EU/US Safe Harbor – Effectiveness of the Framework in relation to National Security Surveillance

Chris Connolly

Galexia

Speaking / background notes for an appearance before the Committee on Civil Liberties, Justice and Home Affairs (the LIBE Committee) inquiry on "Electronic mass surveillance of EU citizens", Strasbourg, October 7 2013

LIBE Committee:
http://www.europarl.europa.eu/committees/en/libe/home.html

Galexia:
http://www.galexia.com

SPEAKING NOTES

Introduction

The Safe Harbor framework 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 Safe Harbor framework is a compromise agreement between two very different approaches to data protection, and as a result it has many limitations.

In November 2008 Galexia conducted a study of the US Safe Harbor[1]. The study identified widespread problems with the level of privacy protection being provided.

The Galexia study was briefly updated in 2010[2].

This research (in part) led to the Federal Trade Commission taking some minor action against six organisations who made false claims in relation to Safe Harbor membership in 2009.[3]

The FTC has subsequently included Safe Harbor related concerns (briefly) in its enforcement action against MySpace, Google and Facebook.[4]

Galexia's research has helped to provide a factual basis for discussions regarding the effectiveness of the Safe Harbor, and some improvements have been seen in both compliance and enforcement in the period since Galexia's first report. However, the overall level of Safe Harbor non-compliance and false claims remains high. Galexia continues to play a role in advocating for improvements to Safe Harbor compliance, including ongoing research and reporting.

In 2013, the focus has turned to whether the Safe Harbor is an effective mechanism for protecting privacy in the light of revelations about the mass surveillance of both US and non-US citizens by the NSA and other intelligence organisations.

---

[1] Connolly C, *The US Safe Harbor - Fact or Fiction?*, Galexia, December 2008, http://www.galexia.com/public/research/articles/research_articles-pa08.html

[2] Connolly C, *The Future of the EU/US Safe Harbor Privacy Framework: Can it be improved or does it require a complete overhaul?*, Galexia (presentation to Privacy Laws and Business Conference, Cambridge, July 2010) http://www.privacylaws.com/About_Us/Media-Centre/Annual-Conference-2010-Videos/

[3] Collectify (2009) http://www.ftc.gov/os/caselist/0923142/index.shtm ;
Progressive Gaitways (2009) http://www.ftc.gov/os/caselist/0923141/index.shtm ;
Directors Desk (2009) http://www.ftc.gov/os/caselist/0923140/index.shtm ;
Onyx Graphics (2009) http://www.ftc.gov/os/caselist/0923139/index.shtm ;
ExpatEdge Partners (2009) http://www.ftc.gov/os/caselist/0923138/index.shtm ; and
World Innovators (2009) http://www.ftc.gov/os/caselist/0923137/index.shtm

[4] Facebook (2011): http://www.ftc.gov/os/caselist/0923184/index.shtm ;
Google (2011): http://www.ftc.gov/os/caselist/1023136/index.shtm ; and
MySpace (2012): http://www.ftc.gov/os/caselist/1023058/index.shtm

Current Practice

Some areas of Safe Harbor compliance have improved since the Galexia reports in 2008 and 2010:

The proportion of Safe Harbor members that offer a public privacy policy is now over 90%. The proportion of Safe Harbor members that include basic information about the Safe Harbor and/or a link to the Safe Harbor website is now over 80%. The Department of Commerce's Safe Harbor List (the database of all current and non-current Safe Harbor members) is now also easier to search, browse and download.

However, a range of conduct that is potentially damaging to consumers in relation to the Safe Harbor persists. As time is limited, this presentation will focus on a few key areas.

1. The Safe Harbor framework is a small, limited scheme

The high profile of the Safe Harbor may lead people to believe that it is a large, significant scheme providing widespread privacy protection. It is useful to remind stakeholders from time to time of the limitations of the scheme.

It cannot cover financial services, telecommunications, energy, transport or the media.

It is a voluntary scheme with less than 3,000 current participants. Many popular services used by European consumers have simply not joined the Safe Harbor (such as Instagram, Pinterest, Tripadvisor and Wikipedia).

Interestingly, the Safe Harbor does not even cover many of the services targeted by National Security surveillance (such as airlines, banks, credit card companies and telecommunications providers).

Even within the scheme, Safe Harbor members may limit their coverage to specific data, such as "online or offline data", or "consumer or employee data", or any combination of these exclusions. Further limitations and exclusions are imposed in many individual privacy policies, so that software downloads and 'apps' are typically excluded from Safe Harbor coverage.

2. Safe Harbor protection is transient

European stakeholders may be used to the stability of *all* organisations being covered by local data protection law, for *all* of their activities, *all* of the time. The Safe Harbor is very different.

Safe Harbor protection is only provided while the organisation is a member, and is only enforceable while they are making a promise of protection (usually in their privacy policy). Membership status changes constantly in the Safe Harbor, and privacy policies are also the subject of constant revision and updates.

More than 1,000 organisations have left the Safe Harbor permanently. Other organisations have left for short periods and then returned. (There is no accurate list or archive of historic membership, and indeed many former list entries have simply disappeared). Organisations also constantly change their trustmark or dispute resolution providers.

Consumers who may have provided personal information during a period when an organisation was a Safe Harbor member, may be unaware that the organisation has now left.

3. Many claims of Safe Harbor membership are false

Many organisations still make false claims in relation to Safe Harbor membership. There is a significant risk that EU consumers will be misled by these claims. This is the most serious category of complaint and requires little explanation in 2013.

False claims have been the subject of some limited enforcement action by the FTC, but this appears to have had little impact on the overall level of false claims. In 2008 Galexia found that 208 organisations were making false claims of Safe Harbor membership. In the 2010 update the figure was 331. Today, it is 427 (September 2013).

Providing the list of false claims to the Department of Commerce and/or the Federal Trade Commission appears to have had little impact on the overall level of compliance.

The organisations who make false claims of Safe Harbor membership include large, high profile, household name organisations with hundreds of millions of customers. They include organisations who appear regularly in the top 100 sites (measured in terms of web traffic) in Europe.

Consumers and privacy advocates have complained about these false claims for many years without success. Some businesses who are legitimate Safe Harbor members are now also starting to complain about the high proportion of false claims. Perhaps they will have more luck.

4. The Safe Harbor relies heavily on trustmarks and seals, which have failed to deliver promised benefits

Many organisations claim to be members of trustmark schemes when they are not in fact members of those schemes. These claims can be checked for some schemes (such as TRUSTe and BBB) but cannot be checked for other schemes (such as DMA). These false claims are now very common, and deceive EU consumers about the level of oversight or dispute resolution that exists when their data is transferred to the US.

In addition to false claims by the organisations themselves, there are very high levels of false claims by third parties. This typically occurs where a trustmark scheme claims that organisation X is a member of the Safe Harbor in their public lists (where these are available). However, the organisation is not listed by the Department of Commerce or is listed as 'not current'. The trustmark schemes have a responsibility to ensure these claims are accurate and up to date.

More than 25% of the organisations who are currently making a false claim of Safe Harbor membership have a link with a trustmark scheme.

In addition, over 10% of the organisations who are currently making a false claim of Safe Harbor membership display the Department of Commerce's own Safe Harbor Trustmark (or the Department's logo). Even if the claims were true, these logos mislead consumers about the level of Government endorsement in what is essentially a self-certification scheme.

This heavy reliance on visual aids and third party endorsements has delivered more problems than benefits for the Safe Harbor.

5. Many organisations fail to provide information to consumers regarding dispute resolution

Many organisations do not provide the name (or the contact details) of their dispute resolution provider. This important information is essential if Principle 7 – Enforcement is to be meaningful.

This is the most common source of non-compliance with the Safe Harbor principles, as more than 30% of organisations fail to provide these details.

Unfortunately, the Federal Trade Commission, in its 2009 decision in relation to Directors Desk[5], failed to take any action on this obvious breach. (Directors Desk did not disclose who their dispute resolution provider was, and in fact it was the American Arbitration Association, which was charging $4,000 just to file a privacy complaint at the time of the case).

This set a poor precedent for compliance with Principle 7 – Enforcement. The case is probably the low-point in the history of Safe Harbor oversight. It is difficult to see how this situation can be repaired without significant intervention.

6. Many of the selected dispute resolution providers are inaccessible to ordinary consumers

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.

Affordability here is 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 are too expensive for ordinary consumers to utilise:

The American Arbitration Association (AAA), selected by 461 current members

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 disputes'. These fees do not include additional costs such as the hire of a hearing room or telephone conference. If a consumer contacts the AAA with a Safe Harbor inquiry they will be referred to these cost schedules.

The Judicial Arbitration Mediation Service (JAMS), selected by 153 current members

JAMS costs $350 to $800 per hour (plus a $1,000 filing fee for international disputes). It is also a significant challenge to find detailed fee information regarding JAMS.

Unsurprisingly, consumers do not utilise these services. No Safe Harbor members reveal the extent of these costs to consumers in their privacy policy. Some organisations include a clause in their privacy policy requiring the consumer to pay or share these costs, but most are simply silent on the issue.

[5] Directors Desk (2009) http://www.ftc.gov/os/caselist/0923140/index.shtm

Again, it is difficult to see how this situation can be repaired without significant intervention. European stakeholders may need to take a role in the selection of appropriate dispute resolution providers.

7. Some important software downloads are excluded from Safe Harbor dispute resolution

When organisations use some trustmark schemes as their dispute resolution provider for the Safe Harbor, the terms often exclude any personal information collected via "downloaded software" from coverage, leaving a significant gap in Safe Harbor protection.

These organisations still claim that they are complying with the Safe Harbor, even when their main business activity appears to be specifically excluded from Safe Harbor dispute resolution.

8. Stakeholders have unrealistic expectations about FTC Enforcement

The potential role of the FTC in enforcing the Safe Harbor is always given significant prominence in any discussion of the framework. The potential role of the FTC is also emphasised in individual privacy policies.

These statements risk raising expectations about what the FTC is likely to do in the case of a Safe Harbor related dispute.

European stakeholders may be used to working with local data protection commissioners and other regulators, who provide an accessible complaints path for consumers. However, if a consumer complains to the FTC their experience will be very different. They may not receive any acknowledgment, information about the process or timeline, or even contact details for the person managing the complaint. There is no obligation for the FTC to provide any information on how (or if) it addresses the complaint, and no reasons need to be provided for the final decision (if any).

Previous FTC action in relation to false claims of Safe Harbor membership has not resulted in improved compliance or better protection for consumers. This is because prior FTC action in relation to false claims was very limited (only 6 cases instead of hundreds), the companies selected for action were small (when large, high profile companies are engaged in false claims), none of the companies selected was a member of a trustmark program (when trustmark programs themselves make numerous false claims of Safe Harbor membership), and no actual sanctions were imposed.

Expectations of FTC oversight or enforcement need to be realistic.

Relevance to National Security surveillance

In summary, the Safe Harbor is a small, limited, transient framework for protecting some categories of data transferred to the US. Its exact relationship to National Security surveillance is uncertain.

The next section examines some potential Safe Harbor issues in relation to National Security surveillance.

Coverage

The Safe Harbor does not (and cannot) cover major categories of data that appear to be the subject of surveillance, including financial records, travel records, and significant portions of voice and data traffic carried by US telecommunications providers.

As a voluntary, transient scheme, the Safe Harbor only covers a small number of organisations at any one time.

However, the level of Safe Harbor membership (and compliance) amongst cloud service providers is quite high. Cloud service providers typically have multiple layers of privacy protection, often combing direct contracts with clients with an over-arching privacy policy. With one or two important exceptions, cloud service providers in the Safe Harbor are compliant with the key provisions relating to dispute resolution and enforcement. There are no major cloud service providers in the list of false membership claims at this time.

The "national security" limitation

The Safe Harbor agreement *allows* (but does not require) a specific limitation to be included in relation to "national security". No further detail or guidelines have ever been published in relation to this limitation. About 1-2% of Safe Harbor members have included the "national security" limitation in their public privacy policies. Most are silent on the issue.

The general impression provided to consumers by Safe Harbor privacy policies is that disclosures will only be made to Government agencies in limited circumstances, and in response to a specific, lawful request. Even where the "national security" limitation has been mentioned in privacy policies, no further details have been provided, and (unsurprisingly) there has been no indication to consumers of any form of mass surveillance or disclosure.

Dispute Resolution

One obvious weakness in the Safe Harbor framework is that the dispute resolution providers who have been self-selected by members are completely inappropriate to deal with a dispute relating to national security. Private mediation services such as the AAA, JAMS and TRUSTe have no prospect of resolving a dispute relating to national security. Consumers are unlikely to want to take such a dispute to the Direct Marketing Association or the Better Business Bureau.

However, at the moment, the consumer must use whatever dispute resolution provider has been selected by the Safe Harbor member, no matter how inappropriate.

This will need to be addressed by a change to the framework. A revised Safe Harbor could require all disputes relating to national security disclosures to be resolved by the European DPAs. There is a precedent for this in relation to employee data, where jurisdiction for all human resources disputes in the Safe Harbor has been given to the European DPAs, even where an organisation has selected another dispute resolution provider for consumer disputes.

Overall levels of compliance

It would be dangerous to rely on the Safe Harbor to manage *any* aspect of the specific national security issue without first addressing the broader issues of false claims and non-compliance.

At the moment, for every seven public claims of Safe Harbor membership, one is a lie. That is an unacceptable level, and it has persisted at that level for many years. What can be done to remove existing false claims and prevent new ones from appearing?

The high level of false claims in relation to trustmarks also needs to be resolved. The prominent role of trustmarks in the Safe Harbor needs to be reconsidered. At the very least, European stakeholders

should have an opportunity to approve the role, scope and standards of trustmark schemes in situations where these trustmarks are being used to attract European consumers.

The complete absence of dispute resolution information in over 30% of Safe Harbor privacy policies is another stubborn issue that needs to be resolved. The FTC's failure to act in the Directors Desk case means that alternative mechanisms will need to be pursued. Perhaps what is needed is for the US and EU to re-think the governance of the Safe Harbor. They could consider jointly appointing a Safe Harbor supervisor – a harbormaster – to ensure basic compliance with the Framework. In the US it may be easier to enforce basic standards through a binding membership agreement with specified sanctions and remedies, rather than relying on the threat of ad hoc (and random) FTC action.

Finally, there should be some discussion about whether or not the Safe Harbor has served its purpose and whether or not it is now time to move on. It was a limited, compromise, stop-gap measure, that has drifted for 13 years without ever delivering high levels of compliance. Are there alternatives that could produce a better result?

About the author

Chris Connolly is a privacy advocate and researcher, and has provided advice to national and international organisations regarding privacy practices, electronic commerce law, and cloud computing. He is currently based in Bath in the United Kingdom. He has previously worked extensively in Australia and the Asia-Pacific. Galexia is a private consulting company based in Australia with a small network of international experts and associates.

http://www.galexia.com