

**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

STATE PRIVACY & SECURITY COALITION

Jim Halpert
Callie Carr

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 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 State Privacy & Security Coalition

The State Privacy & Security Coalition ("State Coalition") is pleased to respond to the Department of Commerce ("the Department") Internet Policy Task Force's "Green Paper" on privacy: "Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework" ("Green Paper").

The State Coalition is the most effective coalition of companies and trade associations working on the huge volume of state privacy, security, consumer protection, marketing, child online safety, government surveillance, Internet advertising, content regulation, taxation and VoIP legislation.¹ The State Coalition has a very strong record of developing and obtaining solutions to these legislative challenges.

We appreciate the thought and effort that went into the Green Paper's proposed framework, and support 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, self-regulatory framework that adapts to technological change and encourages innovation.

As President Obama emphasized in his State of the Union Address, it is essential that the U.S. remain an industry leader in the technology sector, including with regard to the Internet and communications, and that it increase its competitiveness internationally in technological development. This will solidify the position of the U.S. as a global leader in technological innovation and add high-value jobs at a time when such jobs are most needed.

We believe that, for the reasons explained in the Green Paper, self-regulation, rather than legislation, is the best method to address privacy challenges in the Internet environment. With

¹ Its company members include Amazon.com, AOL, AT&T, CareerBuilder, Comcast, Cox, Google, Monster.com, NewsCorp, Reed Elsevier, Skype, Verizon, and Yahoo! NetChoice, the Technology Association of America, The Entertainment Software Association, Internet Alliance, and TechNet also participate actively in Coalition activities, expanding its reach in the states.

regard to data security and data security breach notice only, our coalition would support balanced federal security breach notice and data security legislation, provided that it preempts state breach notice and data security laws. While we are not requesting data security/breach legislation, if legislation moves forward, it must include preemption, and we hope that the Department will recommend clearer preemption and provide specific guidance regarding workable breach notice legislation.

I. National Security Breach Notice Legislation

A. *Generally*

The Coalition is very supportive of many elements of the Green Paper. However, we were disappointed that the Green Paper recommended federal breach notification legislation without recommending preemption of state data security technology mandates, such as Nevada's encryption and PCI mandate. These laws, as well as state laws such as the California Confidentiality of Medical Information Act,² that may be construed to create liability for reportable data security breaches, create direct barriers to innovation and to interstate commerce. If federal breach notice legislation is enacted, we believe it should include the process-based Gramm-Leach-Bliley safeguards data security standards as articulated by the FTC³ and that it preempt specific state data security mandates and any state laws imposing liability for reportable security breaches, as these are significant burdens on innovation and commerce.

Preemption of state breach notification and data security laws would create clarity for regulated entities and consumers alike, and would avoid the drag on innovation caused by barriers to the deployment of technologies nationwide and by the need to engage counsel to navigate conflicting state requirements. Indeed, preemption, if federal data breach/data security legislation is enacted, is critical to the national market for information technologies, such as data security technologies, and national data flows, which are just as important as the international data flows that the Green Paper rightly seeks to promote.

B. *Answers to Specific Questions Raised by the Department of Commerce in the Green Paper*

We provide the following answers regarding the Green Paper's specific questions regarding national security breach notice legislation:

1. **What factors should breach notification be predicated upon (e.g., a risk assessment of the potential harm from the breach, a specific threshold such as number of records, etc.)?**

Answer: We urge the Department to recommend that breach notification legislation be premised upon the unauthorized acquisition of electronic records that creates a significant or material risk of identity theft, fraud, or other economic or physical harm to an individual. Any federal legislation should have a clear "harm" standard that is met before notification is required.

² Cal. Civ. Code § 56 *et seq.*

³ 16 C.F.R. § 314.

In addition, we ask that the Department recommend including in any such legislation a technology-neutral exception for data that have been rendered unreadable or unusable. This is critical to promoting innovation in data security methods because exceptions to breach notice are a significant driver for purchases of data protection technologies. Second, we ask that, with regard to notification, notification may be made by electronic means if the data subject's contact with the business is primarily via electronic means. This result would be fully consistent with the Interagency Guidance regarding breach notification.⁴

II. Answers to the Green Paper's Preemption Questions

In this section of our comments, we provide answers to the Green Paper's questions regarding preemption. We note that most of these questions pre-suppose enactment of FIPPs-based federal commercial privacy legislation. As noted earlier, our coalition does not support such legislation and believes that enforcement of a self-regulatory framework is the most appropriate way to promote privacy enhancing change based on emerging marketplace and consumer demands. As such, we answer these questions instead as regards data security breach and data security legislation:

1. [S]hould national policy, in the case of legislation, contain a broad preemption provision?

Answer: Preemption should apply to any state data security breach or data security regulation of activities related to the subject matter of the federal legislation.

2. How could a preemption provision ensure that Federal law is no less protective than existing State law? What are useful criteria for comparatively assessing how protective different laws are?

Answer: We believe that this is not the correct question to ask – federal data security regulation and federal preemption are almost always a two-way street. The goal of reducing uncertainty – and the value to and incentives for the business community to support a federal framework – would be lost if more protective laws trumped preemption. In theory, there can always be “more protective” laws.

The analysis of “protectiveness” is inherently subjective and not a workable standard. As the Green Paper notes with regard to privacy, the criteria that are useful for assessing the difference between privacy laws are context-specific. In the same vein, , the FTC's Staff Report recognizes⁵ that a confusing or vague opt-in is certainly no more protective than a clearly presented opt-out. Rather than being a determinative factor, “protectiveness” should be part of a cost-benefit assessment of the benefits of the state regulation, weighed against the costs and barriers to innovation imposed by the regulation.

⁴ 70 Fed. Reg. 15736 (Mar. 29, 2005) (“the final guidance does not trigger any consent requirements under the E-Sign Act”).

⁵ Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers (Dec. 1, 2010) at 59-60.

3. To what extent should State Attorneys General be empowered to enforce national FIPPS-based commercial data privacy legislation?

Answer: They should be given this enforcement authority, if they have such authority under state consumer protection laws, provided that they cannot outsource enforcement to the plaintiff's bar. This is because the plaintiff's bar operates with very different incentives than State Attorneys General. They serve their own economic interest and are incentivized to maximize revenue to themselves

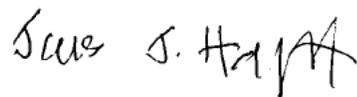
4. Should national FIPPS-based commercial data privacy legislation preempt State unfair and deceptive trade practices laws?

Answer: As noted above, our coalition does not support federal commercial privacy legislation. Federal *data security* legislation should preempt State unfair and deceptive trade practices laws solely to the extent that the state laws provide for enforcement through private rights of action (as a few do).

Unfair and deceptive business practices have long been illegal and there is no reason to preempt them now. However, such laws should not become a vehicle for abusive plaintiff's bar litigation. This is important for a national market for technology services. For example, as patent litigation has shown, there is significant forum shopping in plaintiff's bar actions and actions in a single state can have a huge impact on innovation in the U.S. technology market.

We thank you for considering our views, and are eager to continue to work with you in a constructive fashion to help achieve the Department of Commerce's goals of balancing consumer transparency and choice with beneficial uses of information and continued technological innovation.

Sincerely,

A handwritten signature in black ink that reads "Jim S. Halpert". The signature is written in a cursive, slightly slanted style.

Jim Halpert
Callie Carr
Counsel to the State Privacy & Security Coalition