**Testimony of Emily White of DannLaw on behalf of The National Association of Consumer Attorneys and the National Association of Consumer Bankruptcy Attorneys**

**Senate Committee on Government Affairs May 9, 2018**

Chairman Coley, Ranking Member Schivone and members of the Committee. I am Emily White. I am a partner with DannLaw, a law firm that has and continues to represent consumers in claims related to the loss of their most personal information like their social security numbers, driver's license numbers, credit card numbers and other personal identifying information. I present this testimony today on behalf of the National Association of Consumer Bankruptcy Attorneys and the National Association of Consumer Attorneys.

There is a tension between individual's right to personal information, and the interests of businesses to collect and profit from that information. As the recent spate of data breaches makes clear, the dawn of the digital age has intensified that tension, complicated discussions about potential solutions, and that balancing these competing rights will spawn litigation for years to come.

I'm sure it comes as no surprise that when something of value is created, in this case the personal information of nearly every American, businesses will monetize it and thieves will steal it. That's why banks, safes, alarms, consumer protection laws and cops were invented. Unfortunately, unlike diamonds, cash, and Picassos, the data points internet users expose every time they log onto the internet are incredibly easy to pilfer because the companies that accumulate and sell that data are often incredibly inept at protecting it.

Even though that ineptitude has been on display repeatedly and personal information belonging to more than half the population has been swiped, policy makers had been reluctant to act because businesses like Equifax downplayed the consequences of data breaches and promised to plug the holes in the cyber security dyke on their own.

***DannLaw is an Ohio professional corporation***

| | | |
|---|---|---|
| *Marc Dann[1]* | *Daniel Solar[1]* | *[1] Admitted in Ohio* |
| *Emily White[1]* | *Whitney Kaster[1]* | *[2] Admitted in Illinois* |
| *Brian Flick[1, 5]* | *Bill Behrens[1]* | *[3] Admitted in New Jersey* |
| *Rusty Payton[2]* | *Donna Kolis[1]* | *[4] Admitted in New York* |
| *Javier Merino[3, 4]* | | *[5] Admitted in Kentucky* |

*Mailing address:*
*PO Box 6031040, Cleveland, OH 44115*

*Telephone: 216-373-0539*
*Fax: 216-373-0536*

The dynamic changed, however, when reports surfaced that Cambridge Analytica had surreptitiously "scraped" info from millions of Facebook profiles and used it to persuade voters to support Donald Trump.

Outraged by this attempt to manipulate the American electoral process, Congress summoned Facebook founder Mark Zuckerberg to Capitol Hill and demanded that he explain how this nefarious act occurred. During two days of hearings a couple things became clear: first, that most members of Congress have no idea what the internet or Facebook are, and, second, that Mr. Zuckerberg and his fellow tech billionaires have no intention of voluntarily cleaning up their act.

That means anyone who visits the internet will remain vulnerable to identity theft unless and until policymakers, digital businesses, and consumer lawyers familiar with cyber security issues work together to draft and implement solutions that will protect both free speech and the right to privacy without impeding digital commerce.

While that work has begun in Congress and other states, the Ohio General Assembly is moving in the opposite direction with S.B. 220. SB 220 even in its amended form will make it *more* difficult for Ohioans to protect their data because it removes incentives like civil liability that motivate companies to keep it safe. By slamming the courthouse door in the face of identity theft victims, the legislation opens the door to additional data breaches. Ironically, S.B. 220 could actually protect consumers if the following provisions designed to prevent data breaches and cyber theft were added:

1. Limit the inclusion of class action waivers and forced arbitration pacts in user agreements;

2. Require companies to spell out their data protection policies in language that is comprehensible and transparent. The disclosures mandated by the Truth in Lending Act should be used as a model;

3. Establish civil penalties for security breaches, failure to disclose potential uses for consumer data, and failure to provide understandable user agreements;

4. Allow for shifting attorneys fees in data breach cases so individuals with small or future damages will have access to the courts;

5. Empower federal and state regulators, rather than companies and trade associations, to establish robust standards for consumer data security;

6. Establish that a consumer using a credit or debit card to make a purchase is doing so with the assurance that their data will be protected.

If members of the general assembly include this additional language, then and only then would this committee and the General Assembly be justified in giving companies that experience data breaches safe harbor from lawsuits. But unless and until they are added, the bill shields big business while exposing Ohio consumers. That's both wrong and dangerous.