The potentials and challenges of transitioning the U.S.-E.U. Safe Harbor Program from a hybrid system of authority to a pure non-state market driven (NSMD) system of authority:

Ms. Sarah Brennan, MPA, CUNY Hostos Community College
The potentials and challenges of transitioning the U.S.-E.U. Safe Harbor Program from a hybrid system of authority to a pure non-state market driven (NSMD) system of authority:

A guide for NSMD advocates

Sarah Brennan
Capstone 9199 – Cristina Balboa
Baruch College of The City University of New York
November 20, 2014
Contents
Abstract .............................................................................................................................................. 4
Introduction ......................................................................................................................................... 4
   Background ....................................................................................................................................... 5
   Safe Harbor ...................................................................................................................................... 6
   Non-state market driven (NSMD) framework .................................................................................. 8
II) Methodology .................................................................................................................................. 9
III) Analysis ....................................................................................................................................... 10
   Role of State ................................................................................................................................... 10
      Convergence ................................................................................................................................ 10
      Divergence ................................................................................................................................... 10
   Institutional Governance .................................................................................................................. 11
      Convergence .................................................................................................................................. 11
      Divergence ................................................................................................................................... 12
   Social Domain .................................................................................................................................. 12
      Facebook ....................................................................................................................................... 15
      Convergence .................................................................................................................................. 16
      Divergence ..................................................................................................................................... 16
   Role of Market .................................................................................................................................. 17
      Consumer/Producer Knowledge ..................................................................................................... 18
      Attitudes towards Social Action .................................................................................................... 19
      Market Flexibility .......................................................................................................................... 20
      Convergence .................................................................................................................................. 21
      Divergence ..................................................................................................................................... 21
   Enforcement ..................................................................................................................................... 21
      Enforcement and Sanctioning .......................................................................................................... 22
      Convergence .................................................................................................................................. 23
      Divergence ..................................................................................................................................... 23
   Discussion ........................................................................................................................................ 24
IV) Recommendations ....................................................................................................................... 24
V) Conclusion ..................................................................................................................................... 25
VI) References .................................................................................................................................... 28
VII) Appendices .................................................................................................................................. 32
   APPENDIX A: List of SHP Frequently Asked Questions............................................................... 32
   APPENDIX B: Select E.U. and U.S. Policies Impacting Digital Privacy ....................................... 33

Brennan, 2
European Union ........................................................................................................................................33
United States ........................................................................................................................................34
APPENDIX C: Newspaper Search ........................................................................................................36
APPENDIX D: Brief Summaries of 2011 Greece Protests and Occupy Wall Street in U.S. ..............40
Greece Protests ......................................................................................................................................40
Occupy Wall Street .................................................................................................................................40
VIII) Acknowledgements ..........................................................................................................................41
Abstract
The Safe Harbor Program (SHP) is an economic agreement between U.S. and E.U. which allows U.S. organizations to seamlessly access E.U. consumers online. The economic relationship between the two Unions is worth approximately $560 billion dollars per year. There is a policy gap in the level of protection each Union affords to digital information. The E.U. Commission has deemed that the level of protection in the U.S. is below adequate and therefore requires U.S. organizations to participate in the Safe Harbor Program. The SHP is a self-certification agreement created and administered by the U.S. Department of Commerce and E.U. Commission. More than 3,900 U.S. organization currently participate, and the program operates using a hybrid system of state and non-state authority. The question of this paper is whether transitioning the current hybrid system of operation to a pure non-state market driven system of operation would be a good idea. This determination is reached by using primary and secondary sources to qualitatively assess how well the five key features of Benjamin Cashore’s (2002) non-state market driven (NSMD) framework are represented in the current SHP agreement and operating environment. The role of state, institutional governance, social domain, role of market, enforcement, each, is evaluated and ranked within the context of SHP to identify where state and non-state authority appear. Convergence is recognized and divergence of each feature is weighted to account for its contribution to the integrity of the agreement. The ease or difficulty that might be encountered should a transition be made is also considered. The analysis shows that the current role of government coupled with the option to impose criminal sanctions is a benefit to this SHP international agreement. That determination stands in stark contrast to the type of NSMD authority expected with pure non-state market driven system. Further, the involvement of the U.S. and E.U. governments in this agreement is an element that is often faulted as lacking in other international agreements. The volatility of the modern digital environment, especially post Edward Snowden in the E.U., lends itself to opportunities to review and rebuild the SHP to replace some state driven features with non-state authority. The decision to do so, however, would have to be carefully analyzed to be considered a good idea. A set of recommendations are proposed to help conceptualize what a transition might look like and how easy or difficult a transition might be.

Introduction
The protection of digital information reflects the cultural value of privacy realized by a country’s regulatory environment (Tourkochoriti 2014). Regardless of its cultural importance however, protection of digital information remains difficult (Bowden, 2013; Jolly, 2014; Podesta et al. 2014). E.U. government has been put to the test regarding international privacy breaches as revealed by U.S. National Security Agency (NSA) agent Edward Snowden (Tourkochoriti 2014), and is equally challenged by consistency of intra-national application of privacy policies designed E.U government and regulated by the E.U. Commission Office of Data Protection Authorities (Bigo et al 2013). Breaches notwithstanding, the E.U. maintains comprehensive top-down policies of data protection directives; a policy which all third-countries wishing to do business with E.U consumers are expected to adhere (U.S.-E.U. Safe Harbor Overview, 2013). In E.U., privacy becomes contentious before others use information; permission must be granted first to proactively prevent harm (Tourkochoriti 2014).

The U.S. policy, on the other hand, reflects a sectoral approach (U.S.-E.U. Safe Harbor Overview, 2013). This approach holds businesses and organizations accountable for protecting and handling digital information. This approach reflects an open and democratic application of privacy protection that traditionally becomes contentious in debates emphasizing U.S. constitutional amendments such as the freedom of speech and freedom from illegal invasion (Tourkochoriti 2014). In U.S. the measure of harm caused by invasion of privacy or violation of speech is reviewed in hindsight. In other words, one raises concern after harmful incidents are threatened or occur (Ibid.).

**Background**

Legal and political culture shapes societal attitudes and understandings of privacy. The European Union has a series of elements in place that celebrate privacy and protect data. Starting with the E.U. Charter of Fundamental Human Rights (hereafter, Charter); article 7 describes privacy in terms of safety within family, property and person. Article 8 discusses data protection in terms of protection, treatment, transfer and use of personal data. Furthermore, it requires that individuals be notified of timing and purpose for which data are to be used and mandates that individuals be permitted to access collected personal data. Finally, article 8

---

1 The regulatory aspects identified by Tourkochoriti are fundamental presumptions, limits on contractual freedom, coverage of protection, difference in the weighing of values in conflict, definition of protected data, and enforcing authorities.
requires that data protection be regulated by independent authorities. Accordingly, the European Commission (hereafter Commission) enacted the 1995 Directives on Data Protection (DDP) and supports a staff of digital protection authorities (DPAs). The most recent limitation ratified by E.U. Parliament in May 2014 was the Right to Erasure; more popularly known as the Right to be Forgotten (Factsheet on the right to be forgotten ruling, 2014). The Right to Erasure gives E.U. citizens a legal path to requesting that personal information be removed from/erased from the Internet record.\(^2\) This recent E.U. policy places a state pressure on market forces.

Limiting access to digital information, also known as protecting data, is conceived of very differently in the United States. To begin with, the essence of privacy is extrapolated – not specifically stated - from the fourth amendment as defined by legal precedent.\(^3\) Accordingly, the 1968 Wiretap Act outlawed government invasion of individual privacy without warning or knowledge and was quickly reversed by the 1978/2008 foreign intelligence surveillance act (FISA) and its amendments which served to extend the authority and scope of secret government run surveillance. After the September 11, 2001 terrorist attack, the USA PATRIOT Act of 2001 was passed. This act was faulted as blank access of government surveillance to private consumer activity without limitation. Contrarily, some legal scholars argued that media hype overlooked the relatively small amount of change that actually characterized the differences between FISA and USA PATRIOT Act (Kerr, 2003). The PATRIOT Act was extended in 2011 (U.S. Department of Justice, 2014).\(^4\)

**Safe Harbor**

The Safe Harbor Program (SHP) was designed to bridge the gap between the E.U. top down comprehensive approach to handling and privacy of data and the U.S. sectoral approach to data protection and data privacy (U.S.-E.U. Safe Harbor Overview, 2013). Developed by the E.U. Commission (hereafter, Commission) and the U.S. Department of Commerce (hereafter Department of Commerce), the SHP was implemented in 2000 to maintain a digital economic relationship between the two Unions. The program allows for the transfer of digital information from E.U. consumers to U.S. businesses via Safe Harbor certification (Welcome to the U.S.-E.U. 2

---

\(^2\) The Internet is known as a system that uses “pens” instead of “pencils.” In other words, once information is posted publicly online, the text is virtually permanent.

\(^3\) The 1967 Supreme Court decision outlawed placing recording devices on public phone booths.

\(^4\) Appendix B shares brief information about policies addressing or alluding to digital privacy.

Brennan, 6
Safe Harbor, 2012). To be clear, SHP exists because E.U. Commission, the body responsible for E.U. interests abroad, judges the U.S. data protection policies as offering a below adequate level of protection (Ibid). E.U. digital markets represent a billion dollar industry. In 2010 alone, U.S.-E.U. data transfers resulted in approximately $560 billion with an additional $40 billion transferring between U.S. and Switzerland. “Data transfers are the lifeblood of many organizations and the underpinnings for all electronic commerce (Ibid.).” The Safe Harbor language emphasizes that even information transfer, to the exclusion of currency exchange, impacts an array of fields from banking, medicine and pharmaceuticals to travel and tourism, among others if withheld. Ensuring access to E.U. consumers is in the best interests of all U.S. industries.

The Safe Harbor Program operates using a hybrid system of state and non-state authority. Non-state authority is represented in many forms. The program has aspects of third-party and independent authority, otherwise categorized as private authority. Private authority is described by Tim Buthe’s book review “Private Authority and International Affairs (2003) “…as the attainment of legitimate power by ‘private’ actors that directly or indirectly work for profit: firms, business lobbies, industry associations and other ”corporate actors.” Additionally, market authority has a strong natural presence in the current system of Safe Harbor operations.

The representation of voluntary environmental management system (EMS) appears in this paper as a form of state authority. Voluntary EMS is defined by Stevens et al (2012) as “The need and ability of an organisation to manage and control its impact on the environment.” (p. 1). Applied holistically to the Safe Harbor program, EMS targets the Commission’s ability to govern and control the exchange of E.U. citizens’ digital information in online environments. Here, the public and private organizations that self-certify with Safe Harbor have jurisdiction over the manner in which internal business processes are adjusted to meet the needs specified by the SHP agreement. As will be discussed further in the analysis section, the U.S. and E.U. use SHP to establish clear expectations and requirements for certification, verification, and enforcement to control the engagement of organizations in digital relationships with E.U. consumers. The system is heavily vested in state authority. For example, Department of Commerce monitors submission of self-certification applications and annual renewals. The SHP agreement contains a healthy combination of market-based incentives and disincentives but is forceful in the
presence of state-based incentives and disincentives which include the possibility for imposing criminal sanctions.

Edward Snowden's revelations that U.S. was spying on its E.U. allies created a wave of distrust - among European allies. Headlines such as “After Edward Snowden’s revelations, why trust US cloud providers?” (Naughton 2013) ran in news media outlets across Europe. Further in consideration of Snowden’s possible impact on Safe Harbor, headlines look like this, “European Union: Prepare for Changes to the US-EU Safe Harbor” (Ray 2014). These types of allusions create the perception that change to the SHP may be possible. A transition to a pure non-state market driven (NSMD) system of authority may be exactly what is needed to rectify the existing hybrid system of authority.

Non-state market driven (NSMD) framework

The NSMD framework distinguishes itself from other systems of operation by its prescriptive ground level rules and procedures for actions associated with implementation and ultimately adherence to agreement guidelines (Auld et al 2007). The corrupted digital environment resulting from Snowden’s actions caused concern in the European Union and forced a re-examination of the Safe Harbor Program’s ability to manage the digital exchange of E.U. consumer information to U.S. organizations. As changes are being considered, non-state market driven advocates have an opportunity to conceptualize how the SHP agreement could work as a non-state market driven system.

The non-state market driven (hereafter, NSMD) model developed by Cashore in 2002, Cashore, Egan, Auld and Newsom in 2007 and examined more recently by Auld, Balboa, Bernstein, and Cashore (2009) has five key features: (1) role of state; (2) institutional governance; (3) social domain; (4) role of market; and (5) enforcement. The essence of the NSMD framework empowers actors (i.e. organizations) to rely purely on market forces. Intuitively, the nature of business involves consumer and producer supply and demand which is impacted by market conditions. Traditionally high technology costs have decreased in the recent past because of increased production of and demand for technology devices as well as

<table>
<thead>
<tr>
<th>Divergence</th>
<th>State Authority</th>
<th>Non-state Authority</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Presence</strong></td>
<td>High Divergence</td>
<td>Low Divergence</td>
</tr>
<tr>
<td><strong>Absence</strong></td>
<td>Low Divergence</td>
<td>High Divergence</td>
</tr>
</tbody>
</table>

Table A: Presence or Absence of NMSD Features
availability of and access to reliable global networks. Industries from accounting, construction and forestry to social media, education and travel, among others, have contributed to the widespread popularity of technological options. Cloud computing developments and affordability of mobile technologies render producers and consumers who choose to opt-out of technology at a disadvantage. These market forces - increased supply and ever-increasing demand - coupled with environmental disruption characterized by widespread feelings of mistrust and loss of control over digital information suggest a potential for the NSMD framework to positively impact SHP operations.

II) Methodology

This paper will qualitatively assess the U.S.-E.U. Safe Harbor Program agreement by using primary and secondary sources to determine if transitioning from the hybrid system of authority that currently characterizes the current SHP to a purely non-state market driven (NSMD) system of authority can contribute to a more reliable and sustainable system of operation. In this sense, the paper evaluates the current SHP environment by identifying where in the agreement NSMD features naturally occur and identifies challenges prohibiting a full transition. Moments of convergence and divergence will be explained for each of the five key features. Each divergence will offer a rank of low, medium, or high to capture the level of perceived ease or difficulty in replacing state authority with non-state authority. A high divergence represents a high level of perceived difficulty while a low divergence represents a perceived ease to transitioning. A medium rank represents the potential to shift after a series of steps. A general level of environmental readiness to accept a pure system of non-state authority will be judged based on the accumulation of threats to a full non-state market driven system of authority. Divergence will be ranked based on the natural presence or absence of the identified feature (Table 1) and on the proximity of those characteristics to the ideal NSMD framework (Table 2). The proximity represents a proverbial distance, if any, between existing operations and the ideal scenario. A low divergence rank will represent a strong natural presence of the NSMD feature implicating an easy transition to the NSMD framework (See Table 1). Conversely, a high divergence rank represents a low natural presence of the feature, or a challenging

<table>
<thead>
<tr>
<th>Rank</th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distance</td>
<td>Small</td>
<td>Proportional</td>
<td>Large</td>
</tr>
<tr>
<td>Transition</td>
<td>Easy</td>
<td>Middle</td>
<td>Hard/Difficult</td>
</tr>
</tbody>
</table>

Table 2: Rank, distance, and transition potential

Brennan, 9
roadblock, implicating a difficult transition (Table 1). A medium rank shows some conformity and implicates the possibility of transformation. A set of recommendations will be offered based on these outcomes.

III) Analysis
Role of State

Cashore et al (2007) describe the role of state as the level of government involvement in organizational activities. A pure NSMD system means that government plays no role and Auld et al (2009) explain that “… no one can be incarcerated or fined for failing to comply…” (p. 8). Strong presence of this feature means that SHP market forces dominate and organizations comply with SHP privacy principles and data protection directives guided by ethical principles and best practices. Currently, private authorities engage in verification and enforcement processes and businesses gain access to consumer markets by self-certifying compliance with governmental agencies. The incentive to participate in SHP is a market-based one: access E.U. consumer markets.

Convergence
Positive signs of conformity with NSMD include: allowing organizations the right to decide to self-certify and self-verify and requiring the involvement of third-parties in dispute resolution and enforcement. The self-conducted processes are fundamentally separate from government oversight showing natural alignment with the NSMD framework.

Divergence
Alternatively, submission of self-certification documents is made to a government authority. The Department of Commerce collects processing fees and updates a publicly accessible website listing all currently certified organizations. Moreover, dispute resolution requires involvement of government agents and encourages criminal sanctions in specific instances. For example, consumer grievances alleging mishandling of human resource data must be investigated in cooperation with E.U. data protection authorities (Safe Harbor Workbook, 2012). Additionally, organizations must notify the Department of Commerce of any third-party findings of violations.

5 The processes of verification and dispute resolution are enforcement features and will be discussed more fully in the Enforcement section of this analysis.
or assignment of sanctions, and third-party findings can be escalated to the attention of the Federal Trade Commission if suspicion of “illegal or deceptive practices impacting trade” arise (FAQ Dispute Resolution and Enforcement, 2012). The presence of state authority stands in stark contrast to the NSMD definition of role of state and receives a high divergence rank.

**Consideration**

The current language of the SHP agreement suggests that the level of involvement of E.U. data protection authorities in enforcement mechanisms may be unsustainable:

“The option of co-operating with the DPAs will be available to organizations joining the Safe Harbor during a three-year period. The DPAs will reconsider this arrangement before the end of that period if the number of U.S. organizations choosing this option proves to be excessive. (Role of Data Protection Authorities, 2012)

This administrative concern regarding the potential volume of investigations that could arise represents an opportunity to replace this important government process with third-party authority. This consideration could remove the presence of state authority and receives a medium rank.

**Institutional Governance**

Cashore et al (2007) describe institutional governance as influential systems characterized by “…adaptation, inclusion, and learning approaches… [which] are more democratic, open and transparent” (p. 8) than existing systems of governance. This means that binding agreements should be adjustable based on outcomes. Furthermore, the operating system should be able to change with relative ease. An environment ready to embrace institutional governance will reflect the ability to be successful in two areas: (1) engagement in continuous evaluation and assessment, and (2) commitment to implementing evidence-based solutions designed to strengthen operational shortcomings or adjust to environmental changes.

**Convergence**
There is a considerable level of evidence supporting the NSMD feature of institutional governance. There are several opportunities for self-reflection. Organizations must verify certification annually. Opportunities for the SHP to change are implicated in: (1) lack of direction related to an organization’s adoption of structural and operational processes aligned with SHP; (2) inherent willingness of the SHP agreement to change based on experience and learning over time. Moreover, the SHP informational materials show that organizations are entering a governance agreement with a clear purpose, structure, and plan for operation. These are all positive signs that the SHP system of institutional governance conforms to NSMD ideals.

**Divergence**

Governance belongs to the federal Union officials responsible for creating the program. State authority enacted this agreement; designed the system’s flexibility, and oversees enforcement among other processes. While noble and meaningful, state authority counteracts non-state authority. While involvement of state authority in program development is peripheral, the involvement of state authority in enforcement functions is central to SHP effectiveness.

There is a strong potential to replace state with non-state authority. Third-parties such as private or independent organizations could easily be prepped to serve in similar roles as state government utilizing non-state strategies to ensure smooth operations and large scale compliance. Although there is a strong potential to make this change, large scale compliance remains a question. There is an incomplete evidence regarding the reasons – market-based or otherwise - that organizations comply.

This feature ranks medium for its potential to transition more fully to a system of non-state authority; however strong the presence and impact of state authority is currently.

**Social Domain**

Cashore et al (2007) and Auld et al (2009) describe social domain as an approach to “developing prescriptive rules to which firms must adhere” (p. 188). The scholars explain that the rules developed may require “profit-maximizing firms to undertake costly reforms that they otherwise would not pursue (Cashore et al, 2007, p. 8; Auld et al, 2009, p. 188). The NSMD social domain distinguishes itself from other frameworks such as: (a) private authority and (b) voluntary environmental management systems. An example of private authority is an independent business exercising discretion to implement technological solutions for reasons explained by profit maximizing behavior such as streamlining processes, lowering costs, and
maximizing profits. (Auld et al, 2009, p. 188; Cashore et al, 2007, p. 8). Alternatively, voluntary environmental management systems (EMS) can be described as systems that work to certify organizations which develop internal procedures for handling affairs, but which develop no prescriptions about implementation behavior (Ibid.). The existing Safe Harbor Program agreement emulates voluntary management and private authority. One illustration of profit maximizing behavior is participation in SHP to gain access to E.U. consumer markets. Application of NSMD social domain opens a discussion of existing prescriptive rules and processes.

First, there are a number of prescriptive rules and procedures related to SHP agreement. The SHP workbook outlines E.U. privacy principles and directives on data protection; the benefits of implementing the agreement; direction on which organizations may/should join and how to join; consequences for persistent failure to comply; compliance with verification and dispute resolution and list procedures (Safe Harbor workbook, 2012). The fifteen FAQs broaden the scope of SHP agreement starting with issues ranging from sensitive information, journalistic exception, and secondary liability (FAQ 1, 2, 3 respectively) (U.S.-EU Safe Harbor Framework Documents, 2013). Examples of prescriptive procedures include self-certification, verification, dispute resolution, and enforcement requirements; requirements to adhere to legally binding sanctions; right to withdrawal at any time on either side of the contract; requirement to maintain agreement parameters even after withdrawal, suspension, or decertification; requirement to renew annually and notify Department of Commerce for failure to comply and of assigned sanctions (Safe Harbor workbook, 2012).

After reviewing the Safe Harbor materials, a gap is found in prescriptive rules offered to organizations regarding internal processing and handling of E.U. data. For example, the SHP does not offer specific methods of processing E.U. data which could be different than methods used to handle U.S. data (Safe Harbor privacy principles 2009). There are no prescriptions for this “on the ground activity” other than mandated compliance with Safe Harbor requirements.

Presumably, organizations prefer to make adjustments to ensure access to E.U. consumer markets. Verification presents an opportunity to review organizational compliance. The current agreement allows for in-house verification perhaps due to potential expenses associated with annual renewal which includes verification. The potential expense associated with third party

6 The full list of FAQs appear in Appendix A.
verification may be one reason the agreement allows organizations to opt for self-verification. Intuitively, expense issues pose more problems to smaller less lucrative companies; however, approximately 83% (3,253/3906) of certified organizations chose in-house verification (U.S.-E.U. Certification List). This raises questions related to ease of compliance and, separately, an organization’s potential engagement in deceptive practices as a rule. Facebook is a high earning organization and opts for in-house verification. Assuming expense is not an issue, other concerns arise.

Facebook’s self-certification profile indicates in-house verification (Safe Harbor List, 12/19/2014). Ideally, verification is an objective measure of an organization's compliance with SHP. The seven SHP privacy principles are notice, choice, onward transfer, security, data integrity, access, enforcement; and the seven DDPs are data quality, legitimate data processing, sensitive data, security, data controllers, government data protection authorities, and transfers of data outside E.U. Each principle and directive is defined and a verification statement declares that an organization complies with these and all other requirements of the agreement.

A brief review of Facebook’s privacy policy relative to the SHP privacy principle of “choice” helps show how grey areas can arise during self-verification. This review provides a general sense of the time and commitment involved in conducting a verification process. The SHP privacy principle of “choice” is defined:

An organization must offer individuals the opportunity to choose (opt out) whether their personal information is to be disclosed to a third party, or to be used for a purpose that is incompatible with the purpose for which it was originally collected or subsequently authorized by the individual. Individuals must be provided with clear and conspicuous, readily available, and affordable mechanisms to exercise choice…individuals who do not wish that their data be used as described in the privacy policy can choose not to have their data shared…” (Safe Harbor Workbook, 2013)

There seems to be a public consensus that users who don’t agree with Facebook’s data collection processes must decide not to participate at all in the social media platform (C. Balboa, personal communication, October 2014). The SHP agreement clearly positions choice as an alternative to opting out of data collection while maintaining an opportunity to participate in the online

7 This data was accurate on 10/30/2014 and may have changed. The website is regularly updated and tracks the status of all organizations, both, new and old.
platform. If Facebook is to allow users to opt-out of data collection and still use the social media platform, it may imply a fundamental change to Facebook operations. This may or may not be costly. It is unclear whether Facebook operationalizes different data handling procedures for E.U. data. The language of the data use policy suggests there is no difference between data handling once a Facebook account is created.

**Facebook**

Facebook’s privacy policy, a.k.a. data use policy, is written using simple language and is presented in a user-friendly format as required by the Safe Harbor agreement. Facebook expresses its alliance with Safe Harbor in a section titled, “Other Things You Need to Know.” Facebook makes sure to display prominently compliant filing procedures which vary for non/U.S./Canadian users (Data use policy, 2013).

When taking a closer look, web-users are introduced to a section called “Information we receive and how it is used.” The first sub-section is, “your information.” Facebook explains “your information” as “the information that's required when you sign up for the site, as well as the information you choose to share.” Facebook positions choice as “choosing” to set up an account. Registration information required to set up an account is classified as information that is always public.

The second section of “information we receive…” is titled “public information” and begins with the subsection “information you choose to make public.” This section includes a screen shot of privacy options including options to share information with “everyone,” “friends,” or “custom.” The second subsection is titled “information that is always public” and appears to serve as a disclaimer explaining that information that is always public includes profile fields not limited by name, profile pictures or cover photos, networks, gender, and username and user ID.

---

8 A quick link to Facebook’s privacy policy is accessible via the Safe Harbor List of Organizations site located https://safeharbor.export.gov/list.aspx by entering Facebook in the Organization search field. Facebook’s privacy policy is also accessible by clicking on “Terms” at the bottom of Facebook’s homepage. Privacy policy is accessible without having to create a Facebook account. The site contains easy to read language and navigation through the policy is equally simple.

9 Similarly, Facebook notifies users regarding its willingness to cooperate with U.S. authorities with regard to information access in instances of reasonable suspicion of illegal activity. https://m.facebook.com/policy?page=other&refid=41. Accessed 11/13/2014. For a larger discussion of information surveillance between EU and US see Casper Bowden’s report entitled, Impact of U.S. Surveillance on EU Citizens” [check title]
and other registration information which includes email address, birthday, and gender. Aside from the loss of control over privacy of profile information, some of the categories that are always public could potentially cross into the DDP protection of “sensitive data” including identification of gender (i.e., sex life).

The third section of the data use policy is “how [Facebook] use[s] the information we receive about you.” Facebook elaborates its intentions to use information received to protect rights or property, provide location features and services, understand and measure ad effectiveness, make suggestions to consumers, analyze data, conduct research, and make operational improvements, among others (Information we receive and how it is used, 2013); but, does not seem to separate E.U. citizens from its general population nor present an opt-out of data collection options. Alternatively, a separate section was located for California residents (Some other things you need to know, 2013). The final section is “Deleting or Deactivating Your Account” which allows users to stop using or have an account suspended or deleted. The data use page does contain a “sharing and finding you on Facebook link” which provides more specific directions regarding privacy settings and privacy options to general web browsers which does not require creation of an account to access.¹⁰

**Convergence**

The NSMD definition of social domain depends on two characteristics: (a) the presence of prescriptive rules and procedures; (b) the ability of the established structure to force organizations to make costly reforms when necessary. With a caveat, the SHP agreement perfectly fits with these two components. The agreement shares a host of prescriptive rules that are flexible enough for organizations to adapt and implement in context of their own business principles and practices. As explored in the case of Facebook, organizational adherence to structural guidelines is possible.

**Divergence**

The problem lies in the ability of the system of authority to force organizations to make potentially costly reforms. Self-verification poses a conflict of interest that may lead to grey areas of compliance and unless influential stakeholders such as Facebook are publicly committed

---

to upholding high standards of compliance there is no reason to assume widespread compliance without meaningful consequences for non-compliance. Without fully understanding the motivations behind compliance, state authority and possible criminal sanctions may serve as strong incentives to comply.

Again, the presence of state authority challenges a transition to non-state authority. The sheer volume of organizations certified with Safe Harbor creates conditions conducive to change. There are 3,910 organizations (as of December 19, 2014) certified with Safe Harbor which means an overwhelming number of organizations potentially requiring state-based intervention. Here again, replacing state authority with private/independent authority raises an important thought for consideration.

Finally, there is little prescription regarding methods of changing handling procedures to address the needs detailed in the SHP. The program could create language that would appropriately prepare and guide organizations on methods of differentiating data handling procedures relevant for E.U. and for U.S. data.

For these reasons, this feature receives a medium rank for the many instances of naturally occurring market-based prescriptive rules that stand alongside the many instances of state-based authoritarian involvement. There is a valid opportunity to strengthen existing prescriptive rules and create new ones that more forcefully guide ‘on the ground’ behavior.

Role of Market
The fourth key factor of the NSMD operation is role of market. Auld et al (2009) explain that this feature “accesses authority through the market’s supply chain” (p. 189). So where government is expected to have no authority, the role of market grants total authority to producers and consumers (Cashore et al, 2007; Auld et al, 2009). The ideal environment is depicted when producers respond immediately to consumer needs and consumers react immediately to environmental changes. Further, producers and consumers use their powers to act and influence others to act for the greater good (Green, 2013). Success in this feature relies on

---

market knowledge defined by consumer and producer ability to be informed and to mobilize as necessary using direct political actions such as boycotts or protests (Auld et al 2009). Market flexibility is characterized by the ability of producers and consumers to respond immediately to demand.

**Consumer/Producer Knowledge**

Consumer and producer knowledge (i.e. market knowledge) must be coupled with collective action to achieve market pressure. For consumers to act collectively a strong base of support - containing either a large number of individuals or a small number of key stakeholders - is required. Consumer knowledge is critical and the Internet and media outlets serve as important conduits for achieving widespread awareness and support. Due to time constraints, a limited selection of popular print with online access newspapers were examined to determine media effectiveness related to mass education and mobilization of citizens in U.S. and E.U. A general search of popular online newspapers in E.U. and U.S. was conducted to examine the number of hits arising in news articles and news-items using the following search terms: “information privacy,” “concern over information privacy,” “social media,” and “concern over social media.” The search terms were translated using Google translate.

With the exception of The Guardian which provided more than three million hits to the search term “concern over information privacy” the search terms resulted in more hits in U.S. media sources (Table 4). Steve Holland (2014) - studying E.U. reaction to invasion of digital privacy - compared the level of media attention and citizen interest within individual E.U. countries. Holland noted higher levels of media attention in countries like Estonia, Germany, Netherlands, Sweden, and lower levels of interest in England which seemed non-reactionary or France which seemed surprised by the outrage. Erlanger (2013) points to experience with Nazism as the reason for high levels of interest expressed in Germany. Intuitively, high levels of interest align could align with high levels of collective action; however Holland explains that this wasn’t the case in E.U. countries. Holland notes that even in areas where media outlets provided exhaustive coverage of topics related to information privacy low levels of public action remained. Holland attributed the low level of collective action in Estonia, for example, to political conceptions that invasion of privacy is a natural consequence of global digitalization. Generally, the media has a strong track record in both Unions for promoting mass education on a
wide range of topics as would be expected. The Internet serves as an important tool for access and promotion of public education.

**Attitudes towards Social Action**

**European Union**

Hoskins et al (2012) studied political participation in 54% of E.U. member countries (15/28) and found that E.U. citizens in Western Europe (15-30%) were more likely to participate in protests than E.U. citizens in Eastern Europe (below 10%). Further the researchers controlled for age and found that 25% of youth are likely to participate in political protest suggesting an increase in willingness to engage. Finally, whereas citizens reported a relatively strong disinterest in political protests, more than 60% of E.U. citizens in Western Europe expressed willingness to sign a petition or collect signatures. In Eastern Europe those numbers fell to 15%. These outcomes represent a wide range of interests and willingness to participate politically and generally imply a tendency to be part of more passive than active political activity. Hoskins et al. (2012) acknowledges that the survey results exclude recent events illustrating higher levels of participation in political protests across Europe and they anticipate an overall increase in market willingness to participate moving forward.

EuroStat (2010) offers a set of statistics related to E.U. concern over information privacy, over problems related to Internet usage. Seventy-eight percent of respondents who used the Internet in 2009-2010 expressed strong or mild concerns. To illustrate, 29% of E.U. citizens refrained from sharing personal information in online social media communities (Ibid).

**United States**

The Pew Research and Associates 2012 survey regarding civic engagement in political activities show small percentages of citizens participating in political rallies (6%), volunteering for political parties/candidates (7%), or becoming members of influential public policy groups (13%). Engagement rates start to increase when political participation emphasizes community issues as well as issues of personal interest. Twenty-two percent of respondents attended political meetings on local, town or school affairs; 35% worked with fellow citizens to solve community problems. However, 52% of respondents noted not doing any of the named activities (Internet and American Life Project, 2012). There are relatively low levels of direct-action in community issues and an even lower level of participation in political activities. The ability of U.S. consumers to place pressure on the market supply chain is questionable.
The 2014 PEW report addresses concerns over information privacy in U.S. When asked about control over data, 91% of respondents agreed or strongly agreed that consumers have lost control over how personal information is collected and used by companies; 74% disagreed or strongly disagreed that anonymity was easy; 71% were concerned that information shared on social networking sites might be accessed by government without user knowledge; and most interestingly 61% feel that not enough is being done to protect privacy and feel like they would like to do more. Taking into consideration the generally low levels of engagement in political activity, the 61% who “feel like they would like to do more” may or may not challenge policy makers (Gfk, 2014). When these statistics are considered alongside the scenario described by “Occupy Wall Street” and “Hands Up, Don’t Shoot,” the ability to place pressure on the market supply chain stands at the middle of the road. The U.S. public has shown an ability to respond to issues deemed important to a wide range of individuals, yet shows a general disinterest in political activity which is similar in E.U.

**Market Flexibility**

Another element that is crucial to NSMD success is market flexibility and ability of consumers and retailers to respond immediately to environmental concerns. The NSMD framework distinguishes itself from government involvement based on its ability to respond immediately to environmental indicators and changes. In this way, NSMD counter-acts government’s traditionally slow pace of change (Auld et al, 2009). The fast pace of technological change plays a key role in consumer markets. Governments like E.U. and U.S. have been heavy investors in technological infrastructure that is global in scope (Bowden, 2013). The empowerment of technological companies to be innovative has led to widespread development of software, cloud computing, and mobile hardware and applications (Sullivan, 2014). The proliferation of devices and computing capabilities has effectively decreased production and consumption costs helping the Internet to boom and access to spread like wildfire.

The nature of open access that characterizes the Internet allows frequent interaction between players in the market. Complete industries have arisen tailored to online interactive environments (i.e. social media platforms); to access and analyze online interactions (McNeely and Hahm, 2014); to update archaic processes with digital capabilities. The Internet is so popular and so efficient that non-digital industries are pressured to change practices to include digital...
features. Frequent online participation helps producers and consumers adjust more appropriately to market preferences and needs.

**Convergence**

An NSMD model requires the presence of effective mechanisms for maintaining a minimum level of market knowledge. Media outlets (i.e. newspapers) and the Internet serve as important mediums to filling that function. Each entity helps inform public actors by raising awareness of important issues and opportunities. The Internet allows for individual exploration of competing and dovetailing ideas and encourages collaborative dialogue and exploration of different viewpoints. NSMD market participation demands an informed consumer/producer base as does the SHP.

Market flexibility governs NSMD and flexibility is the rule in online environments. The fast pace of change without a clear road map of what’s ahead is often the complaint of consumers and producers. Furthermore, Safe Harbor does not restrict organizations from tailoring practices to align with their own business preferences.

**Divergence**

Market based disincentives, such as public collective action, that would call consumers and producers to pressure the market supply chain is weak in European Union and United States markets, both. The fundamental design of an open Internet inherently threaten privacy of digital information. Faster Internet uses “digital cookies” and “cache” to store previously viewed websites which are stored for quicker retrieval (Sullivan, 2013). Cloud-based computing creates opportunities for accessing personal information, collaborating on projects with colleagues, and sharing photos and experiences with any users granted permission, but relatively few rules exist to regulate it (Ibid.). Consistent end-user experience depends on translatable computer programming language and reliable infrastructure that once implemented results in an environment so interconnected that it is difficult to change (Podesta et al 2014, Sullivan, 2014). These limitations on producers and consumers ability to control the market call on the power of state authority. For these reasons, there is a high level of divergence in this feature.

**Enforcement**

The fifth NSMD feature is enforcement. Enforcement is described as the “existence of verification procedures designed to ensure that the regulated entity actually meets the stated
“verification is important because it provides the validation necessary for a certification program to achieve legitimacy” (p. 189). In the NSMD system where role of state has no authority and market has full authority, the enforcement plan becomes critical. The NSMD feature calls on market driven enforcement, and for the SHP this means that the market incentives must be enough that the benefits of compliance outweigh the costs of noncompliance. “Auld et al (2009) further explains that “pressure along the market’s supply chain encourages compliance” (p. 189). In other words, NSMD empowers consumers and producers to be agents of change. To measure the proximity of the ideal NSMD feature in current operating system, the following points will be elaborated: (a) the type of enforcement features in the existing agreement (b) types of sanctions. Similar to role of market, enforcement relies on market action and so uses part of the analysis of the role of market to help determine the rank for this feature.

**Enforcement and Sanctioning**

The SHP has a clearly identified component of enforcement. SHP enforcement consists of three parts: verification, dispute resolution, and sanctioning. Verification involves measuring an organization’s performance related to its handling of personal digital information in ways that align with the SHP principles. From this measurement, the organization is declared to be in compliance or noncompliance. Verification offers organizations the option to conduct self-assessments or use an independent third party. Verification statements are submitted with the annual certification request/renewal.

Another aspect of enforcement is dispute resolution. The SHP workbook offers clear guidance about the manner in which organizations develop plans to confront consumer complaints. The SHP strictly requires organizations to contract with third-parties to process arbitration and mediation proceedings. Additionally, as was mentioned, organizations must work with E.U. data protection authorities (DPAs) when addressing specific allegations of mishandling of human resources data. Organizations must comply with any sanctions assigned in confirmed cases of misconduct.

The third aspect of enforcement is sanctioning. The agreement details examples of possible sanctions not limited by: suspension or loss of seal, inability to recertify, publicity of non-compliance, or erasure of data. The SHP agreement empowers third-parties to vary sanctions.
based on severity and type, and to escalate their findings to the Federal Trade Commission if there is evidence of illegal or deceptive trade practices.\textsuperscript{12}

\textbf{Convergence}

First, the NSMD model demands that a plan for active and effective enforcement of standards. The SHP agreement publicizes a system for enforcement that covers three areas: compliance audit or verification, dispute resolution steps for handling public complaints, and sanctioning or imposing accountability for noncompliance. This strongly aligns with the NSMD definition of enforcement.

Second, the NSMD model requires market-driven sanctions compared to state or criminal sanctions. Illustrations of market-driven sanctions include incentives such as price premiums, market access or a license to operate. Conversely market-disincentives include boycott campaigns or public shaming (Auld et. al, 2009, 189). The SHP documents that those types of market-driven sanctions are the first step for assigning sanctions to Safe Harbor certified organizations found in violation. For example, organizations that fall out of compliance are listed with a ‘not current’ status for the web-browsing public to see. These key indicators show an important alliance with non-start market driven authority.

Third, there is evidence, albeit low levels, of citizen willingness to take action which is required to place pressure on the market supply chain. Public action is important for market-driven compliance. As the U.S. polls show, citizen interest in taking action changes when issues impacting individuals directly arise.

\textbf{Divergence}

As discussed, there is a heavy-handed role for state authority in enforcement processes. The ability to escalate cases of digital handling violations to state-level authority for consideration of criminal sanctions actually strengthens the consequences of non-compliance. As stated, state-based options threaten a potential transition to NSMD authority.

Moreover, the low willingness to participate in civic or political activities raises a weary threat. This concern targets the core of NSMD operations meaning that consumer and producer

\textsuperscript{12} The Department of Commerce is responsible to enforce section 5 of its policy which prohibits illegal or deceptive practices that impact trade. If third-parties suspect this type of violation they are required informants: http://export.gov/safeharbor/eu/eg_main_018383.asp. Accessed 11/11/2014

Brennan, 23
culture of disengagement must change for an NSMD model to work effectively. Unless NSMD advocates can convincingly conceive of how the weaknesses in the market forces can be strengthened, this barrier could prevent a further transition to an NSMD model. For these reasons, divergence in enforcement receives a rank of high.

**Discussion**

Generally speaking there is a mixture in the presence of non-state authority in the existing Safe Harbor Program. There are clear instances of divergence that target the core purpose and design of the non-state market driven model. Heavy government involvement coupled with low levels of consumer participation in direct action as well as the complexity of the open Internet environment signify substantial obstacles to overcome. The role of state within its own definition and its reach into the enforcement feature coupled with the concerns raised in the role of market suggest the need for complex and sustained public initiatives to transition the existing agreement successfully. Instead the following recommendations will be made to help change advocates prepare the argument for transition.

**IV) Recommendations**

The analysis reveals a sharp dichotomy that threatens the success of a transition from the current hybrid system of authority to a pure non-state market driven system of authority. The primary challenge lies in the natural presence, strength, and value of state authority. Because the distance between the current and the ideal environments is steep, one recommendation will be made per feature. The following recommendations suggest a plan for brainstorming and formalizing the conceptual work that would leverage theoretical challenges with transitional success.

First, non-state market driven authority must be convincingly conceived of to be as powerful as state authority in the role of state. The potential for state authority to impose criminal sanctions may trump other market-based incentives to comply. A strong plan for imposing market-based disincentives must be able to hold accountable even the most influential stakeholders. A plan to engage the most influential stakeholders must be devised.

Second, institutional governance must be replaced by non-state third parties.Both federal Unions played important roles in establishing the SHP program and designed the program to be
responsive and relatively easy to change. A comprehensive plan for engaging independent and private parties in roles that the state traditionally was responsible for is required. The plan should address aspects of leadership development, volume and expansion of talent and preparedness for engaging leadership roles, funding, training, and transition from state to non-state authority.

Third, the social domain requires a plan that includes increasing third party verifications, training all organizations that opt for self-verification, and developing prescriptive standards for ‘on the ground’ behavior to ensure that organizations change procedures, if necessary, when handling of E.U. data.

Fourth, key media outlets across both Unions will have to formulate and implement comprehensive plans designed to promote the: importance of political activity as civic responsibility and safety from criminal sanctions or political persecution that has been known to result from publicly pressuring the market chain of supply and demand. As parties feel more empowered to act and react the role of market will become the powerhouse it is meant to be in a non-state market driven system of authority.

Finally, enforcement, a critical component in non-state authority, must compel all organizations to adhere to the agreement. Many of the current aspects of enforcement align naturally with non-state authority. Substantial thinking about the replacement of criminal sanctions with market based disincentives must occur before making a change. A transitional plan considering Walmart as an example of a non-state key stakeholder (Green 2013) should include the possibility of returning to a hybrid system of authority were a non-state system of authority not work in the intended ways.

V) Conclusion

The Safe Harbor Program contains many characteristics that reflect a non-state market based framework. The governance structure is designed to change based on learning over time. There are numerous prescriptive rules and processes that guide organization’s compliance activities. Online access and ability to change in the current digital environment is instantaneous. The NSMD model suggests that the ability of consumers to pressure the market supply chain is critical to the success of the system. A knowledgeable and motivated public characterizes NSMD operations. The ability of the news media and the Internet to educate market players about digital privacy is strong. The system of enforcement showcases an important role for market-based incentives and disincentives. The program also houses a substantive role for state
authority. This authority may strengthen the resolve of organizations to comply with Safe Harbor provisions. However effective, the state authority appears as a polar opposite to the NSMD framework which requires the absence of state authority, and relies solely on non-state authority and market driven forces.

On the flip side, media analysts show that even though public interest may be high, the likelihood that consumers will engage in direct action, such as boycotts or protests, are low in both Unions. Recent social movements - such as austerity protests in Greece and Occupy Wall Street in the U.S. – illustrate market driven pressure (See Appendix D). Overwhelmingly however, the evidence shows a general lack of interest among citizens to engage in political activity.

Verification, dispute resolution and sanctioning factors strongly align with NSMD types of market based enforcement. Government plays an important role however and must be carefully examined to determine if an equally effective alternative can be implemented. Weak attitudes on the part of producers and consumers, generally, towards political participation threaten the success of a full transition to NSMD authority. In terms of transition, consumers and producers would have to modify their traditional practices of engagement in politics. Logically, this type of cultural change would take a tremendous amount of resources, support, and time.

The current perception of instability in the digital environment - post Edward Snowden – presents a perfect opportunity for NSMD advocates to showcase plans for change. More specifically, NSMD advocates can detail how third-party authority could replace state authority. Before doing so, removal of state authority must be carefully considered. State authority is an element that can give an agreement what it needs to ensure compliance. It is also an element that other international agreements may lack and which could be perceived as critical component to success.

Although resulting in a challenging proposition to make a true NSMD transformation, the justification for this exploration is that there are so many naturally occurring NSMD components in the Safe Harbor Program that thinking about a full transition seems worthwhile. Jessica Green (2013) found Walmart, a non-state authority, to be more effective than government, or state authority, in reducing carbon emissions within manufacturing industries. In *Rethinking private authority: Actors and entrepreneurs in global environmental governance*, Green shows how Walmart uses its independent influence, power, and authority to shape environmental decisions.
of other organizations. If state authority is to be replaced effectively, NSMD advocates like Benjamin Cashore, Graemae Auld, Cristina Balboa, Steven Bernstein, Elizabeth Egan, Jessica Green, and Deanna Newsom are the scholars who best understand the strengths of the framework and how it best works in industries across the globe. To be sure, a transition is not an afterthought rather is an important concept to proactive consider in context of the U.S.-E.U. Safe Harbor Program. Based on NSMD success in other environmental industries, this option has tremendous potential to make a powerful impact on the Safe Harbor Program as well as on other international agreements.
VI) References


Running Head: Safe Harbor - From a hybrid to non-state market driven system of authority


Brennan, 29


**VII) Appendices**

**APPENDIX A: List of SHP Frequently Asked Questions**

Complete descriptions of each question are accessible online:

http://export.gov/safeharbor/eu/eg_main_018493.asp

1. Sensitive Data
2. Journalistic Exceptions
3. Secondary Liability
4. Investment Banking and Audits
5. The Role of the Data Protection Authorities
6. Self-Certification
7. Verification
8. Access
9. Human Resources
10. Article 17 Contracts
11. Dispute Resolution and Enforcement
13. Travel Information
14. Pharmaceutical and Medical Products
15. Public Record and Publicly Available Information

APPENDIX B: Select E.U. and U.S. Policies Impacting Digital Privacy

European Union

**1980 Protection of Privacy and Trans-border Flows of Personal Data Recommendations**


http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderfl owsofpersonaldatalhtm

“The development of automatic data processing, which enables vast quantities of data to be transmitted within seconds across national frontiers, and indeed across continents, has made it necessary to consider privacy protection in relation to personal data. Privacy protection laws have been introduced, or will be introduced shortly, in approximately one half of OECD Member countries (Austria, Canada, Denmark, France, Germany, Luxembourg, Norway, Sweden and the United States have passed legislation. Belgium, Iceland, the Netherlands, Spain and Switzerland have prepared draft bills) to prevent what are considered to be violations of fundamental human rights, such as the unlawful storage of personal data, the storage of inaccurate personal data, or the abuse or unauthorised disclosure of such data.”

**1995 Directives for Data Protection**
*From SearchSecurity.co.uk
http://searchsecurity.techtarget.co.uk/definition/EU-Data-Protection-Directive

“EU Data Protection Directive (also known as Directive 95/46/EC) is a directive adopted by the European Union designed to protect the privacy and protection of all personal data collected for or about citizens of the EU, especially as it relates to processing, using, or exchanging such data. Directive 95/46/EC encompasses all key elements from article 8 of the European Convention on Human Rights, which states its intention to respect the rights of privacy in personal and family life, as well as in the home and in personal correspondence. The Directive is based on the 1980 OECD "Recommendations of the Council concerning guidelines governing the protection of privacy and trans-border flows of personal data."

**Right to Erasure**

The Cecile Park publishing group (2013) confirms explains the right to erasure:

“require[s] the data controller to take all reasonable steps to have individuals' data erased, including by third parties 'without delay', for the personal data that the controller has made public 'without legal justification'. Under Article 17, data subjects are granted the right to 'obtain from the controller the erasure of personal data relating to them [...] and from third parties the erasure of any links to, or copy or replication of that data', where the data are no longer necessary in relation to the purposes for which they were collected, that individual withdraws consent or objects to the processing of his/her personal data, or where the processing of such data contravenes other parts of the Regulation.

**United States**

*First Amendment – Freedom of Speech*

Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the Government for a redress of grievances.

*Fourth Amendment – Right to Due Process*
The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.

1968 Title III Wiretap Act
*From U.S. Justice Information Sharing – Privacy and Civil Liberties

https://it.ojp.gov/default.aspx?area=privacy&page=1284

“Congress passed Title III in response to congressional investigations and published studies that found extensive wiretapping had been conducted by government agencies and private individuals without the consent of the parties or legal sanction. Congress found that the contents of these taped conversations and the evidence derived from them were being used by government and private parties as evidence in court and administrative proceedings.”

1978 Foreign Intelligence Surveillance Act (FISA) and 2008 FISA Amendments
*From U.S. Justice Information Sharing – Privacy and Civil Liberties

https://it.ojp.gov/default.aspx?area=privacy&page=1286

“FISA was initially enacted in 1978 and sets out procedures for physical and electronic surveillance and collection of foreign intelligence information. Initially, FISA addressed only electronic surveillance but has been significantly amended to address the use of pen registers and trap and trace devices, physical searches, and business records.”

Electronic Communications Privacy Act (ECPA) of 1986
*From U.S. Justice Information Sharing – Privacy and Civil Liberties

https://it.ojp.gov/default.aspx?area=privacy&page=1285

“The ECPA, as amended, protects wire, oral, and electronic communications while those communications are being made, are in transit, and when they are stored on computers. The Act applies to email, telephone conversations, and data stored electronically.”

*From U.S. Justice Information Sharing – Privacy and Civil Liberties

http://it.ojp.gov/default.aspx?area=privacy&page=1281
“The USA PATRIOT Act modified many major U.S. intelligence, communications, and privacy laws, including: The Electronic Communications Privacy Act (EPCA), which modifies Title III of the Omnibus Crime Control and Safe Streets Act (the Wiretap Act); the Foreign Intelligence Surveillance Act of 1978 (FISA); and the Communications Act of 1934.”

APPENDIX C: Newspaper Search

The 4International Media and Newspapers (4imn) rank European newspapers based on popularity. The ranking system is based on two algorithms: (1) page rank which determines the level of importance of pages and links on a newspaper site and (2) Internet traffic which tracks the frequency with which pages are accessed by the web browsing public. Together both algorithms determine the popularity of a given newspaper.

Popularity as determined by the 4imp.com ranking describes elements associated with circulation. The U.S. newspapers are ranked by numbers associated with circulation. Whereas Europe uses the term popularity, the U.S. uses the term circulation (Alliance for Audited Media, 2013; Associated Press, 2013). The 2013 ranking by Alliance for Audited Media was used to select among the top 10 U.S. newspapers.

The European newspapers selected for analysis include: The Guardian (United Kingdom), El Mundo (Spain), Bild (Germany), and Le Monde (France). Their respective rankings are 1, 4, 8, and 10. Two of these sources showed two separate publications. All four websites were used for those two sources: Le Monde, Le Monde Diplomatique, Bild der Wissenschaft, and Bild Zeitung. Each of the European newspaper websites were accessed using the link to worldpress.org through the Baruch College ‘research guide’ ‘news database’ at Newman Library online. To be clear, the tab ‘newspaper websites’ on the ‘news database’ landing page houses a Directory section that includes the link to “worldpress.org – World newspapers and magazines.”

The site allows users to search for individual newspapers sorted by country and does not include links to United States newspapers. The U.S. newspapers selected for analysis were: USA Today (Virginia), Wall Street Journal (New York), Los Angeles

14 http://www.worldpress.org/gateway.htm
Running Head: Safe Harbor - From a hybrid to non-state market driven system of authority

Times (California), and Houston Chronicle (Texas). Their respective rankings are 1, 2, 4, and 10.

Search
Each of the selected European newspapers had active links accessible through worldpress.org. The U.S. newspapers were accessed from the general Internet environment using Google to access each newspaper homepage. The selection of newspapers in Europe\(^{15}\) and United States was intended to achieve: (a) cultural diversity among readership audiences and (b) target the most popular or most heavily circulated newspapers. A search for articles containing keywords were entered into the ‘search’ feature found on the newspapers homepages. The four keywords/phrases used were: concern over information privacy, information privacy, concern over social media, and social media.\(^{16}\) Social media is a content area that requires data protection.\(^{17}\) The number of articles that resulted from the keyword searches are noted in Table 1.

The goal of the searches was to make a general statement about the strength of the media to inform or mobilize individuals regarding information privacy or social media. Social media was selected for its natural popularity in popular culture in both E.U. and United States. In this sense, where the issue is already popular, this paper studies the power of the media to pick-up issues and present them publicly for informational or reactionary responses. The ability to inform and mobilize individuals will be required if the NSMD role of market is to take hold of SHP processes. Many of the papers examined have global readerships.

Search Terms and Translations

- **English:** concern over information privacy
- **French:** préoccupé par la confidentialité des informations
- **German:** besorgnis über informationen privatsphäre
- **Spanish:** preocupación por la privacidad de la información

- **English:** information privacy

\(^{15}\) All selected European papers are published in countries that participate as members of the European Union.


\(^{17}\) Other terms that researchers could use in similar searches include, with and without ‘concern over’ as a preface, educational, human resources, medical, or travel data. See SHP FAQs as well as Podesta et al.

Brennan, 37
Running Head: Safe Harbor - From a hybrid to non-state market driven system of authority

French: confidentialité des informations  
German: informationen privatsphäre  
Spanish: privacidad de la información

English: **concern over social media**  
French: préoccupation sur les médias sociaux  
German: besorgnis über social media  
Spanish: preocupación por las redes sociales

English: **social media**  
French: les médias sociaux  
German: social media  
Spanish: medios de comunicación social

**Results**

*This is a preliminary search for articles containing the selected keywords. Language barriers prohibited a more clear understanding of the information contained within the article. Moreover, the inability to export search results - into a type of database where a more thorough ability to sort and filter data would be possible - prevented a deeper analysis of the keywords present in each article. For the purposes of this paper, the results below will be used to identify a general level of strength (i.e. low medium or high) the media has in each Union. Other keywords such as ‘digital information’ and ‘big data’ could have been used. Further study using this methodology could create a more comprehensive environment for analysis of strength if newspapers in other European Union countries were to be examined, or better yet if all newspapers in each of the EU member countries were to be examined individually and collectively. Time limitations prohibit a more in depth study of these search results and leave open the opportunity for further study.*

<table>
<thead>
<tr>
<th>Newspaper</th>
<th>Source Country</th>
<th>Concern over information privacy</th>
<th>Information Privacy</th>
<th>Concern over social media</th>
<th>Social media</th>
</tr>
</thead>
<tbody>
<tr>
<td>The Guardian</td>
<td>England</td>
<td>3,400,000</td>
<td>316,000</td>
<td>71,000</td>
<td>781,000</td>
</tr>
<tr>
<td>El Mundo</td>
<td>Spain</td>
<td>11</td>
<td>42</td>
<td>116</td>
<td>12,795</td>
</tr>
<tr>
<td>Bild der Wissenschaft</td>
<td>Germany</td>
<td>7449</td>
<td>3,809</td>
<td>7,419</td>
<td>280</td>
</tr>
<tr>
<td>Bild Zeitung</td>
<td>Germany</td>
<td>0</td>
<td>193</td>
<td>0</td>
<td>348</td>
</tr>
<tr>
<td>Le Monde</td>
<td>France</td>
<td>81</td>
<td>1254</td>
<td>1,631</td>
<td>16,924</td>
</tr>
<tr>
<td>Le Monde diplomatique</td>
<td>France</td>
<td>128</td>
<td>36</td>
<td>46</td>
<td>986</td>
</tr>
</tbody>
</table>

Brennan, 38
APPENDIX D: Brief Summaries of 2011 Greece Protests and Occupy Wall Street in U.S.

Greece Protests
Greece protests were inspired by proposed austerity measures and motivated more than 80,000 citizens to take direct action in the form of protest (Donadio and Kinsantonis, 2011). Greece politicians were to vote on a bill that would lower wages and pension payments, change collective bargaining rules, make hiring and firing easier. The protesters consisted largely of labor unions members, however, and were joined by “everyone from trash collectors, teachers, retired army officers, lawyers and even judges walked off the job to protest.” The protest was non-violent and violent with individuals killed or injured. Some protesters were arrested. The 2011 protests have roots starting in 2010 and stretch into 2012.

Occupy Wall Street
Occupy Wall Street was inspired by Arab Spring in Tunisia and Egypt, started in New York, New York in September 2011. The NY protest lasted for approximately two months and spread to over 100 cities in the United States and actions in over 1,500 cities globally. The heart of the protest addresses income inequality and places burden of responsibility for the economic collapse of 2008 squarely on the shoulders of Wall Street executives. Several Occupy movements have arisen globally since Occupy Wall Street first began.

---

18 http://occupywallst.org/about/
VIII) Acknowledgements

The shape of this paper would not have been possible without the assistance of many kind and supportive intellectuals who took time from their busy schedules to work with me over the course of the fall 2014 academic semester. First and foremost Dr. Cristina Balboa, author, activist, scholar, and graduate student educator at Baruch College, CUNY, shared with me the possibility of the using non-state market driven framework – her area of expertise - to shape my preliminary research on digital environments, digital information, and digital privacy concepts as they occur in E.U. and U.S. This lead turned an unwieldy topic into a manageable task with a clear direction. Her ongoing support through the first rocky presentation and final production of a draft has been invaluable. I have learned a great deal about patience, encouragement, and generosity from her. Second, Alexander “Xander” Landfair at the Baruch Writing Center bent over backwards to make sure I was able to stop by weekly to share my work with him and to brainstorm on all aspects of the writing process from establishing topic boundaries to employing effective revision and communication strategies. Thanks also to my peer-review colleagues whose feedback was always thoughtful and supportive and to all of my classmates who allowed me a safe space to make mistakes and pick myself back up. To Ms. Silvia Reyes, Professors Antonios Varelas, Cynthia Jones, and Nelson Nunez-Rodriguez as well as Mr. Darren Kwong and Mr. Andrew Lucchesi, thank you for providing much needed support especially during some of my darker moments of writing. Dr. Kate Wolfe was helpful in realizing what it was I was attempting to write about and in brainstorming ways of narrowing the topic; thank you. She also reviewed some writing and offered feedback. From the Hostos Community College Writing Group, Dr. Sherese Mitchell Professors William Casari and Philip Wander provided helpful and honest feedback on multiple drafts of the introduction. In particular Dr. Jacqueline DiSanto, early childhood teacher education faculty and chair of the Writing Group as well as Dr. Peter Spina, a former English teacher and community college president, deserves tremendous thanks for the kind feedback complete drafts of writing. My professional supervisor Dr. Christine Mangino deserves a heart-felt thank you for the consistent flexibility provided during the semester to work on this project. Finally, my intellectual Brennan family was transformational in helping me consider different topics and viewpoints before selecting the final capstone topic. Thank you to my New York City family who suffered with many late nights of keyboard clicking and coffee brewing and from my extended absence on Monday nights. To my dad, for his always present
and never wavering support and for donating his beloved wife to me in so many instances. Most of all, I could not have produced this work had my mom not dedicated more than 72 hours of her life to caring for my precious babies so I could escape to the Baruch College library to write in a quiet space over the weekend. She, too, provided candid feedback on portions of drafts.