Global Information Assurance Certification Paper

Gimme Shelter: Seeking Protection in the U.S. Safe Harbor
GIAC Security Essentials Level 1 Practical Assignment
January 25, 2001

Cecil Claspell

Introduction

In 1980, the Organization for Economic Cooperation and Development (OECD) published a document with guidelines for protection of personal privacy. This document, known as "Guidelines on the Protection of Privacy and Transborder Flows of Personal Data", establish standards for the privacy of personal records. In 1995, the European Union's (EU) 15 member countries adopted the guidelines, commonly known as the EU Privacy Directive. The EU Privacy Directive became effective in 1998.

Under the terms of the EU Privacy Directive, the EU countries can cut off the flow of data to any country whose privacy laws are deemed inadequate. Theoretically, this permission to withhold data is suspended until June 2001. While some companies in the United States are beginning to feel the impact of the EU's decision and have taken action, only a handful of companies in compliance.

To permit continued commerce between EU and U.S. companies, especially with regard to transferring personal data, the U.S. Department of Commerce developed a set of rules creating a "safe harbor" against EU regulation. These rules comprise a self-certification program that, if adhered to, allow data transfer between the U.S. and EU member countries. This paper briefly describes the principles of the EU Privacy Directive, the U.S. Safe Harbor principles, and why more companies are not taking shelter in the Safe Harbor.

What is the EU Privacy Directive?

The Privacy Directive consists of eight principles intended to protect the privacy of an individual's personal data[1]. The Privacy Directive outlines principles that are to be adopted to ensure privacy protection, and also details remedies in cases where data is used in a manner counter to the principles. These principles were based on international agreements, national laws, and self-regulatory policies in place in EU member countries in the 1980's.

- **Collection Limitation** – All personal data should be collected legally and fairly, with the owner's knowledge and permission (where appropriate).
- **Data Quality** – All personal data should be accurate, complete, current, and relevant to the purpose for which they are collected.
- **Purpose Specification** – Specify the purpose for collecting personal data at the time it is collected; only use the data for the purpose specified.
- **Use Limitation** – Don't disclose the personal data or use it for any other purpose other than that specified, unless the data subject gives their permission, or by authority of law.

- **Security Safeguards** – Protect personal data from unauthorized access, use, modification, destruction, loss, or disclosure by using reasonable safeguards.
- **Openness** – Promote openness with regard to developments, practices and policies related to personal data; ensure that the existence and nature of the personal data and their use can be readily established, and the identity and residence of the data controller is readily available.
- **Individual Participation** – Individuals have certain rights, including:
  - the right to know whether a data controller has personal data about the individual
  - the right to examine the data in a form that is readily intelligible to the individual; the data is to be made available within a reasonable time, at a charge that is not excessive, and in a reasonable manner
  - the right to be given reasons if a request to examine the data is denied, and the right to challenge the denial
  - the right to challenge data relating to the individual, and to have incorrect data fixed
- **Accountability** – The data controller is responsible for compliance with measures related to the other seven principles.

The text of each of the principles of the EU Data Privacy Directive is detailed in Appendix A. The complete text of the Privacy Directive can be viewed at:

http://www.oecd.org/dsti/sti/it/secur/prod/PRIV-EN.HTM

Soon after the publication of the Privacy Directive, 182 U.S. companies claimed that they had adopted the guidelines. However, few of these companies ever bothered to implement the necessary controls to comply with all eight principles.[ii]

Safe Harbor Background

Initially, U.S. Government officials expressed no concern about negative effects of the Privacy Directive on e-commerce with U.S. companies. This was due, in part, to Article 26 of the Directive -- essentially a list of exceptions that are allow free transfer of personal information required to complete e-commerce transactions. Article 26 says that the transfer of personal information is allowed when "necessary for the performance of a contract," and the individual gave unambiguous consent. Based on the belief that the Article 26 exceptions would allow EU nations to participate in unrestricted e-commerce transactions with U.S. companies, there was no immediate action taken to adopt a similar approach to privacy in the U.S.[iii]

There is no explicit guarantee of privacy in the United States Constitution. The U.S. has no blanket privacy legislation, relying instead on various laws that have been developed over the past century. These laws were created in response to specific needs, such as the Fair Credit Reporting Act, the Electronic Communications Privacy Act, the Telephone Consumer Protection Act, and the Health Insurance Portability and Accountability Act to name a few. The U.S. also relies heavily on self-regulation to ensure compliance.

Legislation and regulation in the U.S. is applied very narrowly on a sector-by-sector basis.[iv]

Privacy in the U.S. has historically been treated as a national issue, with protections extended to U.S. citizens and resident aliens. Until the enactment of the EU Privacy Directive, there had been no privacy protection extended to individuals beyond U.S. borders. This lack of privacy protection caused increasing concern in the EU. In early 1997, several EU officials claimed that the exceptions granted in Article 26 were not mandatory. These officials argued that since U.S. laws offered inadequate privacy protection to EU citizens, EU member nations could block transfers of data to the U.S.

This pronouncement that e-commerce transactions with the EU would cease brought a swift reaction from the U.S. Commerce Department. The U.S. Commerce Department began the process of educating EU officials about the sectoral approach to privacy. At the same time, companies engaging in e-commerce with the EU were invited to participate in the design of privacy controls. These controls would convince the EU that the U.S. has functional equivalents to the protections provided in the Privacy Directive. The outcome of this effort is seven principles that, if complied with, entitle companies to enjoy the benefits of a "safe harbor" with regard to treatment by EU countries.[v]

The seven principles of Safe Harbor are:

- **Notice** – Notify the individual about what data is collected, and how and why their data is being used; make sure the notice is clear and conspicuous, and give the individual choices for limiting use and disclosure of the data.
- **Choice** – Individuals must have the ability to opt-out of additional uses for their data, other than that for permission was originally given.
- **Onward Transfer** – When an individual's information is transferred to a third party (with the individual's permission), the third party must provide at least the same level of privacy protection afforded by the original data collector.
- **Security** – Protect personal data from unauthorized access, use, modification, destruction, loss, or disclosure by using reasonable safeguards; also make take precautions to ensure data reliability for its intended purpose.
- **Data Integrity** – Collect only the personal data that is required, and make sure it is accurate, complete, and current.
- **Access** – Individuals have the right to examine information about themselves, and can correct inaccurate and incomplete information.
- **Enforcement** – Put mechanisms in place to handle complaint and dispute resolution, compliance verification, and sanctions for violation of the principles.

The text of each of the principles of the Safe Harbor is detailed in Appendix B. The complete text of the Safe Harbor Principles can be viewed at:

http://www.export.gov/safeharbor/SafeHarborInfo.htm

Privacy Directive Versus Safe Harbor

The following table compares the principles of the EU Privacy Directive with those of the U.S. Safe Harbor. Although there is not a direct mapping between the two approaches to privacy, I've taken some liberty in drawing the following comparisons:

Privacy Principle	**EU Privacy Directive Principle**	**U.S. Safe Harbor Principle**
Data collection should be performed legally, and with the knowledge and permission of the individual	Collection Limitation	Notice
Ensure accuracy, completeness, relevance to the purpose	Data Quality	Data Integrity
Specify the purpose for collecting personal data at the time it is collected; only use the data for the purpose specified	Purpose Specification	Choice
Don't disclose the personal data or use it for any other purpose other than that specified, unless the data subject gives their permission, or by authority of law	Use Limitation	Onward Transfer
Protect personal data from unauthorized access, use, modification, destruction, loss, or disclosure by using reasonable safeguards	Security Safeguards	Security
Promote openness with regard to developments, practices and policies related to personal data; ensure that the existence and nature of the personal data and their use can be readily established, and the identity and residence of the data controller is readily available	Openness	N/A
Let the individual know if personal data is collected, and give them the right to examine, challenge, and correct the data.	Individual Participation	Access
The data controller is responsible for compliance with measures related to the other seven principles	Accountability	Enforcement
Implementation and compliance monitoring	Formal monitoring by government agencies	Self-certification

From the table above, one might conclude that compliance with the Safe Harbor principles meets the requirements outlined in the EU Privacy Directive. However, one area of concern has been over implementation and monitoring. The EU requires the creation of government data protection agencies with formal monitoring and penalties for non-compliance. The US relies on a self-certification program with penalties for non-

compliance. This disparity was debated right up to the final vote on acceptance by the EU, and may again cause problems in the future.

Who's in the Harbor?

The Safe Harbor framework was given the nod by the EU in July of 2000, with an effective date of November 1, 2000. This approval implies that the U.S. Safe Harbor framework provides adequate privacy protections to EU member countries. The U.S. Department of Commerce maintains a list of companies that have self-certified their compliance with the Safe Harbor framework.[vi] With the number of U.S. companies doing business with European customers, the Safe Harbor compliant list should number in the hundreds if not thousands. When I accessed the list on November 1, 2000, there was only a single listing: TRUSTe. Accessing the same list on January 25, 2001, I find that the number of companies has swelled to 13.

This begs the question: if implementing the Safe Harbor framework is such a good idea for U.S. businesses, why aren't more of them doing it? I theorize that it may be due to any of the following perceptions:

Safe Harbor is difficult to understand and difficult to implement

According to the U.S. Department of Commerce, Safe Harbor is relatively painless. Here's the checklist:

1 – Read the Safe Harbor overview (including benefits of joining)
2 – Read the Safe Harbor documents (including FAQs)
3 – Review the Safe Harbor workbook
4 – Bring your organization into compliance
5 – Verify that you have done so
6 – Review the information required for certification, and send in the form[vii]

No Benefit to Compliance

If a U.S. company engages in the transfer of personal data to or from EU member countries, the transfers could be suspended until compliance with Safe Harbor is certified. Safe Harbor certification is an expensive way to demonstrate privacy protection, and ensure the continued flow of data.

We Don't Do Business in Europe

Any company operating a web site that asks for personal information could be affected. Any company with employees in EU countries could also be affected.

Strict penalties for non-compliance

While the decision to implement the Safe Harbor framework is voluntary, once certified, a company is subject to civil penalties of up to $12,000 per day for non-compliance.[viii]

Lack of Awareness

There are no more than a handful of online references related to Safe Harbor. I expect much more press on the subject as the EU data cutoff date (June 2001) approaches, but most companies either do not have Safe Harbor on their radar screens, or have no urgent need to comply.

Summary

Seeking shelter in the U.S. Safe Harbor demonstrates to the EU that adequate privacy protections are in place. U.S. companies that are either currently doing or planning to do business with European companies should investigate Safe Harbor compliance.

Appendix A

WHAT DO THE EU PRIVACY GUIDELINES REQUIRE?

"Guidelines on the Protection of Privacy and Transborder Flows of Personal Data" require compliance with the following eight principles:

Principle	Description
1. Collection Limitation	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.
2. Data Quality	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.
3. Purpose Specification	The purposes for which personal data are collected should be specified not later than at the time of data collection and the subsequent use limited to the fulfillment of those purposes or such others as are not incompatible with those purposes and as are specified on each occasion of change of purpose.
4. Use Limitation	Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with Paragraph 9 except: a) with the consent of the data subject; or b) by the authority of law
5. Security Safeguards	Personal data should be protected by reasonable security safeguards against such risks as loss or unauthorized access, destruction, use, modification or disclosure of data.
6. Openness	There should be a general policy of openness about developments, practices and policies with respect to personal data. Means should be readily available of establishing the existence and nature of personal data, and the main purposes of their use, as well as the identity and usual residence of the data controller.
7. Individual Participation	An individual should have the right: a) to obtain from a data controller, or otherwise, confirmation of whether or not the data controller has data relating to him; b) to have communicated to him, data relating to him within a reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible to him; c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and d) to challenge data relating to him and, if the challenge is successful to have the data erased, rectified, completed or

	amended.
8. Accountability	A data controller should be accountable for complying with measures that give effect to the principles stated above. The United States endorsed the OECD Guidelines.

Appendix B

WHAT DO THE SAFE HARBOR PRINCIPLES REQUIRE?[ix]

Organizations must comply with the seven safe harbor principles. The principles require the following:

Principle	Description
1. Notice	Organizations must notify individuals about the purposes for which they collect and use information about them. They must provide information about how individuals can contact the organization with any inquiries or complaints, the types of third parties to which it discloses the information and the choices and means the organization offers for limiting its use and disclosure.
2. Choice	Organizations must give individuals the opportunity to choose (opt out) whether their personal information will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorized by the individual. For sensitive information, affirmative or explicit (opt in) choice must be given if the information is to be disclosed to a third party or used for a purpose other than its original purpose or the purpose authorized subsequently by the individual.
3. Onward Transfer	(Transfers to Third Parties): To disclose information to a third party, organizations must apply the notice and choice principles. Where an organization wishes to transfer information to a third party that is acting as an agent (1), it may do so if it makes sure that the third party subscribes to the safe harbor principles or is subject to the Directive or another adequacy finding. As an alternative, the organization can enter into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant principles.
4. Access	Individuals must have access to personal information about them that an organization holds and be able to correct, amend, or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.
5. Security	Organizations must take reasonable precautions to protect personal information from loss, misuse and unauthorized access, disclosure, alteration and destruction.
6. Data Integrity	Personal information must be relevant for the purposes for which it is to be used. An organization should take reasonable steps to ensure that data is reliable for its intended use, accurate,

	complete, and current.
7. Enforcement	In order to ensure compliance with the safe harbor principles, there must be (a) readily available and affordable independent recourse mechanisms so that each individual's complaints and disputes can be investigated and resolved and damages awarded where the applicable law or private sector initiatives so provide; (b) procedures for verifying that the commitments companies make to adhere to the safe harbor principles have been implemented; and (c) obligations to remedy problems arising out of a failure to comply with the principles. Sanctions must be sufficiently rigorous to ensure compliance by the organization. Organizations that fail to provide annual self-certification letters will no longer appear in the list of participants and safe harbor benefits will no longer be assured.

[i] Center for Democracy and Technology, "CDT's guide to online privacy | OECD," 1998 – 2000, URL: http://www.cdt.org/privacy/guide/basic/oecdguidelines.html (18 December 2000)

[ii] ibid

[iii] Scott Killingsworth and Brett Kappel, "Safe Harbor in Muddy Waters? The Commerce Department Proposes Voluntary Principles for Compliance with the European Union Privacy Directive," 1998, URL: http://www.pgfm.com/publications/safeharbor.html (1 November 2000)

[iv] Center for Democracy and Technology, "CDT's Guide to Online Privacy", 1998 – 2000, URL: http://www.cdt.org/privacy/guide/protect/, (18 December 2000)

[v] U.S. Department of Commerce, "Safe Harbor", URL: http://www.export.gov/safeharbor/ (18 December 2000)

[vi] U.S. Department of Commerce, "Web Page for Safe Harbor List", URL: http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list (25 January 2001)

[vii] U.S. Department of Commerce, "Safe Harbor", URL: http://www.export.gov/safeharbor/checklist.htm (25 January 2001).

[viii] U.S. Department of Commerce, "Safe Harbor", URL: http://www.export.gov/safeharbor/SafeHarborInfo.htm#Benefits (18 December 2000)

[ix] U.S. Department of Commerce, "Safe Harbor Overview," URL: http://www.export.gov/safeharbor/SafeHarborInfo.htm (18 December 2000)