STATE PRIVACY AND SECURITY COALITION

NetChoice

TECHNET
THE VOICE OF THE INNOVATION ECONOMY

CompTIA. The IT Industry Trade Association

October 24, 2017

Senator Terrence Murphy
Chairman of the New York State Senate Standing Committee
on Government Operations and Investigations

Senator Thomas Croci
Chairman of the Senate Majority Task Force on Counterterrorism
and Public Protection

Re: How Best to Protect Consumers from Theft of their Personal Information

Dear Chairmen Murphy and Croci,

The undersigned associations represent thousands of the country's leading technology companies in high-tech manufacturing, computer networking, information technology, clean energy, life sciences, Internet media, ecommerce, education, and sharing economy sectors. Our member companies are committed to advancing public policies and private sector initiatives that make the U.S. the most innovative country in the world. We share your concern about the security of sensitive consumer personal information; in fact, our members invest hundreds of millions of dollars each year to protect this information. Many also provide consumers with services, such as security software and secure storage solutions, to help consumers protect their own information.

Existing standards, such as those issued by the International Organization for Standardization (ISO) and the Cybersecurity Framework developed by the Department of Commerce's National Institute of Standards and Technology (NIST), address the protection of consumer personal information. In addition, both existing federal and New York State laws provide strong protections. New York law includes a strong data breach notification law enforced by the New York Attorney General. The New York Department of Financial Services also promulgated extensive security regulations this year that apply to a wide range of entities subject to the State's Banking, Insurance, and Financial Services laws. The Federal Trade Commission has a robust enforcement program relating to data security. In addition, other laws

State Privacy & Security Coalition, LLC
500 8th Street, NW
Washington, DC 20004
202.799.4000 Tel

impose significant sectoral security obligations, such as the HIPAA and CPNI security requirements that apply to consumer data held by many New York companies.

Regulation is not a silver bullet in the protection of personal data. There is tremendous innovation in attack methods, much of it driven by nation states deploying new cyber weapons that are then copied by criminal hackers. Attack techniques have penetrated the systems of the National Security Agency, the CIA, and the Department of Defense. Expecting private companies to withstand these sorts of attacks in all cases is not realistic. What is more, because attack methods continue to adapt and evolve, data security invariably has to adapt and evolve, as well.

Rather than a compliance-based, "screenshot-in-time" approach, the challenging task of data security instead requires a flexible, risk-management approach that identifies and responds quickly to changing attack methods and recognizes that these attack methods will inevitably result in cyber intrusions. The NIST Cybersecurity Framework developed through a partnership of the Obama Administration and the private sector sets forth best practices and standards to provide guidance that is helpful at driving better security. Implementation varies based upon the context and size of the specific organization using the Framework.

With regard to data security specifically, the Federal Trade Commission has laid out important principles in its "Start with Security" Guide, which sets out a list of the types of measures (not a checklist) which, in combination, the FTC recommends that businesses use to help secure sensitive consumer information. Best practices can and will change in the future, as threats and security techniques evolve.

Other policy ideas, though, would undermine rather than advance data security. One idea that has surfaced recently is very fast – 48 hour or 15 day -- breach notice to individuals whose private information was, or is reasonably believed to have been, acquired by a person without valid authorization. No state has adopted anywhere near such a short deadline and for good reasons, most notably because it is well known and understood that breach investigations of hacking incidents often take substantially longer than 2 or 15 days to identify the nature and scope of a breach, who was affected by a breach, and whom to notify. In the immediate aftermath of a data breach incident, companies should focus their time and resources on investigating and containing the breach, and securing the company's systems. Imposing an unrealistically short notice deadline would divert companies' resources away from these critical, time-sensitive tasks by injecting a compliance obligation to identify individuals affected and prepare notices before taking these other important steps. It would greatly increase the risk of inaccurate and premature notice that either over or understates the scope of a breach, thereby causing confusion.

Another idea is dramatically expanding the definition "private information" that requires security breach notice to cover "birthdates, home addresses or home phone numbers". This information is widely available in telephone directories or social media postings. None of it is sensitive and none can be used in combination with someone's name to engage in identity theft or fraud. Requiring breach notice if such information is acquired would divert security resources

away from protecting sensitive data and systems to information that is widely available and poses no risk.

All of these ideas would divert company security resources and cause delay to essential remediation activities without providing any additional, meaningful safeguards for consumers.

In summary, we urge you to recognize the complexity of data security, the need for flexibility in a rapidly evolving space, and the strong laws already in place to encourage good data security practices.

We hope that this letter is helpful to your Committees and would be happy to answer any questions you may have.

Sincerely,

State Privacy & Security Coalition
CompTIA
NetChoice
TechNet