Deloitte.

March 26, 2012

Deloitte & Touche LLP

Notice of Inquiry Response

U.S. Department of Commerce

National Telecommunications and Information Administration (NTIA)

Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct Notice of Inquiry
Docket Number: 120214135-2135-01

Audit. Tax. Consulting. Financial Advisory.

National Telecommunications and Information Administration (NTIA)

Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct

Docket Number: 120214135-2135-01

Notice of Inquiry

March 26, 2012

Presented by

Deloitte & Touche LLP
1919 North Lynne St
Arlington, VA 22209

Authorized Negotiator:
Carey Miller, Director
Tel: 571-882-6975
Email: caremiller@deloitte.com

Contracts POC:
Juvy Zapanta, Contracts Manager
Tel.: 703-885-6334
Email: jzapanta@deloitte.com

Submitted To:

Aaron Burstein
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW
Room 4725
Washington, DC 20230
Tel.: 202-482-1055
Email: aburstein@ntia.doc.gov

Deloitte.

Deloitte & Touche
1750 Tysons Blvd.
McLean, VA 22102
USA

www.deloitte.com

March 26, 2012
Aaron Burstein
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW, Room 4725
Washington, DC 20230

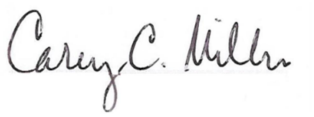
RE: Notice of Inquiry Response to Multistakeholder Process to Develop Consumer Data Privacy Codes of Conduct

Dear Mr. Burstein:

Deloitte[1] is pleased to submit our response to the Notice of Inquiry to serve NTIA. We are excited by the opportunity to provide comment and input to this initiative. We have a long-standing working relationship with the Department of Commerce and its programs.

We hope our response conveys our enthusiastic commitment to provide distinctive client service and highly specialized talent to NTIA, as you undertake a project with so much importance to our Nation. If you have any questions or require additional information, please contact me at 571-882-6975. Should you have any contractual questions, please contact Juvy Zapanta, Contracts Manager, at 703-885-6334.

Sincerely,



Carey Miller, Director
Deloitte & Touche LLP

[1] As used in this document, "Deloitte" means Deloitte & Touche LLP, which provides Identity, Credentialing & Access Management advisory services and Deloitte Consulting LLP, which provides Human Capital, Strategic Communications, and Knowledge Management System advisory services. These entities are separate subsidiaries of Deloitte LLP. Please see www.deloitte.com/us/about for a detailed description of the legal structure of Deloitte LLP and its subsidiaries

Table of Contents

Recommendations for the Consumer Privacy Bill of Rights

Our nation's economic growth is increasingly tied to the Internet. Our ability to use the Internet as a tool to expand the scope and capacity of our economy is important to the growth and security of our nation. Consumers are increasingly moving their buying activity to the Internet. In order to maintain consumer confidence, consumers must trust the environment and have assurance that they are on reasonable footing with other participants. Technology continues to develop at a pace that outstrips traditional legislation. "Consumer Data Privacy in a Networked World", a White House white paper, is a significant positive step toward empowering consumers with a dynamic framework, using enduring principles; however, implementing the recommendations will not be an easy task. The National Telecommunications and Information Administration (NTIA) can use lessons learned from previous initiatives to increase the probability of success in implementing the Administration's vision.

This response provides observations and perspectives. It also includes recommendations for addressing challenges based on lessons learned from other initiatives that seem to have followed similar paths. For ease of reading and mapping, the structure of this document matches the outline of "Consumer Data Privacy in a Networked World" and includes sections for:

- Consumer Privacy Bill of Rights
- Stakeholder Participation
- Enforcement
- Federal Government Leadership

Consumer Privacy Bill of Rights

Every day, millions of consumers willingly share personal information on the Internet. In many instances, the consumer's decision to share personal information might not be informed. A lack of full disclosure or the provision of vague descriptions of data collection, use, and disclosure practices render many consumers poorly equipped to make good choices about their personal privacy. Even if consumers understand what is being collected, they are rarely provided the control and choice relative to the use of the information once it has been collected. When it comes to privacy on the Internet, consumers are finding themselves at a severe disadvantage, subject to rules they don't understand and have little control over.

The Privacy Bill of Rights is a powerful step toward balancing the equation. Its principles provide mechanisms for consumers who are not legally or technologically savvy to make informed decisions regarding their participation in online transactions.

Universal applicability is perhaps one of the most important aspects of the Consumer Privacy Bill of Rights. Taking the direct reference from the US Constitution, the Privacy Bill of Rights would be more powerful it if were applicable to every person in every situation. In particular, that it applies equally to every industry and to every participant. While some highly regulated industries (e.g., Healthcare and Financial Services) already have significant obligations to protect both privacy and data, their obligations vary in intent and execution. Finding a way to align these initiatives with the broader privacy platform would significantly change the consumers' ability to understand and adopt. In addition, the boundaries between industries will continue to blur as "networks" continue to expand and overlap. The "grey area" between these industries could increasingly provide opportunities for consumer exploitation if they are not addressed with consistent privacy rules.

Third Parties

Third-party participants are frequently involved in online transactions, but consumers often do not know that they are involved or the extent of their involvement. The use of third-parties creates unique privacy and data management challenges. Third-party participants include a diverse group of entities, such as Internet Service Providers (ISPs), advertisement companies or hosting facilities. There are a host of direct participants in every transaction and the responsibilities and accountability of those participants must be clearly defined and enforceable.

From the perspective of the Bill of Rights, third parties must be held to the same level of accountability as the first party participants. This must be done formally and with legal standing for it to be effective. This can be achieved by establishing a chain of trust through the addition of required contract terms and conditions in agreements between an entity with primary consumer contact and its third parties, specifying what rights each party has regarding immediate and future uses of the data. It might also be achieved by the

adoption of self-regulatory regimes or new regulation. Consistent with this idea, for the remainder of this section (on the Consumer Privacy Bill of Rights), any mention of the obligations of an entity extends to any direct third party participants of that entity's transactions.

The healthcare industry and its application of the Health Information Portability and Accountability Act (HIPAA) is a good reference for addressing the challenge presented by third-parties. Under HIPAA and related Privacy and Security Rules, a covered entity (group health plan, healthcare providers, and healthcare clearinghouse) must have written satisfactory assurances (business associate agreements) from vendors (business associates) which collect, use or disclose identifiable health information on behalf of the covered entity. In this way, HIPAA's privacy and security requirements are applicable to vendors who were outside the authority of the Department of Health and Human Services. Later, the Health Information Technology for Economic and Clinical Health (HITECH) Act made the privacy and security requirements of HIPAA directly applicable to business associates.[2] Covered entities are still required to obtain satisfactory assurances that business associates will maintain appropriate security and privacy protections. For these reasons, NTIA should consider using the HIPAA model as a starting point for this process.

Individual Control

In many information transactions today, the individual consumer may have little to no meaningful control over what information is collected and how it is used. A balance must be struck between consumer privacy and commerce. An effective solution must provide the consumer with rights and responsibilities while still enabling commerce to be conducted without overly onerous restrictions. This careful balance is tied into several tenets of the Bill of Rights.

The first tenet is enabling the consumer to understand the details of the transaction. This communication occurs when the vendor describes what information it will collect (transparency and focused collection), how it will use the information (context), and the choices that the consumer will have in transaction (individual control). If the communication provided to the consumer is adequate, then the consumer can make a meaningful choice. Some benefits might be contingent upon the consumer consenting to the privacy practices described. Ideally, denying the consumer the ability to continue in the transaction without consent should be discouraged.

Another aspect of individual control is over what information the consumer would have control. Many advocacy groups suggest that the consumer should have control over any information collected about them. Industry suggests that would be over-reaching. A good compromise would allow the consumer to control the use (or non-use) of information that an entity or third party participant collects directly from the consumer as part of the transaction. The consumer would not be able to control any information that an organization outside of the direct interaction (such as purchased by an aggregator) acquires.

No organization, whether directly privy to the transaction or participating as a third party, should be able to collect information without the consumer's knowing participation. The fact that many companies have taken liberties with respect to consent, extending consumers' willingness to allow the company to collect information beyond a single direct interaction, is one of the biggest concerns of consumer advocacy groups.

Finally, the consumer must have the ability to easily revoke previously provided consent. As with the original choice, revocation must be clear and meaningful. It would be over reaching to require the entity to remove all information collected or used during the course of the relationship after a consumer revokes consent. However, the entity would have to acknowledge the changed nature of the relationship going forward. If the organization placed something on the machine(s) used by the consumer, the entity and third parties should have an obligation to see that those devices/tools are removed. The average consumer does not have the knowledge necessary to find and remove the appropriate remainders. It is reasonable to require the entity to undo that action, or make it simple for the consumer to do so, since they performed the initial action.

A vital aspect of this tenet is the ability to collect, maintain and use information for the purposes of authentication and authorization. For transactions with any significant measure of risk, such as accessing financial or healthcare information, organizations must collect, maintain, and use pieces of information to assure that they are interacting with the appropriate person. This can be clearly

[2] The Privacy and Security Rule are currently under revision as a result of the Health Information Technology for Economic and Clinical Health (HITECH) Act. The interim rules were published in 2010 and the final rules are due out in the near future.

communicated in the initial choice, but it may not be negotiable or revocable if the security of the information is to be protected. Making sure that individuals only have access to the appropriate information is just as critical to the transaction as individual control.

Access and Accuracy

To date, individuals have been largely unable to correct information that is inaccurate. While Identity Theft has become a major contributor to the problem of inaccurate information, it is only a minor component when compared with those caused by typos, interoperability issues or simple human error. The ability of individuals to correct data is critical to the process. In almost every instance corrections require direct human interaction. The consumer is the likely source for discovering inaccurate data, but may not be best suited to determine the alterations/corrections needed to make it accurate. A consumer may find it advantageous to eliminate or alter negative or unflattering information in some instances. For this reason, the process to correct information should be more difficult than the original process that created the information, but not impossible.

A frequent concern for organizations in not granting access, but the collection of information and the manner in which it is used can be considered intellectual property and critical to maintaining a business advantage. There is one way that the access and accuracy principle might be limited. Organizations should enable access and modification to information directly collected from the consumer. This provision would not include access to or the ability to correct information that was either acquired from an alternate third party (such as a data aggregator) or data that the organization created using the base information. As part of the corrective process, organizations that sell or share information to other entities must have an obligation to supply updated information as it is corrected or amended, with as much emphasis to correct downstream data as to the original provision of information.

There are significant advantages to all parties in delineating the responsibilities in this manner. For consumers, they need only find the originating source of the inaccurate information and work to correct it once. Additionally, the entity that originally collected the information point best understands the context under which it was collected, making the determination of accuracy easier. For organizations that purchase the information, they would have a higher level of assurance in the information they purchase as the provider has increased accountability for its accuracy.

A regulatory example of this process in action to date is the Fair Credit Reporting Act (FCRA). The right of a consumer under FCRA to obtain a copy of their report demonstrates access. Under FCRA, there is a robust process to correct erroneous information, and the act specifies that any organization that intends to make an adverse decision about an individual covered by FCRA must inform the individual that the action will take place and grant the individual the right to dispute the derogatory information. The multi-stakeholder group should consider FCRA and similar legislation when developing rules related to access and accuracy.

Respect for Context

As the world of privacy has transformed from speaking about Personally Identifiable Information (PII) to the use of context, this principle has become one of the most important parts of the Bill. The Respect for Context tenet is incorporated into the Privacy Act of 1974 and sets a very good starting point for implementing this principle. It may be difficult for businesses to accept this constraint because they often view the use of information outside the initial context as a way to lower transactions costs with consumers.

The Trust Framework Adoption Process (TFAP) provides an example of a workable starting point for a solution related to this tenet. The TFAP is part of the Federal Government's Identity, Credentialing and Access Management efforts currently in progress. Under the TFAP, commercial identity providers who wish to have Federal agencies accept their credentials must comply with certain obligations of the Privacy Act. Of most relevance, the Identity Provider must set their privacy policies so as to reduce the ability to track consumers as they interact with the Federal government. Further, they cannot use information collected during such transactions for any purpose other than facilitating those transactions, thereby restricting the use of the information to the context under which it was collected. Identity Providers can choose whether or not they wish to participate under those requirements, but the requirements are non-negotiable.

Consumer Responsibility

Enabling consumers to make informed choices starts with education. Though a main source of consumer education should come from advocacy groups, every entity should include some measure of education to their consumers so as to enable them to manage their

information effectively. Entities that take these proactive steps to equip consumers have a right to expect that their consumers are similarly accountable to act responsibly. With both parties informed of and accountable for their actions, the existing concerns many entities have regarding potential liability may be reduced, with the benefit of potentially increasing the entities that are willing to participate.

Stakeholder Participation

Developing the appropriate components of this mandate starts with having the right participants at the table. NTIA must balance the necessity of broad participation with the ability to achieve meaningful accomplishments.

Flexible and Sustainable Structure

The structure must consider the scope of the task, market factors and stakeholders, and the role of government throughout the process. The structure must be flexible and sustainable to endure the changes that will be necessary to meet the unique needs of the different phases of the process.

The initial structure should be appropriate for developing the framework for the process, defining participation (both in depth and breadth) and a timeline for completion. The initial group should have a narrower range of participation because their role is to create a charter that describes purpose, objectives, criteria for success, and organizational structure. They should create the managing structure with a management group that promotes broad participation, maintains flexibility, balances power and representation, and reflects purpose. It must also be equipped to lead the effort.

While a managing group (see below) should handle the day to day management of the process, the leadership group would shape the direction of the process of developing the codes of conduct and/or final Bill of Rights. This structure would promote both broad participation and effectively drive progress toward completion. The management group would involve a broad group of participants in the process, including multiple reviews of completed or draft materials, and opportunities for direct public interaction. The breadth of participation must also be flexible as having such at every point becomes detrimental to progress and could preclude a successful completion.

The development of the National Strategy for Trusted Identities in Cyberspace (NSTIC) offers an example for some of these aspects, particularly regarding evolving the structure over time. With NSTIC, the government has taken a role in setting up and funding initial NSTIC efforts, but plans to reduce its role and funding in the future as NSTIC moves to a self-sustaining model.

Balanced Representation

Broad stakeholder participation and acceptance are critical to the success of any code of conduct. The codes of conduct will have a significant impact on industry, government, and individuals as well as international groups and organizations. It is important to include them and afford them the opportunity to voice their opinions, while also considering the ability or willingness of some groups to participate. As stakeholders become involved in the development of the codes of conduct, their contributions will increase their willingness to adopt codes of conduct. Finally, the governance structure must minimize the ability of well-funded organizations to dominate the process, and minimize the ability of groups who are unwilling to compromise from their position to be able to sidetrack the process.

Transparency and Public Involvement

The primary goal of the multi-stakeholder process is to ensure individual privacy in currently unregulated industries. Individuals will have to interact and transact in the environments created under these codes of conduct. If individuals are unwilling to participate in these new environments, the work of the multi-stakeholder groups will be meaningless. Involving privacy advocacy groups, ensuring that all work is publically available, and allowing individuals to participate through alternative approaches (web forums, social media, etc.) will alleviate these concerns.

Collaborative and Adaptable Government Role

The effort should start with developing overarching legislation. The legislation can empower agencies, perhaps the FTC or other regulatory bodies, to develop the regulatory framework that enacts the Privacy Bill of Rights. The multistakeholder process could be leveraged to develop the codes of conduct. This is the process that has been used in developing the substance of HIPAA, GLB, and changes to FCRA.

Once legislation is passed, Federal government role shifts to that of facilitator helping to ensure continued progress, while avoiding perception that it is dominating the process. However, it also has a role in protecting the public interest, and in this role, the government must be both vigilant and aggressive. In the early stages, the government will have a major role in convening the groups. This role will shift to that of a participant as the groups begin their work on codes of conduct. As the development of the codes draws toward completion, the role of the government must rise again, as the goal of the process is turning the codes of conduct developed by the stakeholders into formal regulation. The governance structure must clearly define and accommodate the government's role in this process.

An additional consideration is that there must be an ability for the multi-stakeholder process to be revisited as necessary to revise the regulations. As previously mentioned, the pace of technological advance necessitates that the Bill of Rights are able to be updated as technology changes.

Managing the Process

A critical aspect in engendering trust in the process of developing the codes of conduct is the selection of the organization that will carry out the day to day development of the products. Although the Federal government will fund the initiative, the ability to have a certain amount of distance from the process will be critical in gaining the trust and acceptance of the stakeholder participants. The government must select an external entity (e.g., a contractor or grantee) to perform management support for the process. This contractor must have a significant enough reputation in the privacy space to be credible and have a track record that precludes any perception that they have a substantive position to promote, enabling them to act as an impartial arbiter. As the authors of the documents, the contractor will have a powerful ability to color the results toward a particular result if desired. A contractor with a demonstrable reputation for independence and objectivity can have a strong impact on increasing the good will and support of the process.

Another critical capability of the contractor is the ability to manage the stakeholder participants well, particularly communications. Active support for the process requires that each participant feel involved in the process and has the sense that their position receives appropriate consideration. This can be achieved through more frequent touch points and working sessions and fostering a collaborative environment for the resolution of difficult issues. In cases where many of the stakeholders have diametrically opposed positions, the ability to dispassionately manage the process while recognizing the value of different positions is critical. In this way, the resolutions achieved will be supported because each participant has both ownership and a stake in success.

Ongoing Participation

Technology is dynamic. Evolution in technology presents a fundamental challenge to this process. Actions that are appropriate today may be inappropriate in the future. Stakeholders must acknowledge this challenge and accept that the details of the codes of conduct developed and implemented through this initial effort will require periodic revision. Provisions must be made for a mechanism that will initiate a review and possible revision of the codes of conduct.

Industry Examples

The Affordable Care Act (ACA) and HITECH offer examples of mechanisms for wide stakeholder interaction in the development of requirements and governance around Health IT (HIT) and Health Information Exchange (HIE). A significant advantage of this process is that participation is tied to significant financial incentives to participate for healthcare providers. A significant difference is that the Federal government (through ONC) has the dominant role in that process.

The development of NSTIC and its implementation also provide good examples. In developing the policy document itself, the process was highly inclusive of Federal agencies with limited participation from industry and advocacy groups. At several stages in the development of NSTIC, collaboration tools were employed to engage stakeholders directly. Subsequent to the publication of the NSTIC Strategy, the nature of the work has changed. The process has moved toward creating the infrastructure and governance to functionally carry out the strategy, after which the process will be self-sustaining, with minimal ongoing participation. In the case of the Consumer Privacy Bill of Rights, the goal is completely different because the intent is to eventually enact legislation and to develop regulation. This difference is essential to the success of the initiative, but it means that the structure must be appropriate for the intended outcome.

Enforcement

A fundamental challenge previous efforts have faced in attempting to achieve similar ends is the ability to enforce the standards of behavior. Creating laws and regulations that cannot or will not be enforced is potentially worse than having nothing in place. It creates a false sense of security that can easily be exploited.

Third Party Enforcement

The mechanism for enforcement against first party participants and third party participants is a very different model. Although it is suggested that third parties act consistently, enforcement must necessarily be different. First party participants have a direct interface, which can be addressed through privacy policies and direct contractual obligations. This is not always the case for third party service providers. While it must be incumbent on the first party to include any intended use of the information collected by the third party as part of the privacy policy, there may be no direct relationship between the consumer and the third party. There must be enforcement options available to respond to actions and obligations of the first party as well as the third party. The first party must be responsible for conducting a reasonable level of due diligence to be sure that the third party will follow the appropriate rules and have the appropriate protections in place. The third party must also be held accountable, separate from that of the first party, for failure to act appropriately. The changes to the HIPAA Security and Privacy Rules create that ability for the healthcare industry, though it is not yet clear how effective that will be or how actively it will be enforced.

Self-Regulatory Regimes

In addition to formal regulatory and enforcement options, a strong potential consideration is the self-regulatory regime. The Payment Card Industry (PCI) has a set of requirements that causes financial services to move toward better corporate behavior, primarily because their efforts are tied to monetary incentives. Apart from any regulatory or legislative requirements, self-regulatory regimes should be encouraged to participate and adapt their own version of the codes of conduct. It would give real teeth to implementing this initiative and help to align many more industries and businesses more quickly. Another reason to encourage their participation is that self-regulatory regimes almost always have a shorter cycle for making changes and improvements as necessary and are able to do a better job of promoting ethical behavior than legal obligations and incentives. Finally, self-regulatory regimes are important to helping industries adapt the codes of conduct to their industries.

Creating a Trustmark

A part of the enforcement model of NSTIC is the development of 'trustmarks.' Some existing examples of trustmarks include Underwriters Laboratories (UL), VeriSign and Trust-e. These logos convey a trust level for consumers as they engage in commerce. Some specific aspects of this include: the ability to review policies and procedures in a real-time manner to help ensure compliance; determining that the adoption of technologies reflects the policies; the ability to suspend actions (even if it is only the removal of the logo) as vouched for by the trustmark; and the ability make such enforcements known as necessary. Creation or expansion of such a trustmark organization to focus on privacy could be a very strong enforcement capability of this initiative.

In an effort to get financial institutions to implement usable, readable privacy policies several regulatory authorities, to include the FTC and the Securities and Exchange Commission (SEC), created model privacy policies. These policies are simple to read, simple to understand and provide a mechanism for consumers to make educated choices on whether or not to participate. Although there was no mandate for any financial service organization to participate, the incentive to do so was that adopting the model privacy policy would establish Safe Harbor status for the participating organization, which would enable increased ability to act internationally. Many small financial institutions also saw this as a good strategy to gain customer support as many of these small institutions already acted in the best interests of their customers which they could turn into a business advantage to compete against larger institutions. It also showed that while being violation for lack of compliance will get participation from some organizations, equally important is to provide positive incentives for organizations to actively comply.

The Role of the Federal Government

Consistent with original document, the intent of the document is for the government to become a participant rather than the dominant voice. However, several of the stated goals can only be accomplished with significant government leadership. First, and more importantly, the goal of this initiative is to create legislation and regulation, which can only be done by the government. Voluntary activities may be able to support and drive this initiative to be more effective, but they must be supported by the power of the Federal

government through legislation, regulation and enforcement. Although none of the participants look to the Federal government as representative of their particular perspective, almost all would agree that they can trust the other participants more when the government is part of the process.

The government should seek to limit their role in the multi-stakeholder process to that of a participant. By taking this type of role, the government can foster participation from all interested parties and gain buy-in for the end results. As part of the implementation process, assisting in the development of trustmarks, self-regulatory regimes and other moderating tools, the government can help ensure the implementation of the Consumer Privacy Bill of Rights meet the intention of the initiative.

Fostering Innovation

In addition to developing the infrastructure for the Consumer Privacy Bill of Rights, the Federal government can take the initiative to support the development of privacy enhancing technologies that exemplify the implementation of the Consumer Privacy Bill of Rights. The implementation of privacy enhancing technologies can go a long way to making the implementation of these principles part of the regular fabric of the web. A good example where this has actually taken place is the adoption of pop-up suppressing filters for internet browsers. This started as a competitive advantage for Mozilla's Firefox, and was subsequently adopted by every other browser provider in order to stay competitive. It almost eliminated the use of pop-up advertisements as a business practice. If, as part of this initiative, the Federal government, or industry advocacy groups were to offer grants or hold contests for privacy enhancing solutions, this could help foster the type of innovation that can promote responsible interactions online for all participants.

Summary

Consumer Data Privacy in a Networked World offers a great start to the process of leveling the field of the web for all participants and encouraging responsible behavior by those participants. As with all starting points, it is now time to hone that approach to make it more effective and increase the chance of success. Deloitte is proud to be able to provide our efforts to support this initiative and looks forward to helping to make this initiative successful.