NetChoice *Promoting Convenience, Choice, and Commerce on the Net*

Steve DelBianco, Executive Director
1401 K St NW, Suite 502
Washington, DC 20005
202-420-7482
www.netchoice.org

February 20, 2013

Sen. Joan Carter Conway, Chair
Education, Health, and Environmental Affairs Committee
State Senate Building
100 State Circle
Annapolis, MD 21401

RE: ***Opposition to SB 859 – Maryland Personal Information Protection Act***

Dear Chairman Conway:

We encourage you to reject SB 859 as it puts Maryland at odds with existing laws in 46 states in critical areas: definitions, deadlines, and details. Industry has for years worked with legislatures and attorneys general to protect consumer information and provide breach notifications. SB 859 imposes a new patchwork of notification mandates that is unworkable for industry and unhelpful to Maryland consumers.

Moreover, these changes to data breach law are not justified without some showing that Maryland consumers are not adequately protected under current law.

Creates confusion and an unworkable new standard for notification mandate

SB 859 creates a new definition for "private information" that overly complicates the Maryland notification law and obscures an otherwise nationally accepted definition. For example, it's unclear whether the "private" data items also meet the definition of "personal information," which is where the critical public records exception would apply.

Discourages the encryption of personal information

We worry that SB 859 discourages businesses from using encryption and other new mechanisms to reduce the risk of harm from unauthorized disclosures of data.

Most states recognize encryption in the same way as existing Maryland law: "transformation…into a form where there is a low probability of assigning meaning." This encourages innovation and investment in more effective and efficient means to eliminate risk of harm from disclosure. Under existing Maryland law, businesses are encouraged to encrypt personal information since that is per se not a breach. But under SB 859, a disclosure that only involved encrypted data would still be considered a breach and would require an investigation and certain notifications.

Impacts online services that let users share their photos

This bill would require social networks to implement security procedures to prevent unauthorized disclosure of an image, since images are "personal information". Under this new requirement, social networks and photo sharing sites might have to prevent users from posting a photo that shows another person without first obtaining and documenting that other person's authorization.

The Committee should wait for the Maryland's Cyber-Security Commission's report

As you know, Maryland is conducting a cyber security study that involves legislators, legal experts, and security analysts. The final report, expected next year, will recommend ways to protect Maryland consumers. Moreover, the report will include a comprehensive review of:

> "(i) State and federal cybersecurity laws; and
>
> (ii) policies, standards, and best practices for ensuring the security of computer systems and networks used by educational institutions and State government and other organizations that work with health care records, personal identification information, public safety, and public service and utilities;"[1]

We urge the committee to defer legislation until the work of the committee report is received, at which point you will have better information to craft a bill that protects your constituents.

We appreciate your consideration of our views, and please let us know if we can provide further information.

Sincerely,

Steve DelBianco
Executive Director, NetChoice

Carl M. Szabo
Policy Counsel, NetChoice

NetChoice is a trade association of e-Commerce businesses who share the goal of promoting convenience, choice and commerce on the Net. Learn about NetChoice at www.netchoice.org

[1] *Maryland Commission on Cyber Security Innovation and Excellence Interim Report* (Dec. 23, 2011).