list only 54 are compliant with basic Safe Harbor requirements for *all* categories of data.

The following table summarises the categories of data selected by the 348 compliant organisations:

Category of Data	Selected	Unique Selection[17]
Human Resources	152	41
Online	294	75
Offline	181	4
Manual	134	2
Other	6	6

6. Recommendations

This study has found that there has been little improvement in either compliance or data quality since the negative 2002 and 2004 EU reviews of the Safe Harbor. Indeed, the growing number of false claims made by organisations regarding the Safe Harbor represent a new and significant privacy risk to consumers.

If the Safe Harbor is to operate effectively, an immediate program of improvements is required.

6.1. Recommendations for the EU

The EU is a significant stakeholder in the operation of the Safe Harbor – it is the personal information of European citizens that is ultimately at risk. The EU should take a more 'hands-on' approach to ensuring that the Safe Harbor is providing basic privacy protection:

— The EU should consider re-negotiating the Safe Harbor arrangement so that all member privacy policies are made available on a public website, or posted on the Department of Commerce website, as a minimum entry requirement to the Safe Harbor;

— The EU should consider re-negotiating the Safe Harbor arrangement so that Safe Harbor members are required to select dispute resolution providers that are affordable for ordinary consumers;

[17] 'Unique selection' indicates organisations who *only* selected this category of data.

— The EU should consider providing warnings to EU consumers and businesses regarding public claims that an organisation is a member of the Safe Harbor. EU consumers and businesses will need to check the actual membership in order to avoid false claims (currently 206 organisations). This warning will need to instruct EU consumers and businesses to check the certification dates, as the Department of Commerce record of currency is not accurate; and

— The EU should consider undertaking a comprehensive review of all entries on the Safe Harbor list. This could include collecting each privacy policy and assessing it against all seven EU Safe Harbor principles.

6.2. Recommendations for the US

The US should consider taking steps to rectify some of the more pressing Safe Harbor problems identified in this study:

— The Federal Trade Commission and/or the Department of Commerce should consider investigating the hundreds of organisations who make false claims in relation to their membership of the Safe Harbor and/or their membership of dispute resolution providers;

— The Federal Trade Commission and/or the Department of Commerce should consider investigating organisations who claim that they have been certified by the Department of Commerce or certified by the EU, or who otherwise misdescribe the self-certification process;

— The Department of Commerce should consider revising its public statements about the number of organisations who are 'participants' in the Safe Harbor at any given date, in order to exclude non-current members, duplicate entries etc.;

— The Department of Commerce should consider investigating the unauthorised and/or misleading use of its Departmental logo in the privacy policies and websites of organisations;

— The Department of Commerce should consider abandoning the use of the Safe Harbor Certification Mark, as it is open to abuse and in the majority of cases it is misleading. Alternatively, the Certification Mark should use the words 'self certified' within the graphic, and the graphic should accurately indicate the categories of data covered by that specific organisation's membership;

— Some Safe Harbor dispute resolution providers (notably DMA) should publish public lists of their members so that membership can be validated by the public (most providers already comply with this requirement);

— All Safe Harbor dispute resolution providers (e.g. TRUSTe, BBB and DMA) should develop a process that automatically suspends an organisation's membership if they fail to renew their Safe Harbor certification; and

— TRUSTe should require all of its members to immediately cease referring to TRUSTe as 'non-profit'.

Until the Safe Harbor is reviewed and improved, consumers and business should approach all claims made regarding the Safe Harbor with great care, and undertake their own investigations before providing any personal information to US organisations.

The ability of the US to protect privacy through self-regulation, backed by claimed regulator oversight is questionable. There are growing calls, including campaigns by leading business groups, for the US to abandon the self-regulation approach and embrace comprehensive privacy legislation. Comprehensive privacy legislation ensures that personal information is protected by privacy rights for all organisations, all of the time. Where legislation is in place an individual's privacy rights do not disappear because an organisation has forgotten to renew their membership of a dispute resolution service, or because a dispute resolution service closes its doors.

The International Monetary Fund (IMF) publishes a list of advanced economies – those economies that have advanced markets, high wealth and do not rely on a single resource such as oil. Of the 31 countries that appear on that list only Singapore and the US do not have privacy legislation. It may be time for the US to abandon one list and join the other.

7. Appendix – Methodology for this study

The study methodology is summarised in the following table:

Step	Task	Notes
1	Capture raw data	All 1,597 entries were downloaded on 17 October 2008.
2	Check for doubles	19 organisations were listed more than once or appeared in the list under multiple names.
3	Check currency	Organisations were categorised as not current if their status in the list had been marked as not current by the Department of Commerce and/or their date for renewal of certification had passed.
4	Find privacy policies	Privacy policies were accessed using the direct links provided in the list and / or the home URL of the organisation. This step required numerous additional steps to correct typos, search websites etc.
5	Check privacy policies for mention of the Safe Harbor	Privacy policies were searched for 'Safe Harbor', 'Europe' and variations of these terms.
6	Check privacy policies for compliance with Principle 7 – Enforcement	Privacy policies were searched for 'dispute', 'complaint', 'panel' and variations of these terms. The relevant sections of the policy were then assessed against the requirements of Principle 7.
7	Check website for seals and trustmarks	Websites were checked for relevant seals and trustmarks, including both authorised and unauthorised Department of Commerce seals, and private sector trustmarks such as TRUSTe, BBB and DMA.
8	Check validity of trustmarks	Where possible the validity of trustmarks was cross checked against lists maintained by private sector trustmark providers (only TRUSTe and BBB Safe Harbor maintain public lists).
9	Quality control	The study re-checked the 'not current' status of organisations. As the study took 4 weeks to complete a small number of entries were updated as organisations had renewed their certification.