Before the
U.S. Department of Commerce

In the Matter of the Request for Comments on the Department of Commerce's Report Entitled "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework."	)	**Docket No. 01214614–0614–01**

COMMENTS

OF THE

NATIONAL BUSINESS COALITION ON E-COMMERCE AND PRIVACY

Thomas M. Boyd

DLA Piper
500 Eighth Street, NW
Washington, DC 20004
(202) 799-4000

January 28, 2011

January 28, 2011

FILED ELECTRONICALLY

National Telecommunications and Information Administration
US Department of Commerce

In the Matter of the Request for Comments on
Department of Commerce's Report
Entitled "Commercial Data Privacy and Innovation in the
Internet Economy: A Dynamic Policy Framework."
Docket No. 01214614–0614–01

Comments of the National Business Coalition on E-Commerce and Privacy

The National Business Coalition on E-Commerce and Privacy very much appreciates both the Department undertaking this inquiry and this opportunity to submit comments.

The National Business Coalition on E-Commerce and Privacy (the "Coalition") represents sixteen name-brand corporations engaged in both offline and digital commercial activity. Its membership is diverse, ranging from major financial institutions to equally well-known retailers. All have the same goal: to contribute to the public policy debate in such a way as to help assure that policymakers undertake changes in law and regulation and government practices that are both commercially and economically prudent and workable.

We very much appreciate the opportunity to participate in the Department of Commerce's ("DOC" or the "Department") National Telecommunications and Information Administration's request for public comments on its "Green Paper" entitled ''Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework." We hope our comments will prove to be of value as the Department deliberates incorporating its public policy positions into the Administration's evolving policies on Internet privacy.

We applaud the Department for the effort and consideration it put into the Green Paper and its proposed framework. We particularly commend the Department for its recognition of the important role of self-regulation in the U.S. privacy framework and its recognition of the importance of adopting a flexible framework that encourages innovation.

Introduction

The Department's approach is constructive and offers some interesting and supportable approaches. We very much appreciate that the Department not only suggests the development of

voluntary codes of conduct that provide flexibility but also offers suggestions for encouraging and stimulating the development of such codes. In particular, we endorse the development of meaningful safe harbors for companies that choose to participate in such voluntary codes. In addition, the Department has recognized that prescriptive legislation risks codifying "outdated rules that would fail to protect consumers and stifle innovation."

At the same time, we believe that the Green Paper does not adequately address significant inconsistencies in the U.S. federal and state privacy framework, is too equivocal with respect to the importance of preemption, and unnecessarily suggests the adoption of baseline federal privacy legislation.

The current regulatory environment, composed of sectoral laws, FTC enforcement and self-regulation, provides ample tools for enforcement against bad actors and companies that fail to protect consumer privacy. Moreover, notwithstanding the fact that the Green Paper presumes that the current privacy framework is inadequate, the report does not provide any empirical evidence to support the view that self-regulation has not worked or that its proposed framework is either desired by consumers or necessary to impose on industry. To dispense with self-regulation in exchange for some sort of baseline legislation requires that those endorsing such a shift must provide proof of a need.

Our Coalition Members already have robust privacy protections in place, which are driven by their business models, their concerns with securing their proprietary and customer information, and the demands of the marketplace. Our members treat privacy as a customer service and an essential business practice. In a dynamic marketplace, such as that which surrounds digital privacy, the ability to quickly adapt to new trends and technologies through self-regulation provides the most appropriate protection for consumers. Effective self-regulation facilitates this approach and is a vital part of offline and digital privacy, as laws and regulations are often too rigid and quickly become obsolete.

As the Green Paper recognizes, any privacy framework, even if deemed "self-regulatory," should not be structured so that it risks preventing the development of innovative new privacy protections. Both the free flow of data over the Internet and support from advertising revenue have been critical to the rapid growth of free Internet content and services. Further, any proposed framework that has the effect of increasing consumer costs is highly objectionable to both businesses and consumers, and that concern is only compounded in this economic environment.

We are at a loss to understand why the Administration would want to limit the use of personal information derived from customers and used for targeted marketing purposes. We are unaware of any empirical evidence that such use results in any actual harm, nor have we seen any groundswell of concern on the part of consumers (as opposed to advocacy groups that purport to speak for consumers) that would justify such a policy shift. In our view, it would be detrimental to businesses and consumers alike for the Administration to take a hardline position on a business's use of personal information, especially for marketing purposes. Prohibiting or imposing stringent restrictions on such use would inevitably lead to unfocused and much less effective mass advertising. Further, the shortage of targeted advertising on the Internet would inevitably drive up the cost of providing products and services via the Internet and, ultimately, risk upsetting the "free" status of the Internet.

Strict restrictions on targeted marketing should not be taken lightly; before such restrictions are given serious consideration, the need for such dramatic changes in law and practice should be fully established. Once again, the Green Paper provides no evidence that consumers are willing to pay higher prices for goods and services in order to obtain additional privacy controls or to avoid targeted marketing, a practice that has been shown to enhance, rather than adversely affect, the consumer's Internet experience.

It is also important to note that the system of information sharing that has developed in the United States is a critical component in the success and innovation of our economy. This should not be sacrificed for the sake of global harmony and interoperability. Although its importance is difficult to quantify, it cannot be underestimated. Information exchanges among affiliated organizations, third parties and consumers fuel new product development, innovation and productivity. We need only to look to the way in which the Internet has developed in the United States compared to other nations or to the innovation in the financial services industry to see this at work.

The DOC's primary role in helping shape information policy should be to help the United States retain and enhance its competitive advantage. While the DOC can and should play a role in helping smooth out any bumps when it comes to global information sharing policies, it should not jeopardize our success in order to fit the mold of other countries or geo-global frameworks such as the European Union.

Fair Information Privacy Practices (FIPPs)

In theory, FIPPs such as transparency and accountability represent a potentially promising approach as long as they provide flexibility, are not overly broad, allow for the development of tailored implementation through industry self-regulation, and do not form the basis for a regulatory framework. We agree that there may be room for an overarching system based on notions of transparency, predictability, and consumer choice and control. However, the Department should take very seriously its pledge of flexibility so that any such framework can evolve with continuous and rapid technological change.

The Department should not endorse an array of FIPPs that are overly broad and seek to cover all sources, uses and types of data in the commercial privacy context. The Green Paper sets forth as an example the FIPPs adopted by the U.S. Department of Homeland Security ("DHS") to govern that agency's use of personally identifiable information. The full range of FIPPs appropriate to DHS's unique use of personal information is clearly inappropriate in the context of commercial data generally, and especially so for non-sensitive data (and for the overly broad range of "consumer data" as set forth in the Federal Trade Commission (FTC) Staff Report's definition of "consumer information").

It is important to note that it is not only the type of data (e.g., financial, medical, children's, etc.) but also the form the data are in (e.g., personally identifying, de-identified, aggregated) and their use (e.g., whether they are disclosed to third parties for profiling, used to deny credit or employment) that bear on how FIPPs should apply. Applying FIPPs in the same manner to all

data types is unworkable because not all data are equally sensitive. As a result, not all data or data uses warrant the cost and expenses associated with a FIPPs framework. Business needs and practices differ widely from company to company and industry to industry and do not lend themselves to a "one size fits all" approach.

Further, FIPPs should be technology neutral. While we recognize that the basic principles of consumer privacy – and corresponding protections – should apply in both digital and offline environments, any legislation in this area should take into account that the technological mechanisms available in a digital environment are not the same as in the offline world. Inevitably there will be differences, in both application and choice. In this sense, legislation can never be flexible enough to account for rapidly-changing technology.

Notice and Choice

Notice and choice remains a viable model for addressing consumer privacy, provided that notice is transparent. In its Green Paper, the Department presumes that the current notice-and-choice approach to consumer privacy is outdated or inadequate. We would like to reiterate – much as we did in our response to the Department's Notice of Inquiry – our view that notice and choice have not outlived their value: both are, and continue to be, essential to giving the consumer an understanding about how data collected from him or her will be used and allowing that consumer to make a reasonable and informed decision as to whether to provide requested information.

Companies should—and our Members do—provide meaningful notice and choices about their data practices and acquire consent from consumers where appropriate. Most of our Members already have robust notice and consent regimes in place, and many of these regimes have been driven both by the marketplace and the current U.S. regulatory framework applicable to various types of data and data transfers (*e.g.*, the U.S.-European Safe Harbor framework, the Gramm-Leach-Bliley Act, the Fair Credit Reporting Act and the CAN SPAM Act). We believe that requiring more detailed and elaborate privacy notices electronically or on paper – particularly by those companies that have long been subject to existing federal legal requirements – is unnecessary and would only serve to further confuse consumers.[1]

Further, offering a take it or leave it proposition is appropriate in almost any context as long as there is clear notice to the consumer. As long as there is a robust, clear and conspicuous notice posted on a web site and available to a consumer, the consumer's consent to the merchant's privacy practices should be inferred. Notice and choice is a system that has worked well and has encouraged market-based solutions and industry "best practices" in response to demonstrated consumer needs and expectations. We believe that robust notice that is "clear and conspicuous" is key to the ability of consumers to exercise informed choice. There is no justification for an

---

[1] It may be more productive to avoid duplicative or excessive layers of regulation on businesses that are already subject to a rigorous regulatory regime, and focus any legislative efforts on those entities that are not subject, whether directly or contractually, to such strict laws or regulatory requirements as well as on government agencies that repeatedly receive failing grades on their computer security.

affirmative consent or complex privacy notice requirement, which would be both costly and counterproductive.[2]

Purpose Specification and Use Limitations

In addition, purpose specification and use limitation standards, such as those proposed by the Department, do not correspond with business models or operations. Data are collected for multiple purposes and companies should not be required – and may not be able – to delineate with specificity every possible use of data collected. Such a requirement would likely increase the length and complexity of privacy notices, making them less useful to consumers. Data are usually collected once but used for several or many business needs, rather than one specific need and this should be recognized by the Department.

All companies – but especially those with heightened, regulatory obligations to maintain the security of their customers' data – should be free to alter their use of collected data for lawful purposes, such as increasing security or preventing fraud, without the necessity of an additional notice (even if a category of data that was not previously thought useful for such security has become so).

FTC Role

The Green Paper also asks for comment upon what the FTC's role should be in the development and enforcement of FIPPs. While the FTC should have some involvement in the process, FIPPs should be developed in close coordination with industries, which have a much better understanding of business needs, consumer interactions and technological solutions. FTC regulations would be counterproductive and premature. Flexible guidelines developed by industry are needed in order to accommodate business's needs and concerns, encourage innovation and protect privacy.

Even if the United States took a legislative or regulatory approach to FIPPs, there would be no need for FTC Rulemaking Authority to elaborate on the meaning of FIPPs; FIPPs are designed to be comprehensive and general—not tailored to specific contexts.

Further, FIPPs should not serve as an independent basis for FTC enforcement. The FTC's current Section 5 authority is broad enough for enforcement against bad actors that misrepresent their privacy practices or do not adhere to industry-standard FIPPs. Moreover, the current regulatory environment (e.g., sectoral laws, FTC enforcement, state Attorneys General (AG) enforcement and self-regulation) and competition in the marketplace sufficiently incentivize industry to provide strong commercial data privacy protections.

Private Right of Action

---

[2] For categories of information – such as financial information, medical information and information about children – where disclosure or third party use poses a signification risk of harm, strong sectoral laws have been enacted, such as HIPAA, COPPA and GLBA, to regulate the collection, use and sharing of such categories of information.

With respect to legislation in this area, any baseline privacy legislation enacted should expressly prohibit a private right of action. Providing for a private right of action is not a viable means for effective enforcement. Allowing for a private right of action would attract nuisance lawsuits that consume significant litigation expenses and lead to the inconsistent application of federal law. There are ample alternative incentives to induce companies to participate in self-regulatory programs that would not have similar adverse consequences. If, however, a private right of action were to emerge from the Department's continuing deliberations, we would urge that it include language enabling either party, should it ultimately prevail, to recover all litigation costs including attorneys' fees. In fact, we would urge that this "prevailing party" language be applied to any party engaged in an enforcement action.

Audits and Privacy Impact Assessments

Internal audits are an important governance mechanism for businesses. Most if not all of our Coalition Members already have data governance and management structures in place to protect consumer data, ensure the proper use of personally identifiable information, proactively consider privacy concerns, implement accountable business practices, and employ robust security measures. Our Members recognize that audits play an important role in measuring and adjusting compliance periodically. However, the proper scope and role of such audits varies by business size and industry.

In addition, audit results should not serve as a basis for enforcement actions under the existing FTC framework, nor should they serve as a basis for public criticism. Audits are used in commercial contexts – for example, the Payment Card Industry Data Security Standard – to discern weaknesses in current security systems with a view towards bringing companies into full compliance with policies or standards. Requiring audit results to be published, thereby subjecting them to regulatory and public scrutiny, is counter-productive and would ultimately discourage effective internal audit controls and have a chilling effect on this beneficial process

The purpose of internal auditing is to measure compliance and then fix any identified compliance issues. The accuracy and integrity of audits will be compromised if reports could trigger enforcement actions or private lawsuits. Enforcement actions against companies for non-compliance with internal privacy policies and external laws should only be taken in response to repeated, significant compliance failures. Not every instance of non-compliance by a company would meet this standard or warrant public scrutiny and/or regulatory enforcement.

Voluntary, enforceable codes of conduct

As the Department proposes, voluntary, enforceable codes are an appropriate approach for privacy protections because they develop faster and provide more flexibility than legislation or regulation. The market should be provided time to develop new protections and privacy features, such as voluntary codes of conduct. Any rigid standards imposed by statute could stifle innovation. The Department should encourage industry to continue its efforts to self-regulate online information practices.

Industry has shown its ability to develop and implement non-regulatory codes of conduct and robust security standards on many occasions. For example, the robust industry-developed Payment Card Industry Data Security Standard and the ISO 27001/02 standards already exist and are widely followed. Other examples of widely established self-regulatory industry guidelines include the NAI Self-Regulatory Code of Conduct and the Self-Regulatory Program for Online Behavioral Advertising released by a coalition of associations—American Association of Advertising Agencies, Association of National Advertisers, Direct Marketing Association, Interactive Advertising Bureau and the Council for Better Business Bureaus. Industry has a track record of developing and implementing robust and effective voluntary codes of conduct, and the Department should continue to support such development.

We strongly support the Department's suggestion for the creation of safe harbors against FTC enforcement for companies that adhere to appropriate voluntary and enforceable codes of conduct. A safe harbor would incentivize companies to participate in voluntary codes of conduct and would encourage the development of codes that are appropriately tailored to certain industries or practices. In order to encourage adherence to the FTC's principles for online behavioral advertising, the Self-Regulatory Program for Online Behavioral Advertising, which was developed by leading industry associations in accordance with the FTC's online behavioral advertising principles, should be recognized as a qualifying voluntary code under any safe harbor program.

FTC Enforcement

Subject to our comments above concerning the role of the FTC in the development and implementation of FIPPs, we agree with the Department that, in the absence of industry-specific federal regulation and oversight, the FTC should continue to be the primary enforcement agency for consumer privacy issues; the FTC should continue to have enforcement responsibility for entities not subject to the jurisdiction of other federal regulators. The FTC is best positioned to enforce privacy-related legislation, except with respect to parties that are specifically governed by other regulators, such as the "financial institutions" subject to the Gramm-Leach-Bliley Act ("GLBA") that are specifically governed by other regulators and the entities under the Health Insurance Portability and Accountability Act ("HIPAA") that are regulated by the Department of Health and Human Services. In those cases, the federal functional regulators that are most familiar with the regulation and operations of the regulated entities are best suited to determine such entities' regulatory responsibilities and be the primary enforcers of their privacy and compliance obligations.

Global privacy interoperability

We applaud the Department for its recognition of the importance of the interoperability of global privacy standards. It is imperative that cross-border compliance expectations are equalized. Otherwise, business conducted in the United States will be at a competitive disadvantage over the same business conducted in Europe. It is paramount that international law be equally sensitive to the need for cross-border consistency in both legal requirements and their enforcement.

In particular, it is our view that a persuasive case can be made for the proposition that privacy enforcement in the United States is superior to that which exists elsewhere in the world. No other country is as litigious as the United States, and no one has the range of enforcement mechanisms that we do. It is our strong view that the Department ought to recognize this deficiency on the part of our European competitors and urge the European Union to consider the adoption of American enforcement practices as part of their ongoing review of their privacy law.

Internet commerce and technological innovation are inevitably impacted, in most cases negatively, by the inconsistent application of law, and global privacy law – especially European law which is inconsistently applied. The flexibility demonstrated by some European DPAs, which leads to broad and inconsistent application of data protection laws in the EU, needs to be better understood by policymakers on both sides of the Atlantic. Thus, we reiterate our recommendation that the DOC should conduct a detailed and comprehensive analysis of U.S. and EU privacy and data protection law and enforcement, in order to provide a full and accurate comparison of their respective applications.

National Breach Standard and Effective Preemption

We concur that the development of a national security breach standard is absolutely necessary. At least forty-six states have data security or data breach laws in place and some have both. This patchwork of laws makes compliance increasingly difficult for companies who conduct business in multiple states. Businesses would be much better equipped to develop effective compliance and security programs if they did not have to adapt continuously to an ever-shifting landscape of state laws, which can actually change, as between the states, several times in any given year.

Our Coalition Members strongly support the development of a national security breach standard. However, it is important that a national breach standard include (as the majority of state breach laws currently include) a risk assessment component and harm-based trigger to minimize unnecessarily alarming consumers in situations where the consumer is not at risk of identity theft or financial fraud. Further, it makes no public policy sense to enact such law if it either can be enhanced at the state level, as allowed by section 507(b) of the Gramm-Leach-Bliley Act, or is accompanied by vague, ambiguous or practically non-existent preemption. While we applaud the Department's support for a national security breach standard, we are concerned that its reticence in supporting effective and meaningful preemption serves to undercut the import of the overall effort.

Any national breach standard should be accompanied by effective federal preemption. As most businesses are, each of our Coalition Members is sensitive to the ever-changing compliance environment that inevitably results from a patchwork of state laws when there is imperfect or non-existent federal preemption. It is becoming increasingly difficult, if not practically impossible, to conduct a nationwide business in compliance with sometimes conflicting state requirements. From a public policy perspective, effective preemption is especially important in matters pertaining to the Internet and interstate commerce.

As a trade-off for effective federal preemption, we are willing to support vigorous and effective enforcement of federal law at the state level, so long as either party in an enforcement action is authorized to recover its costs if it prevails. We recognize that federal agencies simply do not

have the resources necessary to enforce the application of federal privacy law across the country. State Attorneys General can supplement the work of the federal government in this area. Their authority, however, should be limited to the exclusive jurisdiction of federal courts, not state courts, to better ensure the consistent application of federal law across state lines. Accordingly, there would be better predictability, for consumers and businesses alike, as to their personal rights and legal obligations, respectively.

The extension of enforcement authority to various unnamed state agencies or bureaus beyond state Attorneys General is neither legally warranted nor politically justified. State Attorneys General have the best sense for the consumer-based privacy needs of the citizens of their respective states and, consequently, they have experience and expertise in this area. Delegation to other less knowledgeable or experienced state agencies or officials is likely to result in less effective or rational enforcement and only serves to dilute the importance of the federal law. If the alleged violations are serious enough to warrant prosecution then they ought to be serious enough to warrant the attention of the State Attorney General.

Harmony with current sectoral regulations

Existing law should not fall victim to conflicting principles in an informal self-regulatory framework. No imposed self-regulatory framework should conflict with existing statutory obligations. Companies, including our Members, have developed and operate under internal policies, procedures, and practices that exceed statutory requirements. The FTC should take care to apply consistent rules to entities that work within an industry that already has established rules, including the "financial institutions" that the FTC currently regulates under GLBA and to "service providers" within the financial services industry that are not directly regulated by GLBA but operate in accord with GLBA, due to both contractual obligation and client need.

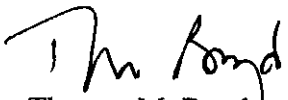
To avoid disrupting existing practices that have been developed in compliance with requirements under federal law and in recognition of business needs, any mandated self regulatory framework should carve out both activities and entities that are subject to either existing law or contractual terms that impose requirements equivalent to a statutory or regulatory obligation. For example, service providers that offer outsourced services such as payments processing to financial institutions, while not explicitly subject to GLBA, are bound by the terms of their outsourcing agreements to comply with the GLBA information privacy restrictions and protections; financial institutions subject to GLBA must contractually bind their service providers to abide by such provisions.

Conclusion

The Coalition very much appreciates the opportunity to participate in the Department's request for public comments on its Green Paper. We hope that our views will contribute to the Department's internal deliberations. Privacy is a broad and diverse subject, and it embodies the reasonable expectations of business and consumers alike. For that reason, and because it inevitably has economic implications, we encourage the Department to remain actively involved, as it represents the only entity within the Executive Branch that is uniquely positioned to reach

across global and domestic boundaries and influence balanced and workable public policy solutions. We look forward to the opportunity to remain involved and to be of whatever assistance we can be throughout this process.

Respectfully submitted,



Thomas M. Boyd
Counsel