PENNSYLVANIA ASSOCIATION FOR JUSTICE

212 North Third Street, Suite 101 • Harrisburg, PA 17101
Phone 717.232.6478 • Fax 717.232.6487
pajustice.org

Pennsylvania House of Representatives

Commerce Committee hearing on HB 1010

February 25, 2020

Nittany Lion Inn, 9:30 a.m.

Testifying on behalf of the Pa. Association for Justice:

Aaron Rihn, Esq., Robert Peirce & Associates, PC

Dan Levin, Esq., Levin Sedran Berman, LLP

Good morning, Chairman Keller, Chairman Galloway, and Members of the House Commerce Committee. Thank you for inviting the Pa. Association for Justice to participate in today's hearing on HB 1010, a bill to update Pennsylvania's cybersecurity law and allow for a private right of action. My name is Aaron Rihn, an attorney at Robert Peirce and Associates in Pittsburgh, Pa. I'll be speaking about the need for increased privacy protection. With me is Dan Levin of Levin Sedran Berman in Philadelphia, who will discuss the benefits of an updated law to Pennsylvania consumers and businesses.

The need for increased privacy protection

In today's evolving online marketplace, there is likely no greater threat to commerce than data breaches, and this problem will only get worse in the future as technology becomes more prominent. On September 7, 2017, Equifax issued startling news: 143 million Americans were exposed to the future risk of identity fraud after the company experienced a significant data breach. Since Equifax, the United States has fallen victim to even larger data breaches. Locally, the data breach of Wawa in 2019 was one of the biggest card breaches known to date. According to the New York Times, the breach affected over 850 stores and potentially exposed 30 million sets of payment records.[1] And just earlier this month, another large breach was announced by another Pennsylvania gas station and convenience store chain, Rutter's, which appears to have compromised the credit cards of thousands of Pennsylvanians at over 70 locations within the Commonwealth.

Michael Collins, a California citizen, had his identity stolen during the Target data breach in late 2013 after he used a bank-issued Visa Card to make purchases at a store near his home. Collins realized he was a victim once he received an email stating that several attempts had been made to access his account. When Collins called the number provided in the email, he learned that over the course of just two days, over two dozen credit card accounts had been applied for–many successfully–at a variety of large-scale retailers. Although he took immediate steps to stop the fraud, the damage had already been done. Over the course of the next few months, Collins tried to unravel the mess. Credit card bills with run-up balances kept arriving in the mail, and he frequently received harassing phone calls from collection agencies. Unlike many others, Collins was lucky to have made it out with only $100 lost in copying and mailing costs. This was not the first time Collins was a victim of identity theft from a data breach. In fact, Collins had been a victim of identity theft six times. Collins explained that "once someone has fallen victim for the first time, the likelihood of them being victimized again increases exponentially over someone

---

[1]. Derrick Bryson Taylor, *Wawa Announces Data Breach Potentially Affecting More Than 850 Stores*, N.Y. TIMES (Dec. 20, 2019), https://www.nytimes.com/2019/12/20/business/wawa-data-breach.html.

who's never experienced it before." This reality exists because once an individual becomes a victim, the victims' information is out in cyberspace and freely available.[2]

Inadequate corporate privacy practices and intentional intrusions into private computer networks have exposed the personal information of millions of Americans. At the same time, internet connectivity has increased in recent years, expanding from personal computers and mobile phones to everyday objects such as home appliances, "smart" speakers, vehicles, and other internet-connected devices. Based on the increased demand for online transactions, from both consumers demanding convenience and business entities pursuing economic efficiencies, the growth of online data transmission is predicted to continue for many years. Accordingly, so will the occurrences of data breach. Some experts argue that covered entities must adopt a "culture of security;" however, the recent mega data breaches indicate that companies do not take security as seriously as they should. This lack of seriousness inevitably leads to expansive and expensive data breaches, at the expense of your constituents' personal privacy.

Federal law & its inadequacies

At the federal level, while there are a number of data protection statutes, they primarily regulate certain industries and subcategories of data. Most notably, the Federal Trade Commission (FTC) fills in some of the statutory gaps by enforcing the prohibition against unfair and deceptive data protection practices. But no single federal law comprehensively regulates the collection and use of personal data, or imposes an explicit duty on businesses to protect consumer information. Adding to the federal patchwork of data protection statutes are the laws of the fifty states. However, most state and federal data breach laws alike often fail to offer real remedies for the loss of personal data, and individuals may falsely perceive that the disclosure of their private data will be punished. With the number of data-breach incidents rising and remedies for consumers being minimal, it is necessary to take a closer look at current laws.

Data theft touches many industries, and like any other type of widespread theft, data breaches come with a heavy cost. Improper data storage and the resulting data theft have exposed enormous amounts of consumer data to unintended third parties, ultimately resulting in billions of dollars in losses. The Herjavec Group estimates that a business will fall victim to a ransomware attack every 11 seconds by 2021. IBM's Cost of a Data Breach Report found that the average total cost of a data breach is $3.92 million

---

[2]. Jamie White, *The Nightmarish Experiences of an Identity Theft Victim*, NORTON LIFELOCK, https://www.lifelock.com/learn-identity-theft-resources-nightmarish-experiences-identity-theft-victim.html (last visited Feb. 14, 2020).

and moving in an upward trend. Moreover, CyberSecurity Venture estimates that Cybercrime will cost the world a total of $6 trillion annually by 2021.[3]

Internet crimes continue to run rampant due to a limited risk of prosecution. Each year, cyber criminals can steal millions of dollars with impunity. For every 1 cybercriminal that is caught, 10,000 go free.[4] The highest barrier in prosecuting cyber criminals is jurisdiction. Most of the time, the person committing the crime is either located outside the country or outside the legal jurisdiction of the court and prosecutors seeking the conviction. Further, even if we are able to collect good legal evidence and even verify the identify and location of the cybercriminal, we have no legal ability to arrest the person. We have established cross-boundary reciprocal legal rules with many cyber allies, but many more countries will not participate. China and Russia, for example, will never honor our arrest warrants. Because it is nearly impossible to prosecute the criminals, it is imperative that we ensure business entities are taking proper precautions to protect the information of their consumers.

Pennsylvania law & the need for an update

Pennsylvania's Breach of Personal Information Notification Act, P.L. 474, was enacted in 2005. However, since then the number of cyber-attacks has continued on an upward trend. According to Statista, which reports on the number of data breaches and records exposed in the United States, in 2005, 157 data breaches were reported. In 2014, 783 data breaches were reported, with at least 85.61 million total records exposed, representing an increase of nearly 500 percent from 2005. That number more than doubled to 1,579 reported breaches by 2017 that left nearly 179 million records exposed.[5] While data breaches were certainly occurring prior to 2005, most of the biggest data breaches recorded are reported after 2005 since the world's volume of data has grown exponentially year after year, giving cyber criminals a greater opportunity to expose massive amounts of data in a single breach.

As such, Pennsylvania's data breach laws are outdated, and must be updated to respond to the increasing number of breaches. Maryland, Virginia, Tennessee, North Carolina, South Carolina, Illinois, New Hampshire, Louisiana, Nevada, California, Oregon, Washington, Hawaii, and Alaska are among the

---

[3]. Rob Sobers, *107 Must-Know Data Breach Statistics For 2020*, VARONIS (Jan. 28, 2020), https://www.varonis.com/blog/data-breach-statistics/.

[4]. Roger A. Grimes, *Why It's So Hard to Prosecute Cyber Criminals*, CSO (Dec. 6, 2016) https://www.csoonline.com/article/3147398/why-its-so-hard-to-prosecute-cyber-criminals.html.

[5]. J. Clement, *Cyber Crime: Number of Breaches and Records Exposed 2005-2018*, STATISTA (Aug. 5, 2019), https://www.statista.com/statistics/273550/data-breaches-recorded-in-the-united-states-by-number-of-breaches-and-records-exposed/.

states that currently allow for private causes of action.[6] An update to Pennsylvania law would ensure that consumers in Pennsylvania will have the same protections and rights as consumers in other states.

Currently, the damages caused by identity thieves are borne only by the victims of the theft, because there are no viable claims that may be brought by an individual against an entity whose poor security measures allowed the theft. Current Pennsylvania law is only enforceable through the Attorney General, and not the individual victims. This leaves the decision to pursue redress solely to the state. Thus, decisions of whether to bring an action can easily be influenced by the availability of resources, arbitrary decisions regarding the seriousness of the breach, and even politics. Further, the current law does not authorize the Attorney General to bring an action for failing to take adequate measure to protect personal information. Ironically, the Breach of Personal Information Notification Act was enacted to protect Pennsylvanian consumers; however, the consumers themselves cannot seek redress if they suffer harm from non-compliance. If a citizen's privacy is violated but there are no remedies available, privacy has not really been protected.

Due to a limited risk of prosecution, data theft will become increasingly profitable, so those entrusted with our data need to be vigilant in protecting and combating the increasing levels of complexity used by data thieves. Consumers should be able to hold wrongdoers accountable, which encourages data holders to maximize data security and protection, thereby reducing the costs overall.

Actions by the Court

Even without an updated law, businesses already face liability for data breaches as the courts have started ruling on the issue. On November 21, 2018, the Pennsylvania Supreme Court drastically changed the data breach litigation landscape by holding that an employer has a common law duty to use reasonable care to safeguard employees' personal information stored on an Internet-accessible computer. In *Dittman v. UPMC*[7], the court further held that Pennsylvania's economic loss doctrine permits recovery for "purely pecuniary damages" on a negligence claim premised on a breach of such a duty. In response to the Court's decision, entities that operate in Pennsylvania or collect personal information about Pennsylvania residents should evaluate their current cybersecurity policies and procedures to ensure that they are taking reasonable measures to protect personal information from unauthorized access or acquisition.

---

[6]. John M. Parker, *Data Security Law—Who Can Enforce Violations of Data Security Breach Notification Statutes? —In Re Target Corp. Data Security Breach Litigation, No. 14-2522, 2014 WL 7192478 (D. Minn. Dec. 18, 2014)*, 38 AM. J. TRIAL ADVOC. 631, 634 (2015).

[7] 196 A.3d 1036 (Pa. 2018).

Whether, and under what circumstances, there is a private right of action is best left for the Legislature, not the courts. If liability is left up to common law interpretations of business' duties, we risk having drawn out litigation and inconsistent rulings—which are bad for business. Importantly, *Dittman* only imposes a common law duty on employers to safeguard the personal information of their employees. Whether other types of entities are subject to this standard is unclear. Therefore, it is even more important for the Legislature to clearly define exactly what duties are imposed on business entities. Given the importance of privacy norms, the Commonwealth should enact laws to adequately protect its citizens.

Increased privacy benefits Pennsylvania consumers & businesses

Data breaches are incredibly costly to both consumers and businesses. Though consumers are affected largely by expenses from identity theft and fraud—expenses which may be reimbursed through litigation—businesses that suffer a data breach can incur much more. Legal fees, notification costs, help desk support, and damages are immediately apparent. But businesses also lose substantial revenue from the stigma attached to a data breach. 70% of consumers say they will stop doing business with a company following a data breach, and businesses lose on average $4.2 million in revenue after a data breach. Further, the effect of data breaches on businesses and consumer confidence hurts the economy as a whole. Lost revenues are reflected in higher prices, higher interest rates, and lost jobs, which affect all consumers and businesses.[8] In short, businesses also suffer from data breach.

Entities that contain sensitive data have a duty to the consumers to protect their information from being released, but also to insurer banks. When personal information is released from debit and credit card transactions, the harms suffered by banks can be extremely costly. For one, the banks may ensure all credit and debit transactions for breaches that occurred to consumers' data.[9] Banks may also be required to indemnify the consumers for their loss as a result of fraudulent activity. Additionally, they may need to issue new credit cards to consumers as a result of the data breach. These damages alone can be debilitating as a result of the data breach.

Data security experts continue to develop greater understanding of data breaches and the ability of hackers to fraudulently or maliciously steal and utilize personal information from poorly-secured servers. In addition to protecting consumers' privacy, data breach statutes provide clarity to businesses that have a duty to protect their customers, clients, and employees' personal information. Consequently,

---

[8] Gregory S. Gaglione, Jr., *The Equifax Data Breach: An Opportunity to Improve Consumer Protection and Cybersecurity Efforts in America*, 67 Buff. L. Rev. 1133, 1152-58 (2019).
[9] See *In Re: Target Customer Data Security Breach Litig.*, 2014 WL 6775314 (D.Minn. 2014).

data breach laws should be updated periodically to respond to changes in technology, data security best practices, and industry standards.

Businesses that store personal data often have trouble understanding what their duties are with respect to securing that data and with notifying the owners of that data following a breach. Unless those requirements are made clear by a statute, many small business owners would have no guidance on their duties and could be greatly exposed to liability for haphazardly storing personal information—a problem they might not know that they had. Data breach statutes prompt businesses to store only the information necessary to meet their business needs, delete information they no longer need, and encrypt, redact, and limit access to sensitive data. These are good data security practices, and they can shield businesses from liability in the event of a breach.

We often think of data breaches in the news as affecting massive corporations with hundreds of millions of records, but any small business that has clients, customers, employees, or an e-commerce website is a potential target. In fact, 43% of data breaches are aimed at small businesses because only 14% of small businesses have adequate data security to defend from an attack. A data breach costs on average $3.92 million to remedy[10]—from direct response, to securing the system, to notifying affected individuals, to reimbursing for fraud and identity theft. More than half of small businesses have been targets of data breaches in the last year because a single malware program can be used to target hundreds of companies without much added effort.[11]

The lack of clarity in the law without a statute increases the uncertainty of liability from a data breach and coverage under a general liability insurance policy, therefore resulting in higher insurance rates, even for businesses with good data security practices.[12] A statute with clearly defined duties and damages makes both compliance and insurance relatively straightforward.

Businesses that use vendors for payment processing, billing, shipping, accounting, inventory management, web hosting, databases, and other cloud services may be liable to their customers if their vendor is hacked. 59% of data breaches are caused by a third-party vendor. Data security statutes will promote better data security practices by vendors, define liability for third-party data breaches, and help all businesses avoid costly data breaches. In September 2019, DoorDash, a restaurant delivery service

---

[10] https://www.ibm.com/security/data-breach; Scott Steinberg, *Cyberattacks now cost companies $200,000 on average, putting many out of business*, CNBC (Oct. 13, 2019), https://www.cnbc.com/2019/10/13/cyberattacks-cost-small-companies-200k-putting-many-out-of-business.html.

[11] Jon Schram, *For the Average Hacker, Your Small Business Is an Ideal Target*, Entrepreneur (Dec. 18, 2018), https://www.entrepreneur.com/article/324711.

[12] *Top 3 Types of Third Party Caused a Data Breach*, NormShield, https://www.normshield.com/top-3-types-of-third-party-caused-a-data-breach/ (last visited Feb. 12, 2020).

platform, announced that 4.9 million users—merchants, delivery drivers, and customers—were affected by a data breach. This is an example where a popular platform that many businesses rely on for their customers, employees, and contractors exposed them to liability for a data breach. In November 2019, Marriott announced a data breach of its Starwood guest reservation database affected 500 million customers. The breach began before and continued after Starwood was acquired by Marriott, exposing Marriott to liability.

Data security statutes also help protect individuals who value the privacy of their data and businesses whose reputations depend on safeguarding their clients and customers' data. By holding businesses accountable with clear data security rules, individuals and businesses have greater assurance that their privacy, and the privacy of their clients and customers, will be protected.

Effects of HB 1010

HB 1010 mandates what types of data businesses must encrypt or redact, how businesses must notify affected individuals following a data breach, and remedies for individuals for a violation of the statute. Each of these aspects of the law are necessary to create a clear set of rights and remedies for the parties.

First, HB 1010 clearly defines what specific values qualify as "personal information" that must be protected, such as a Social Security number. This ensures that businesses are aware of which values must be protected, either by redaction or encryption, both of which are also defined in the statute. It also states that businesses must secure their data systems and "unredacted personal information" with "reasonable measures, consistent with the nature and size of the entity." This duty ensures that personal information is protected and also avoids stringent or impractical standards by taking into account that all business have different data security needs.[13] Data security is a necessity in modern business. It is demanded by both customers and other businesses who deal with them – if a business is not equipped to maintain adequate data security, it should hire a service provider who can do so. HB 1010 provides guidance to businesses and their service providers to make data security needs and insurance more straightforward.

Second, HB 1010 ensures that businesses follow their duty to promptly notify individuals who are affected by a breach. The statute clarifies that the duty to notify only attaches when a business suffers a data security breach which causes "unencrypted and unredacted personal information" to be accessed or

[13] The Federal Trade Commission publishes a data security guide with best practices for businesses of all sizes. *See Start with Security: A Guide for Business*, F.T.C., https://www.ftc.gov/tips-advice/business-center/guidance/start-security-guide-business (last visited Feb. 10, 2020).

acquired by an unauthorized person. So, as long as businesses adequately encrypt and redact personal information, there is no requirement to notify. In this way, the bill defines a minimum requirement for an injury that businesses can easily defend, thereby limiting potential litigation. Conversely, in the absence of a statute, the courts might permit cases to proceed without any allegation that unencrypted and unredacted personal information was compromised.

Finally, HB 1010 provides remedies for affected individuals for identity theft and fraud as well as financial institutions that are forced to reissue payment cards. Statutory damages are necessary for consumers to be made whole after dealing with the frustration and inconvenience from monitoring their accounts, at minimum, after a data breach, or identity theft and fraud, at worst. Statutory damages also inform businesses of the value of privacy, instead of leaving such an uncertain calculation up to the courts.

HB 1010 can provide the clarity that businesses need to understand their duties and defend themselves from data breaches. For example, in June 2019, Quest Diagnostics revealed that its billing contractor, American Medical Collection Agency, suffered a data breach resulting in 11.9 million patient records being accessed, including payment card numbers and Social Security numbers. This is an example in which both consumers and businesses are victims of poor data security—customer data was breached, but Quest also had to deal with—and still is dealing with—with fallout from their contractor's poor data security practices.

HB 1010 provides a cause of action to remedy individuals and financial institutions who were harmed by data breaches. This bill that does not hold any responsible party strictly liable for a breach but rather compensates victims when reasonable care is not exercised. Entities should have a legal duty to take reasonable care to protect sensitive consumer information from unauthorized access. Security standards are found in policies of the computer security division, a component of the National Institute of Standards and Technology Information and Technology Laboratory.[14] Carnegie Mellon University's CRT Program is devoted to ensuring that appropriate technology and system management practices are used to resist a tax on the network system.[15] The Payment Card Industry Security standard counsel provides

[14] Computer Security Division, Nat'l Inst. of Standards and Tech., http://nist.gov/itl/csd/index.cfm (The Computer Security Division (CSD), a component of NIST's Information Technology Laboratory (ITL), provides standards and technology to protect information systems against threats to the confidentiality, integrity, and availability of information and services; NIST is a nonregulatory agency); *see also* Fisher, *Secure My Data or Pay the Price: Consumer Remedy for the Negligent Enablement of Data Breach*, 4 Wm. & Mary Bus. L. Rev. 215 (2013).
[15] Software Engineering Institute, Carnegie Mellon University, http://www.cert.org/faq/cert_faq.html ("The CERT Program is an organization devoted to ensuring that appropriate technology and systems management practices are used to resist attacks on networked systems ...."); *see also* Fisher, *supra.*

standards and supporting materials to enhance payment card data security.[16] These reasonable standards can be adopted by businesses to ensure consumer information is protected to protect the public at large.

Conclusion

Cybersecurity attacks are not new, and sadly, neither are the laws to prevent them and protect hundreds of millions of Americans' personal data. Consumers entrust hundreds of companies—and by extension, the thousands or millions of people who work for those companies—with their personal data. Increasingly, consumers have no choice but to share their private data in order to participate in the modern economy. More and more companies require customers' emails, passwords, addresses, credit card numbers, and Social Security numbers, and that data is regularly stored on Internet-connected computers that are potentially unsecured. Even medical records are being increasingly digitized and stored on the Internet. These pieces of data can be used to turn a person's life upside down through identity theft and fraud. Consumers do not always realize that the data they share with companies can be used against them in the wrong hands. Consumers care about their privacy, because they care about their financial livelihood and reputations, but consumers still willingly share their private data with companies, because they expect that the company will value their privacy as much as they do.

HB 1010 is a desperately needed bill to protect both consumers' private data, and protect consumers and businesses from breaches. The Pa. Association for Justice applauds the sponsor and co-sponsors for introducing such a bill to protect citizens' privacy, and we thank the Commerce Committee for inviting us to testify.

[16] PCI Secuity Standards Council, https://www.pcisecuritystandards.org/security_standards/; *see* Fisher, *supra*; http://www.bu.edu/infosec/policies/data-protection-standards/.