

Before the
U.S. Department of Commerce

In the Matter of the Request for
Comments on National
Telecommunications and Information
Administration's Notice of Inquiry,
"National Privacy and Innovation in the
Internet Economy"

)
)
)
)
)
)
)
)
)
)
)

Docket No. 100402174-0175-01

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

June 17, 2010

June 17, 2010

FILED ELECTRONICALLY

**National Telecommunications and Information Administration
US Department of Commerce**

**In the Matter of the Request for Comments on
National Privacy and Innovation in the Internet Economy
Docket No. 100402174-0175-01**

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

I. INTRODUCTION

The National Business Coalition on E-Commerce and Privacy very much appreciates both the Department's 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 online commercial activity. Its membership is also 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 which are both commercially and economically prudent and workable.

We particularly appreciate the opportunity to participate in the Department of Commerce's National Telecommunications Administration's Notice of Inquiry ("NOI"), "National Privacy and innovation in the Internet Economy", and 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.

The NOI lists several areas in which it invites comment, so we will present our thoughts to correspond to each one, as appropriate.

1. US Privacy Framework Going Forward

The NOI seems to predicate this question on the assumption, based on the Department of Commerce's extensive "listening sessions", that "the customary notice and choice approach to consumer protection may be outdated, especially in the context of information-intensive, highly interactive, web-based services." It goes on to say that "in lieu of, or in addition to notice and

choice, some have advanced the notion that sophisticated data managers migrate to a 'use based' model."

The view of the Coalition is that notice and choice have NOT outlived their value, that both are, and continue to be, essential to giving the consumer an understanding about how data collected from him/her will be used and whether that consumer wishes such collection to continue. We already have a "use based" system in place, with functional regulators responsible for supervising the use and collection of data used within their areas of oversight. This 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. It is our belief that robust notice that is "clear and conspicuous" is key to the ability of consumers to exercise informed choice. And that choice need not default to the affirmative consent requirement that is observed in the breach overseas and which is both generally unnecessarily costly and counterproductive in this country. The sole exception, in our judgment, ought to be "sensitive personal information," such as a credit or debit card, in combination with factors that might lead one to identify the holder of the card and access those accounts, or the first and last name of the consumer, in combination with a series of factors that, like the credit or debit card, might lead to the disclosure of, and thereby access to, the consumer's sensitive financial or personal information. This category of information is clearly in need of a higher level of security and stricter access and use, but absent a compelling societal need, we do not think an affirmative consent, or "opt-in," is either necessary or desirable, as a matter of public policy.

Our concern, and it is deeply held, is that a move away from traditional notice and choice is tantamount, ultimately, to prohibition of access, without justification or the establishment of demonstrable economic harm. "Use" is a sufficient distinction, and it is already in place, but any efforts to modify existing notice and choice practices should face strict scrutiny as to the economic consequences and the public policy need. The solution is NOT to redefine "notice" to such an extent that written notices themselves are required to focus, as one policymaker has suggested, on a wide array of intended uses, with such detail as how data is collected, how it is stored and for how long, and how the data is disposed of, among others. In trying to cover every possible use of personal data in a notice, the purpose of which should be to make the consumer aware that personal data pertaining to him/her is being collected and to provide a means by which to learn more details, this kind of approach is self-defeating, for if few consumers care to read notices now, they will surely decline the opportunity if the notices become even longer and more detailed than they already are.

It is our view that the existing framework is working, and adjustments to it should be pursued with extreme delicacy and enhanced sensitivity to the likely "real world" consequences. Most notably has been the recent focus, on the part of some policymakers, on the use of personal data for use in marketing, as though marketing products and services to the public is somehow inherently suspect. On the contrary, it is absolutely essential to the growth of the economy. Without effective marketing, especially when enhanced with data which permits consumers to be presented with and educated about products and services for which they have already demonstrated an interest, companies will have to resort to less efficient and more intrusive mass marketing. The First Amendment precludes an outright ban against commercial speech, which marketing clearly is, so efforts to restrain corporate marketing initiatives through the

broad application of affirmative consent requirements has been the approach of choice recently. And it is both misguided and counterproductive. It is, instead, an academic and highly political solution to a complicated economic reality, and such tools as mailing and prospect lists, catalogues, consumer prospecting mail and customer development are critical to the continued viability of the free market. Without their ready availability, many companies will simply wither and die over time. To the Coalition, any federal efforts to further restrict marketing should first be required to establish a demonstrable economic or personal harm which requires the force of government intervention; nebulous social "harms," such as embarrassment or inconvenience, should be rejected outright as substitutes for the need to define harm strictly and unambiguously. The actual harm standard, unlike the "social" alternatives, are well established and quantifiable, and therefore reliable as a compliance guideline. Anything else is open to interpretation and conjecture, and therefore inconsistent application.

2. U.S. State Privacy Laws

As noted in the NOI, some 44 states already have data security or data breach laws in place, and some have both. So far, these state laws have been more or less aligned, resulting in a manageable compliance environment for companies, such as our members, that are all engaged in interstate, if not global, commerce. But this general consistency of law is a product of both momentary good fortune and the use by some states of the legislative templates developed by another. It is NOT an empirical basis on which to make a public policy assumption that continued and unrestricted state regulation over economic activity with clear interstate implications is either wise or prudent.

The Coalition believes that offline and online laws affecting privacy should be similar, if not virtually identical, and that such laws should be accompanied by effective federal preemption. It makes no public policy sense to enact federal law that can either be enhanced at the State level, as allowed by section 507(b) of the Gramm-Leach-Bliley Act, or by federal law that is accompanied by vague, ambiguous or practically non-existent presumption. Our members are happy to comply with whatever policies are enacted into law, but they simply do not wish to have to comply, nor should they have to, with an ever-shifting "patchwork" of different State laws that can actually change, as between the various States, several times in any given year.

The obvious trade-off for effective preemption is vigorous and effective enforcement of federal law at the State level, and we endorse that exchange of responsibility. Federal agencies simply do not have the resources that would be necessary to enforce the application of federal privacy law across the country. State Attorneys General have an inherent responsibility to protect their citizens from violations of such personal intrusions as the use of personal data, especially sensitive personal data, for illegal purposes. Their active and augmented involvement in the federal framework for privacy protection is therefore useful and desirable. However, the involvement of State Attorneys General should be limited to the four corners of the federal legislation and should find exclusive jurisdiction in federal court, not State court, both because that choice of forum enhances the prospects for the consistent application of federal law across State lines and because consumers and businesses alike can have better predictability over what their legal obligations and personal rights are. The extension of this enforcement authority, as has been proposed of late, to unidentified State agencies or bureaus, or to those State agencies

or bureaus "designated" by State Attorneys General, is neither legally warranted nor politically justified. The State Attorney General has the best sense for the consumer-based privacy needs of the citizens of his/her State, and that should be sufficient. Further delegation only serves to dilute the importance of the federal statute; if the alleged violations are indeed "serious", then they ought to be serious enough to warrant the attention of the State Attorney General.

3. International Privacy Laws and Regulations.

Virtually all of our members engage in global business, both online and offline, and so the nature of international privacy law -- and its level and consistency of enforcement, is of considerable interest to them. We have been engaged, on the periphery, in the recent deliberations of the Asia-Pacific Economic Cooperation (APEC) and are certainly aware of the European Union's recent interest in revisiting its 1995 Data Privacy Directive.

What is paramount to the Coalition is that, like our need for predictability and consistency in the application of federal US law, international law be equally sensitive to the need for cross border consistency in both what the law requires by way of compliance as well and how well and how consistently it is enforced. In fact, the latter is an area in which very little attention has been paid by global policymakers. It makes little difference what laws and regulations say if they are not adequately enforced, and to this point the European attitude has been to compare its 1995 Directive with US law and render the latter "inadequate", leading, in part, to the creation of the Commerce Department's US-EU "Safe Harbor" Framework. We believe, however, that a persuasive case can be made that the nature and level of enforcement applicable to US privacy laws are as "adequate", if not more so, than is the case in Europe. 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, is without doubt inconsistently applied. We would therefore urge the Commerce Department to undertake what does not now exist, so far as we know, but which is absolutely necessary for a truly informed discussion about the delicate balance between economic need and personal privacy expectations: a detailed, comprehensive analysis of US and EU law AND enforcement so as to provide a full and accurate comparison of their respective application.

Unlike Europe, the United States has in place a highly regulatory, aggressively enforced enforcement regime, both at the federal and State level, whereas Europe depends exclusively on its Member State Data Protection Authorities (DPAs) for enforcement of its laws and regulations, and that enforcement can be fairly characterized as inconsistent at best and, at worst, as selectively non-existent. Our members are aware of the "flexibility" demonstrated by certain DPAs in the use and application of affirmative consent, and we believe that flexibility to be the product of regulatory hubris confronted by economic reality. It merely reflects the flexibility exercised regularly by functional regulators in the United States, but its broad and inconsistent application in the EU needs to be better understood by policymakers on both sides of the Atlantic; hence the recommendation for a detailed analysis of the two systems.

4. **Jurisdictional Conflicts and Competing Legal Obligations.**

This section duplicates the concerns stated above, in that consistency of law and its application are inextricably woven together, and both are at the very core of what a meaningful privacy compliance environment actually is, both here and abroad. Our members are constantly concerned about how European law will be enforced and under what guidelines, and they are equally concerned about the current "patchwork" of State laws that exist in this country, as well as about the periodic efforts of policymakers, both at the State and at the federal level, to put politics and a good press releases above the practical effect of law and regulation on their constituents and the economies in their States.

The impact of competing State laws on consumers is obvious. Companies are unable to afford a range of different compliance tools for use in different States depending on the law of that State. They instead tend to gravitate to conforming their compliance needs to the most restrictive States, thereby applying in one State law which another has adopted for itself. Also, the wide range of dates on which State legislatures are in session only adds to the uncertainty our members face on a regular basis. The same is true when extraterritorial jurisdiction is applied to otherwise domestic US actions, and the converse is also true.

5. **Sectoral Privacy Laws and Federal Guidelines.**

As we have said before, the sectoral approach to privacy that comprises the US framework is preferred over all others, and the EU's newly discovered "flexibility" is an admission that economic reality has begun to set in. This "de facto" compliance approach should be codified in Europe, as a result of its current re-examination of the 1995 Directive, so as to equalize cross border compliance expectations. Otherwise, US business conducted in the United States will be at a competitive disadvantage over the same business conducted in Europe, when both should be treated equally.

The absence in Europe of an "American Rule" pertaining to attorneys fees suggests that those governments and individuals are or should be aware of what constitutes an effective enforcement system and if the EU is not going to adjust its enforcement system to mirror our more aggressive litigation reality, then it needs to make allowances for the privacy enforcement regime that operates in this country and revisit the EU-US "Safe Harbor" and financial "adequacy" frameworks.

6. **New Privacy-Enhancing Technologies and Information Management Processes.**

Like everyone else who collects and uses personal data, our members are very sensitive to the need to secure and selectively use that data. Our members are brand name companies with decades if not centuries of history, and their customers are their first priority. We believe in industry self-regulation, carefully monitored by functional regulators, including the Federal Trade Commission, and we are open to the need for government action if the justification can be universally understood and accepted. For example, we recognize the need for strong and reliable data security, and we have helped write and promote preemptive federal legislation that would

require every covered entity to provide strong security and notice to consumers when and if a data breach might occur. Each and every time we have become so engaged, others in the policymaking arenas, who wish to stray beyond data security into other areas, such as online privacy, have either consciously or unconsciously side-railed any meaningful and necessary federal legislation. There is certainly a role for government, but it must be sparingly exercised and should not be the first option, as it is in Europe.

7. **Small and Medium-Sized Entities and Startup Companies.**

This is not a category which really applies to the Coalition, as our members are all large, multinational companies based in the US but doing business globally.

8. **The Role of the Government / Commerce Department.**

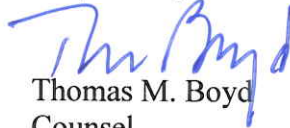
Having worked with the Commerce Department in this and in the previous Administration, it is our considered view that the Department's continued involvement, from both a political public policy as well as a implementation perspective, is necessary in order to provide the White House and Congress with a balanced view that incorporates all perspectives. The FTC plays an important role as the regulator of choice from within the "unregulated" community. But each of these entities are driven in part by its own vision of its specialized responsibility. Only the Commerce Department is positioned to arbitrate disagreements between the functional regulators and to help produce uniform public policy, in the form of research conducted in combination with the functional regulators, and actual coordination, where applicable, after which policy recommendations would then be approved by the White House for implementation or referred to the Congress for its consideration. The Department is also in the unique position to work with the functional regulators to assure that their oversight practices are consistent and that their resources are adequate. The Commerce Department also has relationships overseas through which they would be best positioned to try and harmonize their and our respective privacy regimes. The Department has been at the forefront of interaction with the OECD, the EU-US "Safe Harbor" framework and the APEC deliberations, and its global reach enables it to become an outspoken advocate for the proper balance between the marketplace and consumer privacy expectations.

Conclusion

Once again, the Coalition very much appreciates the opportunity to participate in the NOI, and 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 which 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.

Respectfully submitted,



Thomas M. Boyd
Counsel