The Honorable Michael Sirotkin
Chair of the Senate Committee on Economic Development, Housing and General Affairs
Vermont State House
115 State Street
Montpelier, VT 05633-5301

Subject: Cybersecurity and S. 180

Dear Chair Sirotkin and Members of the Committee:

We have heard about it for years but there is no doubt that the "Internet of Things" or IoT has arrived. But, what is it really? The IoT is billions of Internet-connected products that provide a myriad of services that simplify things, enabling them to become smarter and make decisions aided or un-aided by people.

IoT can make lives easier and it can also provide life-saving services like we have never seen before. It could be something as mundane as a smart refrigerator automatically re-ordering milk when you have had your last glass or your thermostat alerted by your smartphone that you are 10 minutes from home and the heat should be turned up. It can also be something life changing like road sensors alerting your car's internal computer of black ice or radiation-detection devices automatically alerting nuclear power plant management and emergency management systems.

At the core of every IoT application is the ability to securely connect to the Internet and other authorized services and products, while safely protecting personal and business data. From 2013 though 2017, I led a Vermont- and Massachusetts-based company Pwnie Express, an emerging leader in cyber security specifically addressing the challenge of connected and IoT devices in business. At Pwnie Express, my job was to create security solutions that enabled companies to maximize the benefits of connected devices -- such as "Bring Your Own Device" programs and IoT -- while minimizing the risk.

The unique benefits of connected and IoT products also come with unique challenges. In a connected world, one rogue product can be weaponized by a hacker to do damage to others across hundreds, thousands or millions of connections and devices. When it comes to product manufacturers, I was a very critical voice on social media and in our annual Internet of Evil Things report.

For the past 4+ years, I have been vocal about the need for manufacturers to take responsibility for the security of their products. Security must be baked in. I have always said that convenience cannot trump security because there is nothing more "inconvenient" than a breach that costs time, dollars and lives. Most leading manufacturers have stepped up and heard the call.

However, I am concerned that S. 180 would undue all the work industry has done over the past several years to better protect consumers and critical data. I fully understand the good intentions of the bill. However, I fear that it will provide hackers with the details to nearly every Internet-connected product.

The bill is forcing original equipment manufacturers (OEMs) to open the kimono and provide ANY product owner with the ability to alter products to perform tasks that can do damage to consumer security and privacy.

The connected world is one like we have never seen before. No longer do industries or products operate in individual silos. We are truly living in an inter-dependent world and technology policies and legislation need to be looked at through a new lens.

I fear that S. 180 is a pre-Internet solution for a digital world. I look forward to discussing my thoughts in more depth. However, as a veteran of the cybersecurity industry, I do not believe that the trade-off of security for a perceived convenience would be beneficial for consumers, businesses or the economy in any way.

Regards,
Paul Paget
paulpagetjr@gmail.com