The Safe Harbour Agreement and Maintaining Status Quo

Linda Margaret Broughton
Title: The Safe Harbour Agreement and Maintaining Status Quo
Module: Legal Aspects of Contemporary International Problems

Student: Linda Broughton, Word Count: 4,700
Introduction

The introduction of online commerce and data exchange via the Internet has led to debate over the implications of the legal applicability of the sovereignty of the geographically defined State in the virtual world. The Internet collapses geography, allowing users to interface and exchange data with other individuals, companies, and additional online actors regardless of differing locations or nationalities. This paper will argue that, despite the construction of new arenas of debate and negotiation, State sovereignty over the law within its territory remains a priority in the creation, interpretation, and implementation of eCommerce-related law, specifically in the area of the protection of the private data of individuals.

In particular, this paper will consider an international legal negotiation between the European Union (EU), inclusive of its Member States, and the United States of America. The negotiations discussed in this paper were inspired by interpretations of the 1995 European Data Privacy Directive 95/46/EC with regard to private data collection by private companies operating in the USA and the EU. These negotiations resulted in the Safe Harbour Agreement. Despite the historical and current political, legal and commercial interaction between these international actors (and their composite States and states), the negotiations triggered around the EU Privacy Directive denote the potential legal controversies embedded in the rise of online data transfers. Despite appearing to
construct new hybrid international legal agreements, the conclusions reached through the Safe Harbour negotiations demonstrate that EU and US governmental responses, with regard to the transfer of private data, at least with those laws that might be applied within their territories, are to protect and maintain respective legal traditions and powers.¹

Prior to this discussion, it must be noted that State sovereignty within the EU is a hotly debated topic. Many Member States maintain that the European Union Treaties derive their power not from the EU institutions that distribute European legislation but from the sovereign nations that agree to the legislation via the Treaties. For examples, please see, for the United Kingdom, case 

_McCarthys Ltd. v. Smith²_ or, for Germany, the case _Brunner v. European Union Treaty, Bundesverfassungsgericht._³ This paper will not consider these issues but will assume that the EU institutions consider and respect EU Member State

---

¹ Where possible, footnotes are accompanied by an online reference that requires no special academic access. This serves to illustrate the transborder nature of information and data online. Most information accessible via the Internet does not necessarily consider the location of the individual entity that seeks to access the data. Exceptions to this rule that apply to the US and the EU generally result, as argued in this paper, from territorial sovereignty-related legal disputes. For example, in France, the website Yahoo! was fined up to 13,000 dollars a day for permitting French citizens to access auction sites of Nazi and Klu Klux Klan memorabilia. While the company complied with French laws on its French site, which in accordance with anti-racist policies in France did not permit the sale of such paraphernalia, the French judge Jean-Jacques Gomez determined that Yahoo must install a filter in order to forestall French visitors to the American site from accessing the prohibited material.¹ In a California court in 2001 Yahoo! successfully argued that it could not be expected to shield French users from a site based in the United States, where the sale and purchase of such objects was permitted as a form of Constitutionally-protected free speech. However, subsequent legal battles prolonged the question until the most recent US Federal court ruling in March 2005, stating that Yahoo had not suffered undue hardship due to the French ruling (in fact, Yahoo largely had largely complied with the judgment) and that US courts held no jurisdiction over the French courts in this case, and thus French rulings were sound.¹ For further information, see Juan Carlos Perez of IDG News Service, “Yahoo Loses Appeal in Nazi Memorabilia Case”, _PCWorld_, 12 January 2006, Accessed 10 December 2007, [http://www.pcworld.com/article/id,124367-page,1/article.html?RSS=RSS](http://www.pcworld.com/article/id,124367-page,1/article.html?RSS=RSS).


sovereignty insofar as the legal decisions that it makes with regard to non-EU States, specifically the United States of America, and the Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and the Free Movement of such Data.
I. The United States and the European Union: Traditional legal approaches to Private Data Protection

This paper will first consider the legal traditions related to the interpretation and regulation of private data transfers in both “European” legal traditions, that is legal traditions espoused by the EU on behalf of its Member States, and US legal traditions. This section will demonstrate that both EU and US institutional authorities attempted to initiate standards within their States and rooted in the legal and economic traditions of their States that might be internationally recognised and implemented. This section will emphasise how the European and US private data protection legal frameworks parallel rather than intersect, despite mutually recognising common international objectives. First, the EU Privacy Directive 94/46/EC, with which the EU created the initial conditions to standardise private data protection throughout its Member States, the origins of this Directive’s concerns and regulations, and the Directive’s implications will be analysed. Concurrent developments in US institutions with regard to private data protection and regulation will then be examined.

State territory and legal sovereignty

The State has frequently used physical territory as a means of debating legal influence and consideration. International legal debates have considered, among other aspects, the territory or territories from which originates an individual citizen that initiates an action, the territory or territories in which an individual initiates an action, as well as the territories of individuals influenced by
an action. This paper will first consider the legal traditions in private data interpretation and regulation in both “European” legal traditions, that is legal traditions espoused by the EU and its Member States, and US legal traditions. EU and US institutional authorities in the 1990s initiated standards within their States, rooted in the legal and economic traditions of their States, which complied with their respective interpretations of international recommendations related to eCommerce and the transborder transfer of private data. As these respective interpretations complied with international recommendations, European and American authorities suggested that their standards and practices might be internationally recognised and accepted within and without their sovereign legal jurisdictions.

Representatives from the US government and the European Union Council endorsed the private data protection guidelines created by the Organisation for Economic Cooperation and Development (OECD) as a basis for beginning to standardise OECD Member State data protection practices. The first OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data were published in 1980 and foresaw the eventual conflict embedded in national legislation regarding transborder data exchange. A subsequent Declaration on Transborder Data Flows, issued in 1985, “intend[ed]
to make clear the general spirit in which OECD Member countries [would] address policy issues connected with these transborder data flows”.

John Dryden, Head of Information, Computer and Communications Policy Division in the OECD’s Directorate for Science, Technology and Industry sums up the importance of national government in transborder data flow: “Responsibility stays with national governments, notably to protect vulnerable groups”. Dryden goes on to emphasise that “the regulatory environment should be a balance between self-regulation and regulation by government and international bodies developed co-operatively by government, business and the public voice”. The consistent participation of national governments through legal regulation in this process is imperative in the perception of the EU and the OECD.

The EU and the Citizen Consumer

The origins of the EU motivation to standardise private data protection develop out of the common market, the area of core competence for the EU institutions and the basis for the majority of EU legislation. The EU institutions include the Commission, in charge of issuing much EU legislation, the Council, representing individual Member States in different areas of European concern, and the European Court of Justice, the judicial branch of the EU. These

---

institutions derive their power and jurisdiction from a number of EU and European Communities Treaties and Protocols overseeing the construction and implementation of the European common market. The European common market is increasingly defined through a number of European Treaties and related legislation and practices; one of the most comprehensive documents describing the laws and practices of the European common market in the last two decades is the Treaty of Maastricht. The European Commission composed the EU Privacy Directive from the powers and responsibility accorded the Commission largely as a result of this Treaty.

The 1992 Maastricht Treaty of the European Union made provisions to institute a European single currency in order to “establish [an] economic and monetary union”, a main objective outlined in the Treaty. The Treaty also established EU policies in six new market-related areas, one of which was consumer protection for EU citizens. With the upcoming implementation of a common currency and the promise to try to equally protect all European consumers, the EU needed to first establish private data protection guidelines to be achieved and enforced throughout the Member States. Pursuant to that end, the European Commission issued the European Data Privacy Directive in 1995.

---


In EU legislation, a directive “shall be binding, as to the result to be achieved, upon each Member State to which it is addressed, but shall leave to the national authorities the choice of form and methods.” The EU Privacy Directive further elaborated upon the OECD Framework, legally requiring the Framework described in the Directive to be practiced throughout the EU Member States. As a “directive”, the EU Privacy Directive served to standardise the interpretation and treatment of private data within the EU through legislation that existed and/or was adopted by the Member States. While the EU institutions do not directly implement a Directive, a Directive can have direct legal force. The Privacy Directive provided a legislative basis for interpretation and judgement by the European Court of Justice (ECJ) should Member States not properly implement the standards outlined.

The Directive promised equal private data protection for all EU citizens both within and without their Member States. In Chapter IV, Article 25, the Directive ordered Member States to maintain the private data protection standards of the Privacy Directive in the event that an EU citizen’s private data is transferred “to a third [non-EU] country” through insuring that the third country complied with the standards of protection set out in the Directive. While equal standards within the EU were presumed once the Directive was implemented by

---


each Member State, allowing the subsequent transborder transfer of private data, non-EU States would require a EU institutional recognition of “adequacy” with regard to private data protection standards in national legislation.

The USA and private commerce

US political representatives agreed with the OECD nonbinding privacy principles but never necessarily agreed to the creation of actionable legislated privacy rights by which to prosecute private firms. It is the tradition of the US government to maintain very little involvement in private business and instead to encourage private self-regulation.14 This is generally considered in US historical and legal tradition to be a more effective and comprehensive form of regulation. One of the largest informational privacy legislation found in the United States prior to the new millennium was The Privacy Act of 1974, which pertains largely to data processing by the federal government.15 There have been other, specific laws passed with regard to data privacy in specific sectors and/or specific states, but there is no formal and comprehensive legislation concerning all transfers of private data enacted by US government authorities.

When US President Bill Clinton’s e-commerce policy creator, Ira Magaziner, crafted the “Framework for Global Electronic Commerce”, published in 1997, the Framework stressed the importance of private self-regulation without


extensive government interference. The Framework explained that
“Governments should avoid undue restrictions on electronic commerce” and
“Where governmental involvement is needed, its aim should be to support and
enforce a predictable, minimalist, consistent and simple legal environment for
commerce.” 16 The emphasis in Magaziner’s approach appears to be commerce
itself with the expectation that is in the interest of commerce to protect the private
data of the consumer.

In US legislation, government is frequently an aid to private regulation and
standard setting. Unlike the EU, which created a common market out of distinct
national markets, the US already oversaw a unified national market with
international commerce and subsequently manoeuvred to craft a private data
framework that would recognise and reinforce the market practices already in
existence. The endorsement of Magaziner’s “Framework”, by US President Bill
Clinton and Vice-President Al Gore, noted,

“The administration supports private sector efforts now
underway to implement meaningful, user friendly, self-regulatory
privacy regimes. These include mechanisms for facilitating
awareness and the exercise of choice online, private sector
adoption of and adherence to fair information practices, and
dispute resolution. The government will work with industry and
privacy advocates to develop appropriate solutions to privacy
concerns that may not be fully addressed by industry through
self-regulation and technology.” 17

US policy perceived this legal framework as a more pragmatic means of creating standards that would be respected internationally and thus more conducive to international commerce.

Private organisations agreed with and in many ways had already implemented this rationale. For example, the Internet Engineering Task Force supported the emphasis on government non-interference found in the Framework. The IETF was a self-organised private actor that Magaziner noted had previously succeeded in resolving many technical issues related to the Internet without any need for government legislation.\(^{18}\) Magaziner and several big firms also encouraged the Better Business Bureau, a self-regulating group with a strong offline reputation, to create an online programme of data protection standards. This evolved into an online commercial dispute resolution system, the Better Business Bureau Online (BBBOnline). Ira Magaziner’s ideas, according to Russ Bodoff, Vice-President of Marketing for the Better Business Bureau, included the beginning of a globally coordinated initiative to create online protection standards.\(^{19}\) Through these and similar initiatives, the U.S. government purposefully avoided crafting private data protection legislation related to eCommerce, instead endorsing principles of private data protection as well as the principles of private self-regulation.


The potential conflict of coordination

Despite a joint 1997 statement by the EU and the US concerning the potential of private sector initiatives to self regulate, the EU still planned to legislate the regulation of private data transfers through its Directive while the US continued to encourage private self-regulation rather than public legislation.\(^\text{20}\) It is obvious that these different approaches to private data protection must cross more than oceans in order to coordinate; however, no institutional authorities on either side of the Atlantic agreed to alter the institutional and legal practices adopted and actively practiced by their own political and commercial actors in the area of private data transborder transfers. As the traditional trade between the US and the EU makes up one of the world's largest bilateral trade relationships,\(^\text{21}\) a condition occasioning the frequent transborder transfer of the private data of individuals, a crisis of coordination was swift and inevitable.


II. The Safe Harbour Agreement: Conceiving a Basis for Coordination?

In the first section, this paper contrasted the legal and institutional approaches to private data protection pursued in the EU and the USA. The EU insisted upon uniform public legislation in order to insure the protection of individuals’ private data. The USA refused such legislation and encouraged the foundation of private self-regulating organisations to create the standards for transborder private data transfers. Because the USA lacked the legislative protection of private data demanded by the EU Privacy Directive, it was not considered an “adequate” third country to which the private data of EU citizens could be legally transferred. Some form of coordination was necessary to sustain the commerce already in place as well as to allow for continued commercial interaction between citizens and businesses located in the EU and the USA.

In this section, this paper will consider the initial negotiations held to achieve these objectives, the Safe Harbour Agreement. This section will discuss how this Agreement was perceived as a means of international legal coordination that was able to sustain yet reconcile the separate legal positions of the EU, its Member States, and the USA. Constructivist theories have argued that the international dialogue that resulted between EU and US actors in the Safe Harbour Agreement developed an innovative platform for international coordination. Rather than attempting to impose conflicting legislation in the EU or the US, constructivist theory suggests that negotiators from both areas “constructed”, that is, developed, new means of cooperation and mutual
understanding.\textsuperscript{22} The Agreement made possible new channels of collaboration between two opposing legal foundations. However, this section will demonstrate that the tactics chosen by the political institutions involved more effectively maintained traditional legal practices and powers rather than coordinated contrasting legislation and interpretation.

\textit{The points of contention}

The Safe Harbour Agreement arose in response to the EU Privacy Directive’s stipulation that the onward transfer of a EU citizen’s private data to a third country is permissible “only if…the third country in question ensures an adequate level of protection”.\textsuperscript{23} The EU planned to standardise protection of citizens’ privacy within the EU and (per the Directive) within transborder data transfers between EU Member States and non-Member States. The EU Commission reserved the right to request a Member State to block the transfer of data to an “inadequate” third country. The ECJ, as the judicial branch of the EU, held the authority to interpret an alleged misapplication of the Privacy Directive.

The USA as a third country could not be recognised as “adequate” under the EU Privacy Directive because the USA lacks comprehensive formal legislation with regard to the protection of private data. As discussed in section one of this paper, the government of the USA supports private self-regulation.


US companies operating in the EU may have initially hoped to achieve permission to transfer data through the derogations listed in Article 26 of the Privacy Directive; however, while the Commission granted a brief reprieve to facilitate commercial interactions during the negotiations that produced the Safe Harbour Agreement, no permanent derogation was forthcoming, nor was it likely that such a permanent derogation could be legally justified in European law. Neither the US nor the EU political position appeared overly amenable to alteration in favour of the other, nor did a compromise seem legally practical without legislative modification by one side or the other.

Assuring adequate protection was not the only concern. In addition, it was necessary to coordinate what constituted private data in the EU and the USA, especially sensitive private data. Internet interdependence with respect to private data involves not only the coordination of legislative standards but also resolving conflicts over “fundamental social norms”. European nations are sensitive concerning personal identification data such as sexual preference and religion. In light of European history (most conspicuously the events of World War II), this private information is considered data worthy of careful protection through government legislation. In contrast, studies demonstrate that many Americans, with or without justifiable reasons, have more faith in the private sector in the collection and protection of private data. Government agents have historically been condemned for the legal manipulation private data such as ethnic identity in order to restrict US population segments (for example the segregation of African-Americans from non-African Americans in public places).
Such practices are more perceived as more legally vulnerable in the private sector. The private sector in the USA is historically perceived as more susceptible to the scrutiny of the public and the media than the government.\textsuperscript{24}

\textit{The search for solutions}

The US Ambassador to the OECD David Aaron initiated negotiations in 1998 with John Mogg, the European Commission’s Director-General for the Internal Market. The first aspect of the Safe Harbour Agreement involved redefining the notion of “third country” to include commercial actors, specifically US-based companies, and thus avoid the need for the US government to introduce legislation. Aaron noted that his concept of a “Safe Harbour” emerged from American tax law. The idea suggested that the private data protection standards of the companies could be deemed “adequate” if not the US government.\textsuperscript{25} A “Safe Harbour” would provide a safe repository for data within the USA.

The United States explanation of the Safe Harbour Agreement stipulated that “organisations will also be able to provide the safeguards necessary under Article 26 of the Directive if they include the [Principles specified in the Agreement] in written agreements with parties transferring data from the EU for the substantive privacy provisions, once the other provisions for such model


contracts are authorised by the Commission and the Member States.”

Private organisations or companies, can therefore receive the Commission’s “adequacy” rating and permit the transborder transfer the private data of EU citizens despite the “inadequate” legislation of the country in which the data is received, notably the USA. Companies were given the option of applying directly to the EU for an official recognition of adequacy or of joining private organisations such as TRUSTe or the BBBOnline for a “seal” of adequacy that the EU agreed to assess and endorse.

The Agreement adopted the EU Privacy Directive’s seven principles. These principles appear to present a compromise that permits a coordination of private data legislation between the EU and the USA. Choice for the individual must allow the individual to participate in what is done with the data outside of the immediately specified purpose for the initial collection of the data. “Sensitive information” was further described to include “i.e. personal information specifying medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership or information specifying the sex life of the individual”. Conditions were set up for the onward transfer of the data, specific security precautions were required, as well as conditions concerning data integrity, individual access to the information, and the means of enforcement for the Agreement.


Yet possible perception of the principles as a legislative compromise is usurped by the Agreement signatories, which are neither all public nor private. Both US and EU authorities legally sanctioned the position of the other as long as their own positions persisted within their own territories. Both pursued the establishment of their own private data protection regulation as international practice: the EU through the international adoption and practice of its seven principles and the US through the continued use of private self-regulation. European and US legal traditions and powers are still perceived as fulfilling the OECD suggestions as agreed to and interpreted by the respective States. The parallel positions are further described in the Agreement; however, they do not intersect in interpretation or implementation.

It is arguable that US government pressure on private companies and organisations compelled cooperation between private US companies and public EU authorities. Susan Scott, the Chairman of TRUSTe in 1998, noted that membership growth was “strangely coincidental to about the time when the [US] government started really putting down their heavy hand”. Such an argument would suggest that the EU Directive succeeded in indirectly setting legally actionable protection standards within the United States despite the lack of comprehensive US legislation. This would support the constructivist view that new precedents of international legal cooperation were initiated in the Safe Harbour Agreement. However, while threats of US legislation in the absence of privatised solutions to the negotiations may have encouraged US companies to

---

participate in web-seal programme membership, current membership in the Safe Harbour Agreement and the adoption of EU data protection standards is legally voluntary, not legislatively required, in the USA.

If a company agrees to the principles, enforcement is permitted through several channels: cooperation with authorities with whom the Safe Harbour participants agree to cooperate (an ADR mechanism, such as BBBOnline, TRUSTe or the Direct Marketing Association29), or direct cooperation with EU Data Protection authorities (a form of enforcement that is required with respect to certain types of data). Failure to comply with the regulations to which signatories to the Agreement voluntarily accept can result in action taken by the United States Federal Trade Commission (FTC). EU Member States may halt data flows should FTC actions prove ineffective in correcting the violation.30

The combination of enforcement mechanisms in the Safe Harbour Agreement further illustrates the protection of respective legal practices rather than their coordination. Enforcement is thus only possible after the company first voluntarily agrees to the principles and then fails to fulfill the agreement, a concept in complete agreement with US legal practices.31 The ability of a EU Member State to halt the data flows of citizens is also in keeping with current political and legal practices. Additionally, as a result of the Directive, the halt of data transfers within one Member State is hardly constrictive as companies can

31 Breach of contract law, pacta sunt servandum, is a common aspect of civil law in several Western States’ legal systems, among them the United States of America.
legally transfer data via an alternative Member State regulator before continuing
a transborder transfer to the USA. In order to truly halt data flows to the USA, all
EU Member States and private regulators would have to agree to unilaterally halt
the flow of data. The legal diffusion of implementation combined with the various
means of enforcement negates the uniformity of the interpretation of the Privacy
Directive standards.

Conclusion

The EU Directive 94/46/EC on the Protection of Individuals with Regard to
the Processing of Personal Data and the Free Movement of such Data created
the conditions that precipitated the first EU-US international negotiation with
respect to transborder data transfers considered in paper, that of the Safe
Harbour Agreement. The negotiations leading to the Safe Harbour Agreement
outlined seven principles that determine EU standards for “adequacy” in private
data protection. These principles originated from the EU Privacy Directive in
order to facilitate the exchange of private data within the European common
market. However, the Directive also impacted private data transfers between EU
Member States and non-EU States, such as the USA. In the Safe Harbour
negotiations the US government did not adopt EU standards of private data
protection, as was initially thought to be required by the Directive. In fact, US
negotiators sought to avoid the adoption of a unified private data policy in US
legislation and to preserve US legal traditions with respect to private industry
self-regulation. The EU also successfully manoeuvred to maintain European
standards and avenues of public EU enforcement of those standards while permitting commerce with US multinational companies to continue.
III Further implications of the Privacy Directive and Safe Harbour

The Safe Harbour Agreement is indicative of EU and US approaches to private data protection as it relates to eCommerce. Both legal systems used international debate to frame an Agreement that is legally binding in the EU and voluntary in the USA. The results of the Agreement do not create a compromise or a new means of respective legal coordination or understanding. The Safe Harbour Agreement sustains the legal jurisdictions, traditions, and practices of the States involved in the negotiations.

It can be argued that by requiring US multinational companies to voluntarily agree to the principles found in the EU Privacy Directive as well as permit EU and European Member State authorities to enforce the implementation of these principles violates the self-regulation practiced by the companies with respect to private data transfers in the United States legal system. However, enforcement of the Privacy Directive’s standards of protection would be difficult without compelling all the Member States to halt the data transfers practiced by a US multinational. It is largely up to the individual Member States or various regulators to find a company’s private data protection standards wanting and then put the matter before an EU institution and other regulators.

The Safe Harbour Agreement is too broad to be a basis for effective coordination. The principles agreed to within the Agreement, and the different levels of enforcement diffuse the interpretation and implementation of the application of the principles. Despite rhetoric praising the coordination offered via the Agreement, the Safe Harbour Agreement is more useful as a means of
sustaining current transactions. At the end of 2007, the social networking platform Facebook, incorporating users from France and the United Kingdom, two EU Member States, and a member of the TRUSTe Safe Harbour seal programme, experienced the ambiguity of the Safe Harbour Agreement.\(^{32}\)

The Facebook Beacon publishes the purchases of Facebook users to their Facebook “Friends”\(^{33}\) on retailers' websites. The protests voiced by Facebook users following the initiation of Beacon resulted in the creation of an “opt-out” clause permitting Facebook users to opt-out of Beacon (as opposed to an “opt-in” clause, by which users would choose to participate). Online media reports wonder if an EU institution will take Facebook CEO Mark Zuckerberg before the ECJ, as Facebook is a member of the TRUSTe Safe Harbour Seal organisation. No clear coordinated legal action exists.\(^{34}\) The Facebook server is located in the USA, users volunteer their private data and agree to the platform’s Terms of Service. In the USA, the protest of the consumers altered the practice of the platform while in the EU, additional legal actions are being considered.

In a possible plan to extend the Privacy Directive following the Facebook Beacon, the EU published a report. The report combines European and American experts in both the public and the private sector. The report “Security Issues and Recommendation for Online Social Networks”, written by the EU’s European Network and Information Security Agency, demonstrates the agency’s concern over the use of profile data after a user closes a personal account. If a


\(^{33}\) Users that share the same Facebook network or networks.

user deactivates an account, an email that is sent to the user to explain how to reactivate the account suggests that Facebook does not immediately delete the user’s information despite the fact that the user does not have access to his or her private data anymore, a practice that would be in contradiction to the standards of protection listed in the Privacy Directive.35

The Safe Harbour Agreement and the Facebook debate reveal the continued parallel development of incompatible practices and traditions in the EU and the USA. While territory itself is not posited as a central basis for argument in the legal negotiations surrounding the Safe Harbour Agreement, it is implicit in its construction and conclusions. Neither the EU, inclusive of its Member States, nor the USA government nor the US-based multinational corporations definitively altered their legal bases or traditional practices to be effectively compliant with another legal authority’s base or practice. During the negotiation and the final Agreement, those involved preserved rather than coordinated traditional practices and legal powers.

Works Cited


