Debra N. Diener, J.D., CIPP/G
ID 360 Conference: University of Texas Center for Identity Management: April 23-24, 2012

GLOBALIZATION OF PRIVACY AND IDENTITY MANAGEMENT ISSUES: EMERGING TRENDS AND CHALLENGES

I. INTRODUCTION

The ever-expanding online world is simultaneously blurring and contracting geographical boundaries. Easier, more rapid communications between and among individuals and businesses have created an explosion of detailed personal information being provided, collected, used and shared online--- no longer just nationally but internationally. Privacy and data protection can no longer be viewed, or effectively addressed, only from a national perspective. This globalization trend is exemplified by two recently released proposals. Each proposal will have a significant impact on the way personal information in the United States and Europe is collected, used and controlled by individuals, businesses and organizations.

These proposals are the Administration's *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy"(U.S. Framework) (issued on February 23, 2012)* and the European Commission's *Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals With Regard to the Processing Of Personal Data and on the Free Movement of Such Data (General Data Protection Regulation)* (*Proposed Regulation)* (issued in late January 2012).[1]

The full impact of these documents will be clearer as they are implemented which means many open questions currently exist. However, the broad scope and potential impact of each proposal means that U.S.-based businesses and organizations need to understand the changes and new requirements in privacy and identity management that will be required.

This White Paper provides a high-level roadmap of key issues so U.S.-based businesses and organizations can begin to get prepared. Given the *Proposed Regulation*'s length (116 pages) and complexity, only selected provisions of most interest and impact are highlighted. Suggested "best practices" applicable to either document are identified. These are practices that make sound business sense regardless of the need to comply with any new requirements.

II. OVERLAPPING POLICY GOALS OF BOTH DOCUMENTS

Two important distinctions are needed at the outset. First, the *Proposed Regulation* is a complete regulatory regime of great complexity and detailed specificity. The *U.S. Framework* provides comprehensive and important proposals, some of which will be undertaken through voluntary, collaborative partnerships while others will require legislation.

[1] The *Proposed* Regulation explicitly does not apply to judicial, criminal justice and law enforcement activities (see, Chap. I, "General Provisions", Art. 2 (5)(e). A separate Directive was simultaneously issued outlining the protections associated with processing of personal data for law enforcement and criminal justice and judicial purposes. That Directive is not covered in this White Paper. The official title of that Directive is "Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data."

Second, the enforcement approaches differ between the two proposals --- the *U.S. Framework* is voluntary while the *Proposed Regulation* will be mandatory following its adoption[2]. However, each espouses common concerns and overarching goals that can be summarized as follows:

- Providing individuals with greater control over, and access to, their personal information, thus engendering greater trust in, and use of, online activities and transactions.
- Addressing privacy and identity management issues within the domestic and global contexts.
- Projecting what will be needed for both the present and future commercial Internet global environment.
- Enhancing privacy and security will increase trust levels so that individuals believe that their personal information is being protected.
- Easing cross-border sharing of personal data through simplified mechanisms to make commerce easier and more efficient for companies.
- Increasing economic growth resulting from companies' adoption of privacy-enhancing procedures and mechanisms.

There are significant differences between the two approaches for achieving these goals. In order to fully understand the overlaps and divergences, the key provisions of each proposal need to be reviewed.

III. U.S. FRAMEWORK

Summary of Key Provisions

A. General Scope

In the "Forward", the *U.S. Framework* states that the "...consumer data privacy framework in the United States is, in fact, strong." (see, page i). There are two missing elements from the current framework and the *U.S. Framework*'s proposed initiatives seek to fill those in. What is missing are "...a clear statement of basic privacy principles that apply to the commercial world, and a sustained commitment of all stakeholders to address consumer data privacy issues as they arise from advances in technologies and business models." (see, page i). Filling those two missing elements in the U.S. consumer data privacy framework is the goal of the *U.S. Framework.* Those goals are echoed in the *Proposed Regulation* discussed below.

B. Specific Components

The four key components of the Administration's framework are: the Consumer Privacy Bill of Rights; a process for engaging multiple stakeholders in applying the Consumer Privacy Bill of Rights principles to different business contexts; means for effective enforcement; and a commitment to achieving increased interoperability with the privacy frameworks of U.S. international partners.

- **Consumer Privacy Bill of Rights**

The Consumer Privacy Bill of Rights is the centerpiece of the Administration's proposal. It "...embraces privacy principles recognized throughout the world and adapts them to the

[2] The *Proposed Regulation* will now undergo review by EU Member States and the European Parliament. Following that review, and any modifications, the *Proposed Regulation* would then be approved. It will go into effect two years following its approval and adoption. It will then replace the EU Data Protection Directive 95/46/EC.

dynamic environment of the commercial Internet." (see, "Forward," page i); page 5 and FN 3). The Administration will encourage the adoption by the private sector of the articulated privacy principles through codes of conduct as well as via legislation.

The *U.S. Framework's* privacy principles are based on the Fair Information Practice Principles (FIPPs) that are recognized and adopted (with some country and region-specific variations) worldwide. It is important to underscore the universality of the FIPPs ---- these principles are reflected throughout the *Proposed Regulation* and are explicitly the underpinnings for its numerous provisions and requirements that will become legally enforceable once the *Proposed Regulation* has been adopted.

The FIPPs are formulated in the *U.S. Framework* as the following consumer rights:

- the right to control the personal data that is collected from them and how it is used (Individual Control);
- the right to have easily understood and accessible privacy and security practices (Transparency);
- the right to expect companies to collect, use and disclose personal data consistent with the reasons given when the data was provided (Respect for Context);
- the right of secure and responsible handling of personal data (Security);
- the right to have personal data maintained correctly and accessibly (Access and Accuracy);
- the right for reasonable time limits on retention (Focused Collection); and
- the right to have their personal data handled with appropriate measures to assure adherence with the Consumer Privacy Bill of Rights (Accountability).

(see, page 1).

The *U.S. Framework* recognizes the value technology offers concerning user control and identifies "Do Not Track" technology as especially privacy-enhancing. However, the *U.S. Framework* calls upon the Federal Trade Commission (FTC) and the online advertising industry to develop a self-regulatory set of principles and guidance as well as a "...common mechanism to allow consumers to opt out of targeted advertising by individual ad networks." (see, II. "Defining a Consumer Privacy Bill of Rights," pages 12-13, 24).[3]

As discussed below, this voluntary, self-regulatory approach stands in contrast to corresponding provisions in the *Proposed Regulation.* The *Proposed Regulation*, for example, will require an individual's explicit consent before a business may use "cookies" for online direct marketing targeted to individuals (see, "Whereas", paragraph (50), page 25; Chap. III "Principles", Art. 5, page 40, *Proposed Regulation*).

- **Enforceable Codes of Conduct**

The *U.S. Framework* details a voluntary process through which multiple stakeholders will be engaged to develop "codes of conduct" for particular business markets or business contexts. A stated goal of producing these codes is that they will lead to privacy solutions and protections easily understood by consumers. The *U.S. Framework* also identifies the additional benefits of such voluntary produced codes: one, no Federal regulation produced at the conclusion of the

[3] This voluntary approach to "Do Not Track" is one of the recommendations in the FTC's "Protecting Consumer Privacy in an Era of Rapid Change" report released on March 26, 2012. The report commented favorably on the voluntary "Do Not Track" technology advances being made by a number of Internet browser vendors as well as by the Digital Advertising Alliance.

collaboration; and two, that "...in an enforcement action based on conduct covered by a code, the FTC will consider a company's adherence to a code favorably." (see, pages 23-28).

- **Strengthened Enforcement**

The Administration believes that the Federal Trade Commission (FTC) plays a key role in ensuring that companies follow their stated privacy policies. Such enforcement also has the goal of making sure that companies following their privacy policies are not disadvantaged by those that do not do so. The Administration will encourage Congress to enact consumer data privacy legislation that includes specific authority for the FTC and State Attorneys General to enforce the Consumer Privacy Bill of Rights.

- **Global Interoperability**

This element mirrors a foundational rationale for, and theme of, the *Proposed Regulation*. Recognizing that the Internet assists U.S. businesses expand across geographical borders, the *U.S. Framework* also recognizes that the multitude of privacy laws between and among countries imposes difficulties companies have in transferring personal data across national borders. This will be achieved by having more interoperability between and among the different privacy regimes --- via mutual recognition of the different commercial data privacy frameworks.

As stated in the *U.S. Framework*, "...accountability refers to a company's capacity to demonstrate the implementation of enforceable policies and procedures relating to privacy (whether adopted voluntarily or as a result of legal obligations)" (see, page 32). Compliance can be demonstrated through to-be-developed codes of conduct or the "safe harbor" program that permits companies to self-certify that they are in compliance with the EU Directive 95/46/EC; the former will make companies subject to FTC enforcement of these self-certifications; they are already subject to FTC enforcement under the "safe harbor" program. However, the financial services, telecommunications common carriers and insurance sectors are not FTC-regulated. So the *U.S. Framework* envisions the Commerce and State Departments collaborating to develop mechanisms, such as a code of conduct, for these sectors (see, pages 32-33).

- **Recommended Commercial Legislation**

The *U.S. Framework* also contains a section proposing provisions for consumer data privacy legislation (see, VI. "Enacting Consumer Data Privacy Legislation", pages 35-39). The legislative proposals are for codifying the above-cited provisions including giving the FTC the authority to grant a "safe harbor" to those companies that follow an FTC-approved code of conduct. That would mean that companies with such a code of conduct would be exempted from enforcement of the Consumer Privacy Bill of Rights (once enacted into law).

An important additional legislative proposal needs to be highlighted. This is the proposal to create a national standard for security breach notification in those instances where there is not an applicable federal law. This proposal was included in the Administration's cyber security legislative package. That package was not incorporated as part of the *U.S. Framework*. However, it has been reviewed separately in order to compare its requirements to the data breach notification provisions in the *Proposed Regulation.*

The Administration's security breach notification would require that individuals be notified "without unreasonable delay" following the breach's discovery. Unreasonable delay is defined as not to exceed 60 days except in those instances where the business asks the FTC for

additional time to assess the scope of the breach and to determine, among other questions, how to restore the data system's integrity. The proposal also includes a notification delay if a Federal law enforcement agency determines that the required notification would impede, or interfere with, a criminal investigation or national security activity.

The Administration's proposed timeline for notification contrasts with corresponding provisions in the *Proposed Regulation*. The *Proposed Regulation* requires notification to supervisory authorities and individuals no later than 24 hours, when feasible, after discovery.

B. *U.S. Framework:* Potential Policy Issues and Questions

As noted above, some of the *U.S. Framework* elements will need to include as part of, and then passed as, legislation. Other elements will be undertaken by the Administration with external stakeholders in order to develop and implement voluntary mechanisms.

It is hard to predict the exact contours of any legislative package or timelines for its consideration and passage. However, there are issues businesses can and should start to consider now such as:

- Participating as a stakeholder in a sector appropriate collaborative effort.
- Adopting one of the to-be developed codes of conduct. As noted above, voluntary adoption would be construed as a positive factor in case of any FTC enforcement action based on conduct that is covered by one or more of the codes. (see, page 24)
- Voluntarily adopting a code would also bring FTC review of conduct since the "...Administration expects that a company's public commitment to adhere to a code of conduct will become enforceable under Section 5 of the FTC Act (15 U.S.C. Sec. 45), just as a company is bound today to follow its privacy statements." (see, page 27)
- Getting ready to comply with the more stringent standards of the *Proposed Regulation* could also enable a business to meet future enacted U.S. privacy standards. Businesses might consider this a "cost-benefit" analysis, i.e., do more at the outset and be assured of meeting the U.S. and EU privacy and identity management standards simultaneously.

IV. *PROPOSED REGULATION*

A. General Scope

As noted above, this White Paper reviews only selected provisions presenting the greatest potential interest and impact. These foundational concepts are like the key anchor pieces in a jigsaw puzzle. They have to be explained so the full picture can be understood, i.e., new roles, new requirements with very real sanctions for non-compliance.

The *Proposed Regulation* addresses processing of personal data directed to EU data subjects (individuals). However, the analysis cannot stop there for U.S.-based businesses and organizations. They will need to examine their operations and practices to assess to see if they will eventually have to comply with the *Proposed Regulation.* Why? Because the *Proposed Regulation* applies when business activities entail processing of personal data "...directed to data subjects residing in the Union, or serve (sic) monitor the behavior of such data subjects, including for commercial or professional activities, such as offering products and services." (see, "Whereas", paragraph 14, page 20).

The *Proposed Regulation* enumerates multiple factors when assessing whether a processing operation is directed to a EU data subject. Factors to be assessed include: the "...international

nature of the activities..."; the use of language or currency other than that normally used in the country of the activity; or the "...use of a top-level domain name other than that of the country in which the controller is established." (see, "Whereas" paragraph 15, page 20). But there is an important carve out --- "..the mere accessibility of the controller's website by a data subject residing in the Union in insufficient." (see, "Whereas", paragraph 15, page 20).

Public statements about the *Proposed Regulation* support the assumption that it does not cover U.S. residents. But the above-cited clauses only underscore the complexity of the *Proposed Regulation* and the need for a comprehensive review by a business' senior operational staff and attorneys (both in-house as well as any outside counsel) before reaching conclusions about its applicability.

B. Highlighted Key Foundational Provisions: Requirements and Impact

- **Application of EU Privacy Laws Outside the EU**

The *Proposed Regulation* would extend EU privacy law to non-EU countries if personal data of EU residents were processed by companies that are active in the EU market. This represents a major change in privacy law jurisdiction. As noted above, a business is considered to be active if it offers goods or services in the EU or monitors online behavior of EU citizens. Furthermore, EU privacy laws would become applicable regardless of the physical location of a business or company. (see, "Whereas", paragraph 13, page 21).

- **Personal Data**

Personal data is broadly defined as "...any information relating to a data subject [;]" (see, Chap. i, "General Provisions," Art. 3(2). That covers information about an individual whether it be in his personal/private or professional capacity, e.g., name, photos, email address, social networking site posts, bank details, financial and medical information. Certain categories of personal data (e.g., health, employment) require even stricter rules about processing. (see, Chap. II, "General Principles", and Art. 8, pages 41-42).

- **Data Processing**

This core concept covers, in reality, nearly anything and everything that is done with or to personal data. There are 18 different specified operations covered by the processing definition. Processing of personal data or sets of personal data happens when any one of the following operations, is done alone, or in a combination: "collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, erasure or destruction [;]" (see, Chap. I "General Provisions," Art. 3 (3) page 37). Moreover, to underscore the intended legal reach of the *Proposed Regulation*, it is clearly stated that it covers processing "...regardless of whether the processing itself takes place within the Union or not." (see, "Whereas" section (12), page 20).

A business or organization will have to explicitly state the specific purposes for which the personal data is being collected; only collect the minimum needed for those specified purposes; limit the amount of personal data collected; and retain data for only the minimum time needed. (see, "Whereas" section (28), page 22). some news reports have discussed the *Proposed Regulation* primarily in terms of its impact on Internet companies. Other businesses and organizations should not automatically assume they will not be covered.

- **Electronic and Paper Formats**

The overarching impetus for the *Proposed Regulation* was responding to changing and new technologies such as social media, cloud computing and smart cards. Due to that emphasis, The document clearly states that the scope "[a]pplies to processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system." (see, Art. 3, (4) page 37). Other provisions specifically discuss the proposed changes to the processing of data "...whether or not by automated means..."(see, Chap. I, "General Provisions," Art. 3 (3) page 37).

C. Additional Requirements for Businesses and Organizations

- **Data Controllers and Data Processors**

These are the individuals within a U.S. business who will be responsible for ensuring compliance with the *Proposed Regulation's* strict requirements.

The Data Controller is "...the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes, conditions and means of the processing of personal data [;]" (see, Art. 3 (5)). The Data Processor is "...a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller [;]"(see, Art.3 (6); Chapter IV "Controller and Processor", Articles 19-23).

The *Proposed Regulation* creates numerous detailed duties for each. Data Controllers and Data Processors carry significant responsibilities that will require them to be very pro-active. Compliance will require that they develop and adopt internal controls that document that processing operations comply with the *Proposed Regulation*. They will be required to implement appropriate and extensive technical, administrative, security and organizational measures to ensure a level of security appropriate to the risks represented by the processing and the nature of personal data to be protected. (see, Chap. IV, "Controller and Processor", pages 50-59).

- **Data Breach Notification Duty**

Among the Data Controller's critical duties is notifying appropriate supervisory authority (e.g.regulator) and affected individuals "...no later than 24 hours after the personal data breach has been established." (see, Chapter IV, Section 2 "Data Security", Art. 28(1) and Art. 29(1)).

- **Data Protection Officer**

A Data Protection Officer (DPO) will have to be appointed if the processing entity has more than 250 permanent employees. The DPO's qualifications and duties are specified in great detail. (see, Chap. IV, "Controller and Processor", Sec. 4, Arts. 32-34, pages 60-62).

- **Fines and Sanctions**

Non-compliance will result in tough sanctions and fines ranging from 1% to 3% to 5% of a business' worldwide revenue for intentional or negligent violations. (see, Chap. VII, "Remedies, Liability and Sanctions," pages 86-90).

D. Specific Data Subjects Rights: Requirements and Impact

The business obligations and responsibilities simultaneously translate into greater protections for individuals' personal information. There are additional separately enumerated rights that will

provide individuals with greater access and control over their personal data. These rights will also translate into new identity management requirements.

- **Consent**

Individual consent is a fundamental requirement expressed throughout the *Proposed Regulation*. Although exceptions exist, the majority of the time consent has to be *explicit* rather than presumed or implicit. Individuals may object at any time to the processing of their personal data and such a request has to be honored and all processing stopped. (see, e.g., "Whereas" section, (29), (30); Chap. II, "General Principles", pages 39-43; Chap. III, "Rights of the Data Subject", pages 43-50)

Individuals will have to be told in detail about "...the existence of the processing operation and its purposes, how long the date will be stored, on the existence of the right of access, rectification or erasure and the right to lodge a complaint." (see, "Whereas" section (41); Chapter III "Rights of the Data Subject", Section 2, "Information and Access to Data", Art. 12; section 3, Art. 14). The individual also has to be explicitly informed: whether it is mandatory to provide the information being collected; if so, the consequences of not doing so; and whether the Data Controller intends to transfer the data to a third country or international organization (see, Chap. III, "Rights of the Data Subject," pages 43-50 and Art. 12).

This is an area where there is a fundamental difference between the U.S. and the EU. Under the *Proposed Regulation*, individuals will have to give their explicit consent to the processing of their personal data for online marketing purposes. This contrasts with the common U.S. practice where websites inform the viewer that "cookies" (usually persistent) will be used to permit online behavioral marketing. The viewer is then given the chance to opt out. Under the *Proposed Regulation*, U.S. businesses will have to adhere to the explicit consent requirement before being able to use the collected data to engage in direct marketing for commercial purposes.

- **"Right to be Forgotten**"

Individuals will have the "right to be forgotten". They can request that a Data Controller erase any and all of the personal data relating to them that the Data Controller has. When an individual no longer wants his data to be processed, and there are no countervailing legitimate reasons for its retention, the data has to be deleted by the Data Controller. (see, Chap.III, Rights of the Data Subject, Art. 15). If the Data Controller has made the data public, then it is his duty to ensure that the data is erased on any public Internet link or search engine. (see, Chap. III, "Rights of the Data Subject," Art. 15, pages 47-48).

- **Data Access and Portability**

Individuals also have the right to access their information and get a copy of their personal data from a Data Controller in those instances where that data is processed by automated means. (see, Chap. III, "Rights of the Data Subject, "Arts. 13 and 16, pages 45-46, 48-49). This is intended to allow individuals to move their data easily from one service provider to another.

- **Benefits: One Regulation and Easier Data Transfers**

Easier compliance for businesses is a key goal of the *Proposed Regulation.* For U.S-based businesses, this means they will only have to comply with one regulation rather than with 27 different EU Member States' privacy and data protection laws and regimes.

Personal data will be more easily transferred to third party countries outside the EU and to international organizations. This new approach represents a significant change from the presumption existing under Directive 95/46 that personal data cannot be transferred outside of the EU without a finding that the receiving country has been deemed to have an "adequate level of protection" or that the U.S. business has been certified under the "safe harbor" program administered by the Commerce Department or is utilizing approved standard contract clauses.

V. *Proposed Regulation:* Potential Policy Issues and Questions

Although modification is expected, key overarching questions such as the following need to be anticipated:

- Exact parameters of "consent." Does this mean that an individual has to give his explicit consent each and every time he accesses a website? Or when he moves between and among sites?
- Technological changes that will need to be made given the need for explicit consent for direct marketing.
- Compliance with "erasure" requests. How will businesses comply with requests to have all of an individual's personal data erased from all sources? And how will such compliance be established?
- Use of cloud computer service vendors. A U.S.-based business that uses such a vendor for processing data of EU residents, or even for monitoring online behavior, will need to assure itself that its vendors are complying with the *Proposed Regulation.*

VI. Suggested "Best Practices" For *U.S. Framework* and *Proposed Regulation*

Businesses may already have some, or all, of the following practices in place. If they do, the practices should be re-evaluated in light of the convergence of key provisions in the *U.S Framework* and the *Proposed Regulation*. If they do not, then they should begin to develop and implement them.

- Assemble a team to begin assessing impact under both documents. Assess if your business or organization could be considered actively marketing goods or services in the EU or monitoring online behavior of EU residents.
  >If yes, then begin to develop a plan for addressing the broad provisions.
- Incorporate "Privacy by design" and "Privacy by Default". The *Proposed Regulation* states that compliance can be demonstrated using these requirements (Chap.IV, Art. 25,"Documentation, pages 53-54). The former means building privacy into products and services from the initial development. The latter means that privacy-enhancing settings should be the default for applications. Plus, the kinds of privacy-enhancing benefits from either approach will be beneficial in showing voluntary compliance with many of the *U.S. Framework's* approaches --- especially if enacted into law.
- Compare current privacy notices and practices against the privacy requirements outlined in both the *U.S.* Framework and the *Proposed* Regulation.
- Consider adopting (if not done already) a privacy notice tailored to a specific sector.
  > For example, financial institutions (FIs) should consider adopting the Model Privacy Notice (MPN) developed by eight federal financial regulatory agencies and issued in 2009. At a minimum, FIs need to have their legal counsel compare the FI's privacy notice to make sure it complies with the MPN. Adopting the MPN is a "safe harbor" as FIs will be deemed to be in compliance with the Gramm-Leach-Bliley Act's requirements; so this could be viewed as part of a voluntary compliance with the to-be-developed U.S. codes of conduct.
- Develop a new, or revise an existing, data breach notification plan. The plan should: identify the senior officials who are to be involved; outline the internal "alert" process and the breach

evaluation regime; include names of the external agencies and organizations to notify; specify the time for such notifications; and detail the means by which, and timelines for, notifying affected individuals.

> There is growing momentum to create a national data breach notification standard. Over 50 bills have been introduced in Congress on this issue as well as the Administration's above-cited legislative proposal.

- Map your organization against the "Data Controller", "Data Processor" and "Data Protection Officer" requirements. Figure out which person, or people, in your organization and/or your contractors and vendors would fulfill these roles.
- Review internal controls to assess what, if any, additional procedures would need to be implemented to establish compliance.
- Create, or adopt an existing, internal "assessment tool" so you can demonstrate compliance.

CONCLUSION

Greater attention is being made nationally and internationally to the explosion of personal information individuals are sharing and being asked to share. Both in the U.S. and abroad, there is a growing recognition that new approaches for protecting and using personal information are required and must reflect the global impact of the online world. The volume of data, the ease with which it can be collected and shared, and the real and potential dangers from its breach or misuse means that more, not less, attention will be paid to these issues. These trends are only likely to get stronger as more and more personal information is put online. Now is the time when U.S.-based businesses and organizations should begin preparing with the adoption of "best practices" as an important threshold step. Doing so has another important benefit --- adopting "best practices" is sound business as privacy-enhancing policies and practices help boost consumer confidence that their personal information is being protected and used appropriately, thus enhancing user loyalty.