Wisconsin Department of Agriculture, Trade and Consumer Protection

Data Privacy and Security Report

Findings of the Data Privacy and Security Advisory Committee

September 2020

Table of Contents

EXECUTIVE SUMMARY

In 2017, the United States experienced one of the largest data breaches in its history. Nearly 147 million people had their data exposed when the credit reporting bureau Equifax was hacked. The company, charged with collecting and storing the most sensitive consumer data, experienced a breach in which millions of people had their Social Security Numbers, birth dates, addresses, and other data compromised. The breach started in May and went on for three months before Equifax detected it. Once the company discovered the breach in July, it did not notify the public until after its postmortem analysis in September 2017. Equifax entered into a settlement with the Federal Trade Commission and 50 states that included up to $425 million for those impacted by the breach.

The Equifax breach occurred on the heels of the harvest of 87 million Facebook user profiles by now-defunct political consulting firm Cambridge Analytica. Facebook allowed the firm access to users' friend networks and other personal data. For some, this event highlighted an important distinction between a consumer's data and a company's data. Eventually, as a result of data breaches related to Cambridge Analytica, Facebook agreed to a $5 billion settlement with the Federal Trade Commission in July 2019.

These two incidents exemplify the complex questions and challenges that arise in discussions about data privacy and security. What data should be protected or kept private? How should it be protected? When a breach occurs, when should companies notify their customers? These questions have no easy answers. Regulators across the country have attempted to provide answers and have approached the issue from a number of different vantage points. In Wisconsin, no legislation has been passed since 2010 that relates to consumer data security, privacy, or breach, despite these security threats as well as the numerous changes in technology and the rapid expansion of public and private databases that hold consumers' personal information. In an effort to better understand the challenges facing consumers and businesses and identify the best ways to balance consumer protection with existing regulatory frameworks, the Wisconsin Department of Agriculture, Trade and Consumer Protection (DATCP) convened an advisory committee.

The Data Privacy and Security Advisory Committee had four objectives:

- To identify and research possible changes to Wisconsin state law,
- To determine the efficacy of existing consumer data privacy initiatives,
- To consider how best to protect and secure information received by public and private entities in Wisconsin, and
- To determine the business community's readiness to adopt potential regulatory enhancements.

Over the course of nine months, the committee listened to presentations by a number of data privacy and security experts, took public comment, participated in large and small group activities and discussions, and conducted independent research and study.

The committee explored a number of existing data security laws and proposals. The committee started with the European Union's (EU) General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) – the first comprehensive privacy legislation in the United States. The committee then heard about laws and proposed legislation nationwide, addressing data privacy, data security and breach. For instance, the committee learned many states have expanded the definition of what data should be protected (personal identifying information or PII), adopted broad breach notification requirements, and required specific timeframes for when a breach notice should take place. Other states have passed

significant laws addressing data security. A couple states have passed licensing laws requiring companies whose sole or significant purpose is to buy, aggregate, store and sell data to register with the state. Still others have passed laws that permit defenses to breach liability for businesses that "reasonably conform to an industry recognized cybersecurity framework" such as the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO). At least one state has passed a law regulating facial recognition technology.

The committee also examined model data security legislation for the insurance industry, which was drafted by the National Association of Insurance Commissioners (NAIC) and has already been adopted by 11 states. Committee members also reviewed the Digital Standard, a data legislation model created and recommended by a consortium of consumer advocate organizations, including Consumer Reports. Finally, the committee considered the best ways to require ethical standards when businesses collect, store, and share consumer data.

After a series of presentations by subject matter experts, the committee broke into three workgroups: Education, New Ideas, and Harmonization. Each group worked to identify possible approaches Wisconsin could take to better protect consumers and businesses alike.

The workgroups quickly discovered the complexities of creating a regulatory framework that addresses the many intricacies of protecting and securing consumer data without creating unintended loopholes, regulatory redundancies or inconsistencies, or placing an undue financial burden on industry. For example, even the most basic question - what data should be protected and held secure? - can be answered in very different ways by industry, consumers, and regulators.

The most important result of the work of DATCP's Data Privacy and Security Advisory Committee is the greater insights developed into these intricacies. The committee's work revealed the differences that still exist between desired approaches by industry, regulators, and consumers. Even without answers to all of the complex questions at the center of our data-driven world, the committee gained an important understanding of the current legislative landscape, consumer needs, and regulatory challenges. The insights contained within this report highlight where work still needs to be done in order to find consensus on these important issues. This report is designed to serve not as a mandate or directive, but as a tool to assist and support lawmakers, regulators, businesses, and all those interested in improving Wisconsin's data privacy and security.

INTRODUCTION

Participating in today's digital economy requires consumers to provide businesses personal identifying information, or PII. That information is collected, stored, shared, and sold like any other product. The systems that store this information are compromised so regularly that businesses and consumers alike have normalized the occurrence of data breaches. Businesses must continually reassess their security systems, as well as keep abreast of the changing data regulatory landscape. These businesses feed into a massive industry: the data storage market is estimated to grow from $56.8 billion in 2019 to $144.3 billion by 2027.[1]

Meanwhile, consumers often struggle to understand the myriad of reasons their data is collected, stored, and shared. In general, consumers do not want to be data experts—they just want to make sure a business will keep their data secure and private. In a January 2020 survey of Wisconsin consumers, Consumer Reports found that 46 percent of respondents surveyed reported being extremely or very concerned about how much consumer data businesses collect or store. Another 36 percent reported being moderately concerned. That means that approximately four of every five Wisconsinites are concerned about the amount of data that is being collected about them.

In the same survey, 57 percent of respondents reported being extremely or very concerned about the security and privacy of the data businesses collect or store, and another 29 percent reported being moderately concerned. This means that in addition to consumers being concerned about the amount of data being collected about them, more than four in five Wisconsinites are at least moderately concerned about the security of that data. Furthermore, Wisconsinites do not believe the situation is getting better over time: 55 percent believe their data is much less secure or less secure than it was five years ago. (Appendix A) It is no surprise that consumers believe their data is less secure today. Risk Based Security, a cybersecurity firm, has called 2019 "the worst year on record" for data breaches.[2]

> *"I have been part of so many data breaches I can't even keep track of them anymore…."*
>
> *Courtney, Reedsburg, WI – Consumer Reports*

Amid these dramatic changes and concerns about the digital marketplace, consumers, industry and regulators continue to grapple with how to address data privacy and security. Although the terms "data privacy" and "data security" are often used interchangeably, they are distinct concepts. **Data privacy** encompasses how and when information is collected, accessed, processed and disclosed, and whether that disclosure involves consent or notice. **Data security** encompasses the administrative, technical, and physical measures used to protect information. Data privacy cannot exist without data security. These concepts must work in tandem with one another to prevent the intentional or unintentional release of secure or private/confidential information to an untrusted environment, better known as a **data breach**.

Many states across the U.S. have introduced or passed legislation to address data privacy, data security and data breach. The National Conference of State Legislatures (NCSL) reports in 2017, at least 42

---

1 M.C. Today. "Global Next-Generation Data Storage Market is Expected to Reach US$ 144.33 Bn by Year 2027. Accessed July 2, 2020. http://www.mobilecomputingtoday.co.uk/11938/global-generation-data-storage-market-expected-reach-144-33-year-2027-credence-research/.

2 HelpNet Security. "5,183 Breaches from the First Nine Months of 2019 Exposed 7.9 Billion Records." Accessed July 2, 2020. https://www.helpnetsecurity.com/2019/11/14/breaches-2019/.

states introduced data security legislation;[3] in 2018, at least 35 states did.[4] NCSL first posted a list of consumer data privacy legislation in 2019 and identified 25 states that introduced legislation.[5] At least 21 states considered data breach legislation in 2019.[6] As an early adopter of data breach notification protections, Wisconsin's now fourteen-year-old law addressing data breach was given a score of two out of five for strictness by *Digital Guardian*. Only two states (Kentucky and Mississippi) fared worse.[7] Wisconsin has passed no legislation since 2010 that relates to consumer data privacy, security, or breach.

The significant consumer concerns about data security and identity theft, coupled with the lack of recent changes to Wisconsin data privacy laws, prompted the Department of Agriculture, Trade and Consumer Protection (DATCP) to form an advisory committee to explore what steps could be taken in Wisconsin to improve consumer data protections. This report summarizes the work of that committee and what it learned. It also provides a roadmap of the various options and considerations that require further examination in order to move Wisconsin forward.

COMMITTEE OBJECTIVES AND STRUCTURE

In October 2019, DATCP convened the Data Privacy and Security Advisory Committee to discuss the complex issues surrounding data privacy, data security and data breach.

The Advisory Committee had four objectives:

- To identify and research possible changes to Wisconsin state law,
- To determine the efficacy of consumer data privacy initiatives,
- To consider how best to protect and secure information received by public and private entities in Wisconsin, and
- To determine the business community's readiness to adopt potential regulatory enhancements.[8]

In an effort to involve as many stakeholders as practical to identify the best ways to balance consumer protections with business regulatory frameworks in Wisconsin, DATCP invited a wide variety of organizations in the state to nominate individuals to serve on the Advisory Committee. From those

---

3 National Conference of State Legislatures. "Cybersecurity Legislation 2017." Accessed July 2, 2020. http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2017.aspx.

4 National Conference of State Legislatures. "Cybersecurity Legislation 2018." Accessed July 2, 2020. http://www.ncsl.org/research/telecommunications-and-information-technology/cybersecurity-legislation-2018.aspx.

5 National Conference of State Legislatures. "2019 Consumer Data Privacy Legislation." Accessed August 25, 2020. https://www.ncsl.org/research/telecommunications-and-information-technology/consumer-data-privacy.aspx.

6 National Conference of State Legislatures. "2019 Security Breach Legislation." Accessed August 25, 2020. https://www.ncsl.org/research/telecommunications-and-information-technology/2019-security-breach-legislation.aspx.

7 Lohrmann, Dan. *Government Technology*. "New Guide on State Data Breach Laws." Accessed July 2, 2020. https://www.govtech.com/blogs/lohrmann-on-cybersecurity/new-guide-on-state-data-breach-laws.html.

8 The Advisory Committee did not attempt to address issues of cybersecurity or cyberterrorism since those matters were considered out of scope for discussion and deliberation.

nominations, 25 individuals were selected, with members representing government, consumers, and industry. (Table 1: Membership List) Members came from all areas of the state and represented different levels of government, consumers of various ages, businesses of varying sizes, and law enforcement. They represented numerous levels of education, retail, technology, telecommunications, banking, healthcare, and insurance industries.

Table 1: Membership List

First Name	Last Name	Organization	Representing	Workgroup
Nicholas	Alexander	Superior Police Department	Wisconsin Chiefs of Police Association	Education
Megan	Balogh	CUNA Mutual	Wisconsin Manufacturers and Commerce	Harmonization
Jason	Corbin	City of Burlington	League of Wisconsin Municipalities	Education
Emilio	De Torre	The Milwaukee Turners	American Civil Liberties Union	New Ideas
Helen Marks	Dicks	AARP Wisconsin	AARP	New Ideas
Lisa	Freiberg	Fond du Lac County Clerk's Office	Wisconsin Counties Association	Education
German	Gonzalez	Great Lakes Inter-Tribal Council	Great Lakes Inter-Tribal Council	Education
Duane	Harlow	Wisconsin Department of Justice	Wisconsin Department of Justice	Harmonization
Chris	Hefter	Summit Credit Union	Wisconsin Credit Union League	New Ideas
David	Hotchkiss	Medical College of Wisconsin	Wisconsin Association of Independent Colleges and Universities	Harmonization
Kamaljit	Jackson	Wisconsin Women's Business Initiative Corporation	Wisconsin Women's Business Initiative Corporation	Harmonization
Michelle	Jensen	Deerfield School District	Wisconsin Association of School District Administrators	Education
Andrew	Maertz	Reedsville School Board	Wisconsin Association of School Boards	Education
Marco	Martinez	Associated Bank	Wisconsin Bankers Association	Harmonization
Jennifer	Mueller	Wisconsin Hospital Association Information Center	Wisconsin Hospital Association	Harmonization
Bill	Nash	Wisconsin Department of Administration	Wisconsin Department of Administration	New Ideas
Sarah	Orr	Consumer Law Clinic	University of Wisconsin Law School	Education
Diane	Schwartz	Nsight	Wisconsin State Telecommunications Association	New Ideas

Naveen	Sharma	Wisconsin Department of Justice	Wisconsin Department of Justice	New Ideas
Peter	Skopec	WisPIRG	WisPIRG	New Ideas
Lara	Sutherlin	WI Department of Agriculture, Trade and Consumer Protection	WI Department of Agriculture, Trade and Consumer Protection	New Ideas Harmonization
Jim	Temmer	Better Business Bureau	Better Business Bureau	Education
Adam	Williams	Sentry Insurance	Wisconsin Insurance Alliance	Harmonization
Michael	Zimmer	Marquette University	Wisconsin Association of Independent Colleges and Universities	Education
Jim	Zylstra	Wisconsin Technical College System	Wisconsin Technical College System	New Ideas
A number of individuals also sat in as substitutes for the above listed members and attended many of the meetings to provide input into the discussions.				

All meetings were conducted pursuant to the Wisconsin Open Meetings Law. Members of the public were given advance notice of meeting information and were welcome to attend. Meetings were also recorded and available to the public upon request. In the interest of capturing the concerns of Wisconsin residents, the Advisory Committee sought public comment in Green Bay, Milwaukee and Madison before the meetings commenced. Comments were also accepted through a dedicated e-mail address (DATCPDataAdvisory@wisconsin.gov) that was promoted through the Advisory Committee membership, the DATCP website, and numerous media interviews. (Appendix B).[9]

A meeting facilitator from DATCP, in addition to one staff support person, conducted the meetings of the Advisory Committee and the three workgroups. The Advisory Committee met monthly from October 2019 to June 2020 (except for February and March) to listen to presentations by data privacy and security experts, participate in small group activities, and discuss the possibilities for improvement in Wisconsin. (Table 2: Meeting Schedule)

Table 2: Meeting Schedule

Meeting Date	Meeting Location
October 22, 2019	DATCP Board Room, 2811 Agriculture Drive, Madison
November 12, 2019	Northeast Wisconsin Technical College, 2740 West Mason Street, Green Bay
December 10, 2019	DATCP Board Room, 2811 Agriculture Drive, Madison
January 28, 2020	Havenwoods State Forest, 6141 N. Hopkins Street, Milwaukee
April 21, 2020	Virtually via WebEx
May 19, 2020	Virtually via WebEx
June 16, 2020	Virtually via WebEx
July 21, 2020	Virtually via WebEx

[9] DATCP planned other in-person opportunities for public comment around the state that were canceled due to COVID-19.

In January 2020, the members of the full committee identified three workgroups (Education, New Ideas, and Harmonization) and chose one on which they would serve. A spokesperson and note taker were selected for each workgroup, and members were asked to consider potential changes for discussion by both the workgroup and the full Advisory Committee.

These three workgroups each met four times, for two hours each, over the course of two months. They discussed what they had learned from presenters, the larger group activities, and their own industry perspectives. The workgroups used these discussions to develop ideas, which they presented to the full Advisory Committee for consideration and feedback at its May and June meetings.

The Advisory Committee workgroups met as follows:

Workgroup	Meeting Dates	Meeting Location
Education	May 6, 13, 27 and June 10, 2020	Virtually via WebEx
New Ideas	May 7, 14, 28 and June 11, 2020	Virtually via WebEx
Harmonization	May 8, 14, 15, 29 and June 9, 2020	Virtually via WebEx

CURRENT LANDSCAPE OF DATA PRIVACY, SECURITY, AND BREACH REGULATION

Wisconsin has a number of laws addressing the treatment of certain types of data, such as health, finance, and education data.[10] However, the state has only one law that protects consumer data across all industries. Wis. Stat. § 134.98[11] went into effect in 2006 and outlines only what notification is required if personal information, as defined by the law, is breached. Despite numerous changes in technology and the rapid expansion of public and private databases containing consumers' personal information, Wisconsin has made no changes to Wis. Stat. § 134.98 since 2008, when technical revisions were made.[12] Given that Wisconsin law has not changed in the area of consumer data privacy, security, and data breach in over a decade; the Advisory Committee recognized the importance of reviewing and discussing data privacy and security-related laws and legislation.

Data Privacy

The push for what are known as today's data privacy standards originated in Europe. The General Data Protection Regulation (GDPR) went into effect May 25, 2018.[13] The European Union predicated their

[10] Wis. Stat. § 146.816 governs the use and disclosure of protected health information[10] and Wis. Admin. Code § ch. Ins 25, under the auspices of the Office of the Commissioner of Insurance, covers the privacy of consumer financial and health data.

[11] Wis. Stat. § 134.98.

[12] 2007 Wisconsin Act 97.

[13] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

regulations on the notion that privacy is a fundamental right, and information about consumers should be under the control of the consumer.[14]

Data privacy encompasses how and when information is collected, accessed, processed and disclosed, and if that disclosure involves consent or notice.

On the heels of GDPR, California passed the first comprehensive privacy legislation in the United States: the California Consumer Privacy Act (CCPA).[15] The CCPA creates four privacy rights for California citizens: the right to know, the right to delete, the right to opt out, and the right to nondiscrimination.[16] The law applies to businesses in California that collect or process personal information and meet at least one of the following three conditions:

- Has an annual gross revenue of more than $25 million;
- Alone or jointly buys, sells, shares, or receives the personal information of at least 50,000 consumers for commercial purposes; or
- Derives at least 50% of its annual revenue from selling personal information.[17]

The California law has had a secondary impact on Wisconsin, since the law covers all businesses who conduct business in California regardless of where they are headquartered.[18] Thus, Wisconsin businesses conducting business there are covered by the CCPA if they meet one of the above conditions. The complex nature of data privacy and data security has led to amendments and changes to the law since its 2018 adoption.

More recently, Nevada amended its privacy law to require websites and online services to post a privacy notice. Nevada's law, which took effect in October 2019,[19] requires operators of Internet websites and online services to follow a consumer's direction not to sell his or her personal data. The Nevada law differs from the CCPA in that it applies only to operators of Internet websites and online services, and it does not include non-electronic information.

Data Security

There has been a growing trend to address not just the disclosure of information, intentional and unintentional, but also to secure the information that is collected and stored. Massachusetts led the way, passing a data security law that accomplishes multiple objectives:

- Establishes minimum standards to be met in connection with the safeguarding of personal information in both paper and electronic records;

---

14 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

15 California Consumer Privacy Act (Cal. Civ. Code §§ 1798.100-1798.199).

16 Black, Raine, and Melissa Schmidt, Wisconsin Legislative Council Issue Brief, "The California Consumer Privacy Act." December 2019, Wisconsin Legislative Council.

17 Black, Raine, and Melissa Schmidt, Wisconsin Legislative Council Issue Brief, "The California Consumer Privacy Act." December 2019, Wisconsin Legislative Council.

18 Friel, Alan L., Laura E. Jehl. and Melinda L. McLellan. BakerHostetler. "The California Consumer Privacy Act: Frequently Asked Questions." Accessed July 2, 2020. https://www.dataprivacymonitor.com/ccpa/the-california-consumer-privacy-act-frequently-asked-questions/.

19 NRS Chapter 603A (Nevada).

- Applies to any entity that owns/licenses information about Massachusetts residents;
- Establishes a duty to protect personal information;
- Defines personal information and who owns or licenses it; and
- Lays out requirements and safeguards.[20]

Other states have passed similar laws addressing data security in recent years including New York, Illinois, and Connecticut.[21]

Data security encompasses the administrative, technical and physical measures used to protect information.

Vermont and California passed what are known as "data broker" laws, targeting companies whose sole or significant purpose is to buy, aggregate, store and sell data. Vermont's law creates a data broker registry, requiring annual registration with the Secretary of State and maintenance of minimum data security standards. The law further prohibits fraudulent acquisition of data and committing "bad acts" with that data.[22] Since the law covers Vermont consumers, it affects a number of out-of-state businesses who collect data in the state. California's 2019 data broker law requires data brokers to register with the Attorney General and defines a data broker more expansively than Vermont's law, as "…a business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship, subject to specified exceptions."[23]

Michigan and Ohio passed data security laws that incorporate a safe harbor for those that create, maintain, and comply with written cybersecurity programs. These laws allow business to assert affirmative defenses to legal challenges if they have instituted security measures that "reasonably conform to an industry recognized cybersecurity framework" such as the National Institute of Standards and Technology (NIST) and the International Organization for Standardization (ISO).[24]

On the industry side, the National Association of Insurance Commissioners (NAIC) has drafted model data security legislation for the insurance industry. In addition to other things, the model bill requires that licensees develop, implement, and maintain a written information security program that contains risk-based safeguards for the protection of information systems and non-public information. The program must also protect data security and curb unauthorized use of data. When data is no longer used, the model law requires that it be destroyed. Under the model law, insurance companies must also conduct risk assessments. To date, eleven states have adopted some version of NAIC's model law.[25]

Ideally, not being compromised in the first place is the most desirable scenario for a business. Therefore, it is vital that businesses have a solid understanding of what types of data businesses possess that are

---

20 201 CMR 17.00 (Massachusetts).

21 New York Shield Act (General Business Law §§ 899-AA); Illinois Personal Information Protection Act (815 ILCS 530); and General Statutes § 36a-701b (Connecticut).

22 Vermont Office of the Attorney General. *Guidance on Vermont's Act 171 of 2018 Data Broker Regulation*. December 11, 2018, Vermont Office of the Attorney General.

23 California Civil Code § 1798.80 -§ 1798.88.

24 Ohio Revised Code, § 1354; and Michigan MCL 445.72.

25 Weatherford, Holly, Jennifer McAdam, and Chara Bradstreet. *The NAIC Insurance Data Security Model Law*. National Association of Insurance Commissioners, June 2020.

likely to be targeted, along with the correct application of controls to make that data more difficult to access.[26]

Data Breach

Consumers and businesses alike focus on the prevention of data breaches. Unfortunately, many industry watchers believe that data breaches are an inevitable aspect of storing data. In 2018, the Ponemon Institute, in research sponsored by IBM Security, predicted that 26.9% of all American companies would have a data breach of at least 10,000 records in the following 24 months.[27]

A data breach is the intentional or unintentional release of secure or private/confidential information to an untrusted environment.

According to the Identity Theft Resource Center (ITRC), the number of U.S. data breaches tracked in 2019 (1,473) increased 17 percent from the total number of breaches reported in 2018 (1,257).[28] Between January 1, 2005 and May 31, 2020, the ITRC received reports of 11,762 data breaches affecting over 1.6 billion records.[29]

The costs of data breaches are borne by consumers and industry. In 2018, $3.4 billion was lost due to new account fraud. The average cost to businesses that experienced a breach in 2018 was $3.9 million.[30] Additionally one cannot generalize data breaches or data theft as being similar across industries. In the report, *Data Breaches: Risk, Recovery, and Regulation*, by the Wisconsin Legislative Reference Bureau, payment data is only stolen in four percent of all health industry breaches, but it is stolen in 93% of all hospitality industry breaches.[31]

The average cost to businesses that experienced a breach in 2018 was $3.9 million.

California was the first state to enact a data breach law in 2002. As of 2018, all 50 states have some form of breach law. Many states have modified or are considering a modification of their breach laws by expanding the definition of personal identifying information, adopting broader notification requirements, and/or requiring specific timeframes for when a breach notice should take place.[32]

---

26 Verizon, *2019 Data Breach Investigations Report*, 2019, p. 19.

27 Ponemon Institute, *Cost of a Data Breach Report*, July 2018, p. 32.

28 McLaughlin, Heather. Identity Theft Resource Center. "Identity Theft Resource Center®'s Annual End-of-Year Data Breach Report Reveals 17 Percent Increase in Breaches over 2018." Accessed August 6, 2020. https://www.idtheftcenter.org/identity-theft-resource-centers-annual-end-of-year-data-breach-report-reveals-17-percent-increase-in-breaches-over-2018/.

29 Identity Theft Resource Center. "Data Breaches." Accessed July 2, 2020. https://www.idtheftcenter.org/data-breaches/.

30 Shepard, Sidney. *Security Today*. "The Average Cost of a Data Breach." Accessed July 3, 2020. https://securitytoday.com/articles/2018/07/17/the-average-cost-of-a-data-breach.aspx.

31 Rosenberg, Alex. *Data Breaches: Risk, Recovery, and Regulation*, May 2019. Wisconsin Legislative Reference Bureau.

32 National Conference of State Legislatures. "2019 Security Breach Legislation." Accessed August 11, 2020. https://www.ncsl.org/default.aspx?tabid= 33382.

Other Privacy and Security Related Laws and Legislation

Wisconsin's neighboring states have also undertaken legislative efforts related to data privacy, security, and breaches. Michigan adopted the Cyber Civilian Corps Act, which created a program where volunteers could help respond to cybersecurity incidents. The new law also created a Michigan Cyber Civilian Corps (MiC3) and provided protection from liability for personal injury and property damage for its members when acting in their capacities as a volunteer of MiC3.[33]

Further south, Illinois adopted the Biometric Information Privacy Act, a law that protects biometric identifiers, i.e. a retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry, from breach. This law requires entities that collect personal information through the Internet to disclose that information and requires individuals to consent to the collection, or opt in. It also allows individuals to file lawsuits if damages result from a breach of their biometric data.[34]

Wisconsin 2019 Legislative Session

In late 2019 and early 2020, the topic of consumer data protection generated widespread attention in Wisconsin. During the 2019 state legislative session, several legislators introduced five significant pieces of legislation.

2019 Senate Bill 784 / 2019 Assembly Bill 819

Senator Patrick Testin and Representative Kevin Petersen introduced companion bills during the 2019 legislative session that addressed cybersecurity for insurance data. 2019 Senate Bill 784 (introduced February 6, 2020) and 2019 Assembly Bill 819 (introduced January 29, 2020)[35] closely model legislation suggested by the National Association of Insurance Commissioners (NAIC). The Wisconsin Insurance Alliance, working with the Office of the Commissioner of Insurance (OCI), supported the bill, which has also been favored by the United States Department of Treasury.[36] Similar bills have become law in eleven other states: Alabama, Connecticut, Delaware, Indiana, Louisiana, Michigan, Mississippi, New Hampshire, Ohio, South Carolina, and Virginia.[37]

2019 Assembly Bills 870, 871, and 872

Representative Shannon Zimmerman introduced three bills, 2019 Assembly Bills 870, 871, and 872; collectively titled the Wisconsin Data Privacy Act on February 10, 2020. The bills generated significant public comment at a hearing on February 12, 2020, and Rep. Shannon Zimmerman stated at the hearing

---

[33] MCL 18.221, et seq. (Michigan).

[34] Illinois Biometric Information Privacy Act (740 ILCS 14/).

[35] 2019 Wisconsin Assembly Bill 819.

[36] From the *NAIC Insurance Data Security Model Law, State Legislative Brief*, January 2020: In an October 2017 report on the asset management and insurance industries, the U.S. Treasury Department recommended prompt adoption of the model by the states. Treasury further recommended that if adoption and implementation of the model by the states does not result in uniform data security regulations within five years, then Congress needs to act by passing legislation setting forth uniform requirements for insurer data security.

[37] Weatherford, Holly, Jennifer McAdam, and Chara Bradstreet. *The NAIC Insurance Data Security Model Law*. National Association of Insurance Commissioners, June 2020.

that the legislation was a first step to discussing the issue of data privacy.[38] These three bills share certain definitions and penalties with the European Union's General Data Protection Regulation.

All three bills relied upon the definition of a "controller," defined in the three bills as, "… a person that alone or jointly with others determines the purposes and means of the processing of personal data, but does not include a law enforcement agency or a unit or instrumentality of the federal government, the state, or a local government."[39] The three also rely on the common definition of "personal data," defined as, "… information relating to a consumer that allows the consumer to be identified, either directly or indirectly, including by reference to an identifier such as a name, identification number, location data, online identifier, or one or more factors related to the physical, physiological, genetic, mental, economic, cultural, or social identity of the consumer, but does not include any information lawfully made available from federal, state, or local government records."[40]

2019 Senate Bill 851

Senator Chris Larson introduced 2019 Senate Bill 851 on February 20, 2020. According to the co-sponsorship memo, the bill mirrors the California Consumer Privacy Act (CCPA).[41] The bill established requirements for businesses related to personal information collected about consumers, and defined which businesses would be affected. As a mirror to the CCPA, among other changes, the bill disclosed privacy rights to Wisconsin consumers, defined what information is collected on consumers, and set conditions for the sale or sharing of consumer data. The bill also permitted consumers to delete data in certain situations, and forbade businesses from discriminating against customers who exercised their ability to ask or make requests.

ADVISORY COMMITTEE MEETINGS

Meeting 1: October 22, 2019

The first meeting focused on organizational matters. The membership introduced themselves during a roundtable session and established meeting ground rules of the Advisory Committee. The schedule was outlined, which would consist of day-long meetings, held around the state. Since the Advisory Committee convened in an official capacity, Jane Landretti, DATCP General Counsel, provided an overview of the Wisconsin Open Meetings Law and public records requirements.

Alex Rosenberg, legislative analyst for the Wisconsin Legislative Reference Bureau, provided a presentation on his paper *Data Breaches: Risk, Recovery, and Regulation*.[42] In his presentation, he indicated four major ways that breaches occur: mistakes, theft, social engineering, and hacking. He also indicated four major motives for data theft: money, espionage, fun, and grudge. Mr. Rosenberg also discussed the five stages of a data breach fix cycle: preparation, detection, containment,

The cost of data breaches are borne by consumers and industry.

[38] *Legislative Council Bill Hearing Materials for 2019 Assembly Bills 870, 871, and 872*, 2019-2020 Wisconsin Legislature, statements by various individuals.

[39] 2019 Wisconsin Assembly Bill 870.

[40] 2019 Wisconsin Assembly Bill 870.

[41] Larson, Chris. Co-Sponsorship Memo to Other Wisconsin Legislators, January 23, 2020.

[42] Rosenberg, Alex. *Data Breaches: Risk, Recovery, and Regulation*, May 2019. Wisconsin Legislative Reference Bureau.

recovery, and remediation. He reiterated that *Digital Guardian* rated Wisconsin as 2 out of 5, which translates as "less strict" than other states.

Meeting 2: November 12, 2019

The committee's second meeting focused largely on understanding laws and initiatives in other states. Justin Webb and Sarah Sargent, privacy attorneys with the law firm, Godfrey & Kahn S.C., delivered a presentation titled "Wisconsin vs. the World: A Comparison of Data Privacy & Security Laws." Attorneys Webb and Sargent explained the difference between data privacy and data security. They defined privacy as "how and when information is collected, accessed, processed, and disclosed" and security as "the administrative, technical, and physical measures used to protect information." They asserted that you cannot have privacy without security.

The two also differentiated between access and acquisition of data. A data breach involving the *access* of data could include the mere opening or viewing of information, while the *acquisition* of data requires something more such as printing, transferring, copying, or selling a file.

As part of the second meeting, the Advisory Committee broke into small group discussions to develop a list of priorities related to data breaches.

Meeting 3: December 10, 2019

The third meeting focused on privacy and security legislation from other states. Maureen Mahoney, a policy analyst for Consumer Reports, spoke on data privacy and security efforts from around the country and provided the consumer perspective. During her presentation, "State Privacy and Security Legislation," she stated that there were few data security laws in the country. For instance, there is no across-the-board federal data security requirement and only about half of the states have a general data security requirement.

Mahoney also spoke about how the difficulty to prove harm in a data breach has hindered attempts to enforce certain data security notification and data security statutes. This has been a difficult legal standard for data security.

Mahoney stated that Consumer Reports has found Wisconsinites are concerned about the security and privacy of their data. Consumer Reports believes that more needs to be done to curb unauthorized access to consumer data.

Preventing unauthorized access to data matters to Consumer Reports. Many items today have an Internet connection (refrigerators, smart speakers, etc.) in what is called the "Internet of Things." To ensure consumers are fully protected from data breaches, Consumer Reports has actively pursued regulation of these household items that continuously access and collect information about consumers.[43]

Mahoney also suggested that concerns about unauthorized disclosure may no longer be based solely on identity theft. A person may not wish for personal matters such as political identification or income level to be known for any number of reasons. This is not just a matter of monetary worth; it is a matter of private personal worth.

[43] While the Advisory Committee did not charge itself with specifically addressing the "Internet of Things," these conveniences overlap with privacy and security concerns.

Mahoney also addressed the enforceability of data privacy and security laws. She indicated that companies will not comply with laws without appropriate incentives to do so. During Mahoney's presentation, one committee member also noted that if a state's laws lack strength and specificity, a business could be compliant with a law but may still not have data security. Lawmakers and regulators must also ensure that the cost of compliance does not outweigh the cost of government enforcement action.

After the presentation, the Advisory Committee broke into small discussion groups to identify best practices for government and industry.

Meeting 4: January 28, 2020

The fourth meeting focused on data privacy and security in Wisconsin and on exploring the business community's readiness to pursue changes related to data privacy, security, and breach. Jonathan Gillman, the founder and CEO of Omniangle Technologies, LLC, gave a presentation in which he provided information about the technology and economics of online browsing. In his presentation, he explained that companies want as much data on consumers as possible, since organizations such as Google pay by the click. A greater number of clicks increases the value of data sold. This creates a disincentive for businesses to be honest about what they plan to do with data collected online, according to Gillman. This also creates a scenario in which a business has no incentive to share information that would assist regulators in successfully clamping down on the data industry. An entire industry has developed around the monetization of consumer data; it may not be easy to resolve the complex issues this new industry creates.

Gillman further explained that the economics of the data industry are complicated by the fact that money is made in both legitimate and illegitimate ways. Gillman cautioned that data can be housed on computer servers in other countries, making it difficult to track and regulate. Indeed, many cyberattacks and fraud occur anonymously, which makes enforcement extremely complicated. If intermediaries are involved, a business may not even know who is paid or where purchasing leads derive. Sometimes, due to the inability to enforce fraud or even find the person committing it, a business who conducts online sales may find it easier to write off losses rather than deal with ineffective regulations. With so many potential limitations, attempts at state and federal regulation can easily complicate the matter further.

The committee's fourth meeting also included an industry panel that addressed Wisconsin business community's readiness for solutions related to data privacy, security, and breach. The participants on the panel were: Scott Eganhouse, the Vice President of TEC Mailing Solutions; Bill Caraher, the chief information officer and director of operations at von Briesen & Roper, S.C.; Chrisann Lemery, healthcare compliance consultant, CL Consulting; Scott Hellberg, director of information security, Sentry Insurance; and Thomas E. Spitz, founder and chief executive officer, Settlers bank.

During the panel discussion, the five panel members agreed that, while there may be legal requirements on the collection and retention of data, consumers and businesses alike hold data protection to a higher standard. They must, since the consequences of a data breach injure both customers and the reputation of the data holder (the business). Institutions generally take on the brunt of this responsibility, since consumers have neither the time nor the inclination to become experts themselves. Institutions also realize they cannot simply rely upon legal standards, since security threats evolve much faster than laws. In fact, the industry panel observed that even information technology professionals may lack some cybersecurity training. The panel also suggested that businesses go through a third-party audit process to

reassure themselves and consumers that security and privacy concerns have been considered and certain standards have been met.

The industry panel also briefly touched on how easy it is for data to be breached, and the importance of taking data security seriously. Some panelists stated that they have even conducted phishing expeditions of their own data in order to test their employees' knowledge and to prevent future mistakes.

Also as part of this meeting, the Advisory Committee members participated in an activity to prioritize the shared goals and objectives in an effort to identify future workgroups.

Meeting 5: April 21, 2020

In the fifth meeting, Richard Wicka, the general counsel for the Wisconsin Office of the Commissioner of Insurance (OCI), presented on 2019 Assembly Bill 819. The bill was based on the National Association of Insurance Commissioners' (NAIC) draft model legislation for the states that was developed after seeking input from their state commissioners, the insurance industry, and consumer representatives.

Attorneys Justin Webb and Sarah Sargent, with Godfrey & Kahn S.C., also presented on three bills introduced in Wisconsin (2019 Assembly Bills 870, 871, and 872) that were collectively known as the Wisconsin Privacy Act. Their presentation compared and contrasted the proposed Wisconsin Privacy Act with the GDPR and CCPA. Unlike other bills, the Wisconsin legislation did not carve out any small business exemptions.

Next, Lara Sutherlin, administrator of DATCP's Division of Trade and Consumer Protection, gave an overview of a survey of Wisconsin consumers conducted by Consumer Reports. Overall, the survey indicated that Wisconsin residents were quite concerned about the issue of data security. (Appendix A)

Finally, Dennis Hirsch, a professor of law at the Ohio State University Law School, gave a presentation entitled, "Advanced Analytics, Privacy and Data Ethics: Implications for Consumer Protection Law."

Professor Hirsch stated in his presentation that when it comes to data analytics and artificial intelligence (AI), privacy laws may not be sufficient to protect consumers. The reason is that privacy law depends on consumers making choices about whether to let others collect or use their personal information. However, Professor Hirsch doubts that the average consumer realizes the many ways in which their data can be leveraged for or against them. Hirsch also doubts that the average consumer realizes how certain purchase decisions can lead businesses to make decisions about individual consumers and their private traits and behaviors. Thus, when it comes to advanced analytics, consumers cannot use the rights that privacy laws give them to protect themselves.

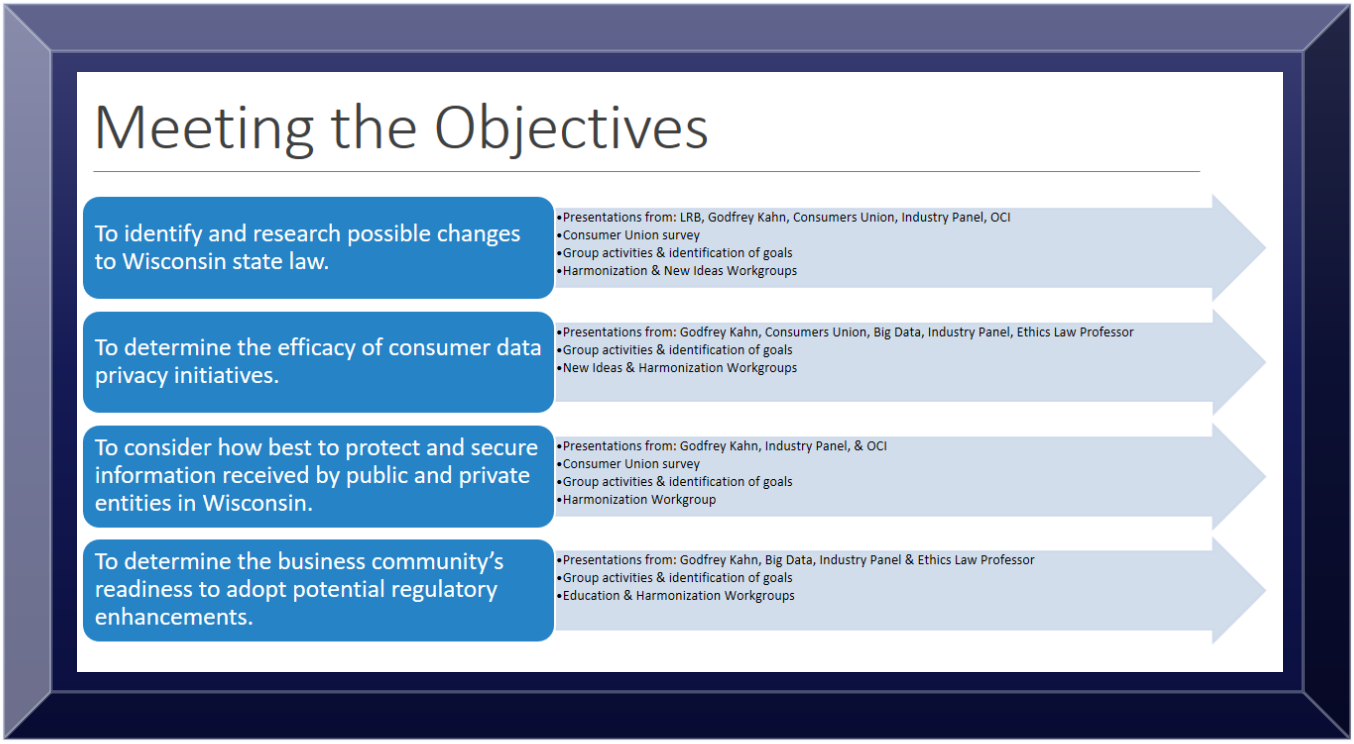
Professor Hirsch's research shows four risks that big data analytics pose: privacy, manipulation, bias, and procedural unfairness. In relation to privacy, he provided an example of a retailer who was able to analyze customer purchase data to infer which of its female customers was pregnant. The retailer marketed baby goods to a 15-year-old girl who was pregnant and had not yet told her father. The father ended up learning of his daughter's pregnancy as a result of this targeted marketing. In such instances, where sensitive data is inferred from other, non-sensitive data such as consumer purchase information, individuals cannot use notice and choice to protect themselves. Yet the public still needs to be protected. Hirsch analogized this situation to food and drugs. People cannot realistically be expected to evaluate every food and drug that they consume. That is why the Food and Drug Administration (FDA) exists.

Hirsch suggested two potential solutions. First, consumer protection laws can fill this gap. State consumer protection agencies generally have the authority to declare certain business practices unfair. They could employ this power to deem the most egregious abuses of data analytics to be unfair business practices, and so limit them. In such a system, consumer protection authority would be acting like the FDA: protecting consumers where they lack the information to protect themselves.

However, such regulation may be far in the future. In the meantime, Hirsch believes that it is in businesses' self-interest to use analytics responsibly and in ways that will protect their consumers. This is the growing field of "data ethics," which Hirsch has studied.

Hirsch and his team of Ohio State researchers interviewed more than twenty leading companies that actively seek to utilize their data analytics and AI in ethical, responsible ways. These companies have explained that, in the absence of laws and government mandates businesses can enhanced their reputations by being known as good stewards of data. This added prestige may also assist in the recruitment and retention of employees. Companies also engage in data ethics in order to preempt government efforts to regulate in ways that business may see as counterproductive. Simply put, Hirsch stated, "Corporate data ethics is beyond compliance risk mitigation; it is corporate social responsibility for data."

Hirsch further explained that businesses have responded to the eruption of the "big data" industry by creating mechanisms within the business to address data stewardship issues. These efforts include the recent creation of a new position – the data ethics officer - as well as data ethics advisory boards that can provide input to company executives. Many businesses locate these positions in their information technology departments rather than their legal departments, to emphasize the importance of doing what is right versus simply doing what is legal.



Meeting 6: May 19, 2020

At the sixth meeting, Advisory Committee members received updates from the three workgroups that were formed to further explore specific areas of Education, New Ideas and Harmonization. Each of the three workgroups had brainstormed ideas during other meetings and offered draft recommendations for presentation, discussion, and feedback at this meeting.

Meeting 7: June 16, 2020

At the seventh meeting, the Advisory Committee members again received updates from the three workgroups. Each workgroup had held additional meetings between the May and June meetings to consider feedback received at the May meeting and to refine the work they had identified.

IDEAS FOR WISCONSIN

Over the course of the nine months during which the Data Privacy and Security Advisory Committee met, members listened to presentations by a number of different data privacy and security experts, participated in large and small group activities and discussions, and did independent research and study on data privacy, security and breach. Time was dedicated to these issues in an effort to meet the committee objectives, gather ideas and insights, and help Wisconsin decide how best to protect consumers as it relates to data breach, data privacy, and data security.

In an effort to dig deeper into the complexities of these issues, the Advisory Committee convened three workgroups that met four times between committee meetings: Education, New Ideas, and Harmonization. The following ideas were identified as possible approaches for Wisconsin to move forward in building protections for consumers and businesses alike in the area of data privacy, security and breach. The workgroups acknowledged these ideas are possible launching points for further discussion, and will require some refinement.

Education

This workgroup discussed ideas for education targeted toward all age levels and audience types using various media platforms. The group also discussed a one-stop repository of information, with uniform language available so all users can readily understand the complexities of data privacy and security. They discussed the need to use multiple data sources, such as the Consumer Reports survey (Appendix A) and the results from the 2020 Census. They also considered demographics to determine what approaches could be effective for both consumer and small business education. The workgroup also considered a wide range of audiences who may require education and what each group would need with the use of a variety of education platforms.

The Education Working Group developed two central ideas:

- Work with industry to develop and train on minimum standards for identifying, securing, and maintaining consumer data; and
- Develop a Consumer Data Privacy and Security Hub, looking to the Cyber Security "Hub" from Indiana as a basic model.[44] The Hub would facilitate cross-agency connections to information.

  The workgroup believed that such a "Hub" could provide both the public and businesses access to a compendium of data privacy and security best practices. The Hub would draw upon a number

[44] IN.gov, "Education." Accessed July 2, 2020. https://www.in.gov/cybersecurity/3827.htm.

of resources from across state government including the Department of Public Instruction; the Department of Justice; the Department of Health Services; the Department of Financial Institutions; and the Department of Agriculture, Trade and Consumer Protection. Content ideas for the Hub include a toolkit for consumers and businesses, sample presentations for various audience types, sizes and languages, frequently asked questions related to data privacy, security and breach, resources for identifying best practices and standards, and the ability to ask questions.

New Ideas

This workgroup explored new and innovative ideas that were mentioned by speakers and members during the full Advisory Committee meetings. The workgroup first considered the data broker registries in Vermont and California. The workgroup was concerned that while California's law was broader in scope than Vermont's, neither required some of the largest collectors of data (such as Amazon and Google) to register, and thus questioned the effectiveness of a registry without those major players.

The group further contemplated whether the use of registration fees from a registry could be used to create a "Victim Recovery Fund" to assist victims of a data breach and also establish a data privacy and security support group for small businesses and consumers to exchange information (i.e. The Hub from the Education Workgroup). In addition, they thought a team of experts could be developed to respond to incidents as a public-private partnership. Another possibility would be modeling a response program after the Ohio Cyber Reserve.[45] Vetting members of any team would pose a challenge to ensure they had the requisite level of expertise to respond to data incidents and, perhaps more significantly, that they could be trusted with the security of data they are charged with security. Another challenge is identifying the level of immunity that a volunteer would be provided based on their expertise.

> *"…Companies should allow users to restrict data shared with others–and make it easy to do so. There should be some way to be able to find out which sites have your data and block any information from being shared."*
>
> *Debra-Jean, Vernon, WI – Consumer Reports*

The workgroup shared a concern that data collected by industry on consumers may not always be accurate, and that consumers should have a right to correct that data. They discussed the possibility of creating a barrier where data cannot be transferred without the consent of the individual. The workgroup explored a system similar to PayPal where Wisconsin consumers could update their preferences in terms of global privacy settings, cookies, retention of data, and the ability to review preferences from time to time. This new system would allow a consumer's data privacy preferences to travel with them from business to business. When similar efforts have been attempted in the past, the stumbling block has been in the implementation. For example, committee members questioned when consumer preferences would be enforced – at the point of collection or at the point of transfer. This system could be meaningful and provide clarity for both consumers and businesses, but its development would require significant further exploration.

Members also expressed concerns about how small businesses could comply with laws and protect the data they collected and stored with more limited resources. Recognizing that businesses are also the victims of security breaches that can result in significant financial harm, members discussed the idea of

[45] The Cyber Reserve, created under Ohio Revised Code, § 5922.01, is a volunteer force under the auspices of the Adjutant General of the Ohio State National Guard. Trained civilians are to assist with cybersecurity vulnerabilities and to provide recommendations to reduce cyber threats.

imposing an insurance requirement on business to protect themselves against data breaches. A business could determine how much protection it may need based on the level and type of data security a business had in place. The group also discussed the concept of creating a "Safe Harbor" provision in the law, which would shield a company from liability in the event of a breach, provided the company adheres to accepted industry best practices related to data security.

Finally, the workgroup discussed the feasibility of regulating the algorithmic manipulation of data to prevent its often-discriminatory result on legally protected classes, such as older citizens, women, and people of color. Professor Hirsch underscored the existence of this type of algorithmic bias when he shared a story of a retailer that received a large number of resumes. In order to prioritize the resumes, the retailer analyzed whom they had hired in the past and screened for those attributes. As a result, the created algorithm began to reject resumes of female applicants. Examples such as these prompted the workgroup members to agree that the ethics of data manipulation should be deliberated as business entities utilize data analytics.

Here is a summary of this workgroup's ideas:

- Create a Data Controller Registry in the state of Wisconsin that collects fees and requires the following of businesses: best practices for data security, data security insurance, and algorithm accountability practices. Any assessed registration fees would be required on a sliding scale depending on the size of the business.

  The workgroup suggested a Data Controller Registry so Wisconsin could have a basis of who collects, stores, uses and shares Wisconsin consumers' data. With a desire to encompass all levels of business that collect, store and share data, rather than just the large data brokers that collect, buy and sell data. "Controller" would be defined as a person that alone or jointly with others determines the purposes and means of the processing of personal data, but does not include a law enforcement agency or a unit or instrumentality of the federal government, the state, or a local government. This definition closely mirrors the definition of controller from the GDPR.
- Create a fund to assist victims of breaches using the fees collected from the Data Controller Registry.
- Establish a Data Privacy and Security support group for small businesses and consumers to exchange information, supported from fees collected from the Data Controller Registry.
- Create a barrier to transferring data without the consent of a person to transfer data.

  This concept could be based on the PayPal model and should include exemptions related to law enforcement, healthcare, fraud investigation, etc. Exemptions would need to be included for data that may be required to conduct business and/or is governed by federal law. Consumer user fees could potentially support this system.

Harmonization

This workgroup was charged with discussing the need for harmonization of consumer data privacy, security, and breach regulation in Wisconsin with other regulatory frameworks. The workgroup analyzed the legislative proposals that were introduced during the 2019 Wisconsin legislative session, identified the pros and cons of each proposal, and provided recommendations for ideas and concepts that may have been overlooked or left out. The workgroup also considered harmonization with other states in terms of laws and proposed legislation. These discussions frequently led to further deliberation about the

challenges of various approaches; these challenges are outlined in the "Looking Ahead" section of this report.

Specifically, the workgroup explored the idea of expanding the definition of personal identifying information; defining small business; whether acquisition of data or access to data should constitute a data breach; and should the data protected simply be electronic data or if physical data also needs to be protected by laws and standards. The group also discussed the concept of allowing a consumer a binary choice to opt in or opt out of privacy settings, and whether future legislation should include a private right of action. The workgroup grappled with whether or not businesses should conduct risk assessments to determine what exposure they have and what exposure their customers have if data is lost or stolen. Since not all data is of equal value, laws and standards need to have perspectives that do not treat all data similarly.

The workgroup discussed at length how any Wisconsin laws would need to recognize existing federal regulations of a wide variety of industries and data sets, i.e. Health Insurance Portability and Accountability Act (HIPAA) and Gramm-Leach-Bliley Act (GLBA). If Wisconsin were to enact new laws, it would need to consider who and what is already regulated and in what way, so as not to conflict or duplicate. A few other states have carved out exemptions if the industry already has sufficient regulation.

Discussions by the workgroup also suggest that not all solutions need to be legislative. The group suggested that industries look into NIST, ISO, and other industry standards to provide guidance on a security program. Following these standards would provide confidence to industry and its consumers that should a security event occur, data is either kept safe through encryption or through other standardized protocols. Due to complexities from one organization to another based on size, amount of data, and generated revenue, one size does not fit all.

While discussions of this workgroup involved a number of complex issues that require further consideration, the members did come together on some important concepts. The workgroup agreed that any legislative package in Wisconsin should:

- Be a comprehensive package including data privacy, security and breach,
- Include harmonization of definitions,
- Have considerations for small business,
- Avoid conflicting with other regulations.

While there is no reporting requirement, DATCP endeavors to collect data on breaches impacting Wisconsin businesses and consumers. Visit datcp.wi.gov for this important resource.

LOOKING AHEAD: INSIGHTS FOR CONSIDERATION AND EXPLORATION

There are a number of areas where industry, regulators and consumers have common goals. How to reach those goals can be a difficult path. What we do know from the work of DATCP's Data Privacy and Security Advisory Committee, however, is that government agencies, consumer groups, and businesses can work well together, and their partnership will be integral to any solution. These collaborative efforts need to continue as all Wisconsinites acknowledge that the collection of data involves a trust between a consumer and an organization (business or government). With this trust comes a responsibility to keep consumers' data safe from abuse and possible identity theft.

Trying to decide how best to address issues of data privacy, security, and breach requires set, agreed-upon, and legal definitions of those terms. The committee universally believes in the importance of all three.

However, implementing a new regulatory structure poses a number of significant, interrelated complex issues and concerns. As stated, the number of data breaches in the U.S. and around the world continues to increase, and companies and consumers simply cannot avoid them. It is a matter of when, not if, a data breach will happen. The severity of the breach will differ; in some cases, data may have been accessed (read over a shoulder at a coffee shop) or acquired (downloaded from a server). The degree of harm should be a consideration in the decision about whether to report a breach and to what extent mitigation may be necessary. A business will want to investigate and possibly involve law enforcement as both consumers and businesses could suffer from theft. While the priorities could conflict, consumers need to know, businesses need to investigate, and culprits must be caught.

The following are specific topics related to data privacy, security and breach with points for consideration and additional exploration. These suggestions came from considering the public comments (Appendix B), and resulted from in-depth conversation among committee members both in the workgroups and during the full meetings, when looking ahead at what may be next for Wisconsin.

Harmonize the Definition of Personally Identifiable Information (PII)

Data that is not currently covered in Wisconsin's definition of personally identifiable information (PII) but is found in other states' laws includes such information as date of birth, usernames, e-mail addresses, all passwords, security questions, passport numbers, tax identification numbers, student identification numbers, mother's maiden names, and tribal identification cards. Not all information is of equal value: while a birthday may be obtained by following greetings on social media, a password would be more useful to an identity thief. Therefore, exposure of data elements need to be assessed for value with special attention granted to data that, if compromised, could be more devastating to the consumer.

Any proposed legislation should consider the nature of the risk that the regulation is attempting to mitigate and balance that against the rigor of the proposed legislation. For example, any expansion of the definition of PII should include a risk assessment of the data element disclosed. That is, will the disclosure of this information harm the consumer? Data that is already in the public realm should not be included in this definition unless it is combined with other identifying personal information, i.e. date of birth in combination with a Social Security Number.

Another matter for consideration is how consistent Wisconsin's definition of PII is with other states and federal laws. If the definition of PII were more uniform with other states, the industry would likely find it easier to comply when reporting a data breach.

Likewise, if federal law already requires robust breach reporting of a certain industry or data set - that should be exempted in Wisconsin law. HIPAA and GLBA are common examples of this. In the health information world, professionals call PII "protected health information" or PHI. HIPAA defines 18 different items as PHI. Some of them coincide with what many states consider PII (names and social security numbers), while some are things that states usually do not include (vehicle numbers and medical device numbers). Washington's recently updated data breach law is a good example of this. Taking effect in

March 2020, Washington's law expanded its PII definition but carved out exceptions for certain federal laws with breach reporting requirements.[46]

In contrast, the Gramm-Leach-Bliley Act (GLBA) protects PII from a data security standpoint in that it requires that financial institutions fulfill three requirements: collected personal information must be securely stored; consumer advice on how the data will be used; and instructions on how to opt out of particular uses of that data. The differences between how these two federal laws treat personal information demonstrates the difficulties that occur when addressing improvements in the various countermeasures.

While consumers may worry about the use of their data, businesses still need data to serve their customers and to engage in marketing activities. Therefore, a compromise was suggested by some committee members: data could be encrypted or de-identified so that it could still be used for the purposes of business and targeting messages. Concerns were raised that this process is expensive and becomes unworkable if applied broadly, as would be the case with a very broad definition of PII. Deidentification accomplishes a similar result without many of the operational challenges that come with encryption. However, it was noted that neither encryption nor deidentification may work in the scenario of targeting messages, as targeting requires identifiable contact information.

An additional point to consider is whether the definition of PII should be harmonized across a package of data privacy, security, and breach regulations. One could argue that if the definition were consistent across all three areas, a consumer would readily know what regulations apply to that information. However, while a harmonized definition of PII for data privacy, security and breach seems at first to simplify and harmonize, it could be problematic in practice. An idea for moving forward while preserving some consistency, but recognizing different contexts is to define "sensitive personal information." Generally, sensitive personal information could be defined by a list of categories that may present increased risk and are thus subject to additional obligations and protections.

Consideration for Existing Regulations

As stated in a letter provided to the committee, various industries (Finance, Healthcare, and Insurance) are already required to protect certain PII under federal regulations such as the Fair Credit Reporting Act (FCRA), HIPAA, GLBA, and the Right of Financial Privacy Act (RFPA). (Appendix C). Many states create exemptions in their state law to recognize these existing regulations. When considering exemptions for existing regulations, there are two approaches – exemption for the data itself or an exemption for the industry. States take differing approaches. For instance, the CCPA provides an exemption for the *data* covered by federal law. Washington, on the other hand, exempts the *industry* if it is already regulated.[47]

Creating a workable exemption is also complicated by the different standards deployed in state and federal law. In the absence of an exemption, state regulations could contradict federal regulations thus causing problems and confusion.

Consideration for the Size of Business and Nature of Risk

When considering to which entities a law should apply, one must define "small business." For instance, the California Consumer Privacy Act (CCPA) created a definition that sets certain legal parameters along

[46] Washington State Legislature. *Final Bill Report, SHB 1071*. March 1, 2020.

[47] Washington State Legislature. *Final Bill Report, SHB 1071*. March 1, 2020.

with gross revenues, number of records, what percentage of the revenues derive from the sale of personal information, and other definitions. Of course, a determination would need to be made if California standards are appropriate or if differing standards would serve Wisconsin better. Even entities that would classify as small in size, in terms of employees or revenue, may collect and process a large, important amount of data. Finding a definition that is not onerous but still protects consumer data is certainly a challenge.

While each industry encounters differing threats at differing levels, another important consideration in classifying the size of a business is pointed out in the *2019 Data Breach Investigations Report* by Verizon. According to this report, only 10 percent of all breaches involve the financial sector, and 43 percent involved small businesses.[48] Given these numbers, it is worth considering what measures a business may already have in place to minimize the risk to the data they collect and hold. Small businesses simply do not have the infrastructure or the staffing to provide the security that a larger organization can. Still, the data needs to be protected, for the benefit of both the business and their customers. Issues of controlling access and conducting risk assessments should be considered in decision-making and in the creation of information security programs.

A risk assessment could take one of two paths. First, a corporation could become a good data custodian through the creation of privacy officers, data ethics officers, and oversight boards who can advise on such matters. Second, businesses could, and should, look at industry standards adopted by NIST and ISO. Since these standards are subject to continuous updating and discussion, adoption of these standards could address the challenges presented by rapidly changing technology. With this in mind, an industry-by-industry approach to business readiness may be the most productive.

Data Breach: Acquisition of Data or Unauthorized Access to Data?

Data access means that information has been opened and viewed (which represents a privacy violation). Data acquisition means that data was downloaded, transferred, printed, copied, or otherwise acquired (presenting the ability for theft to a consumer's identity).[49] Data breach laws usually govern the *acquisition* of data by unauthorized individuals versus *access*.

In analyzing the right approach, regulators and lawmakers must consider the notion of harm. The question that stands is: when does harm begin? When data breaches are defined as data acquisition, this supposes potential financial harm or identity theft. Conversely, while having one's data accessed may not translate into a definite harm, access to personal information may feel as devastating to a consumer as an identity theft. Laws and policies must recognize the uncertainty of whether a consumer may fear acquisition, access, or both. However, they must also recognize the strain on business this choice can have. An "all in" or "all out" approach may not accommodate the multifaceted use of consumer data.

Data Breach: Who to Report to? What to Report?

In Wisconsin, reporting of data breaches to public authorities is not required, but they must be reported to consumers. In most states, businesses are required to report data breaches to a governmental authority like the state attorney general. This reporting typically requires specific information be disclosed

[48] Verizon, *2019 Data Breach Investigations Report*, 2019, p. 5.

[49] Webb, Justin and Sargent, Sarah. "Wisconsin Vs. The World: A Comparison of Data Privacy & Security Laws." DATCP Data Privacy and Security Advisory Committee, November meeting, 12 Nov 2019, Northeast Wisconsin Technical College, Green Bay, WI.

in a letter or communication to both consumers and an enforcement agency. The members of DATCP's Data Privacy and Security Advisory Committee agree that Wisconsin should follow the lead of other states and require direct reporting to a governmental authority, such as DATCP and/or the Attorney General. It should further consider including the chief regulator for a particular industry (i.e. Office of Commissioner of Insurance or Department of Health Services) in the reporting process, as some states require. This additional reporting could inform the authority most in a position to help affected consumers. However, expanded reporting could also put a strain on business.

Currently, Wisconsin law does not require that any specific information be included in notification letters sent to consumers. However, most states do specify what should be contained in these notices. California and Washington, which have become models followed by many other states, require these letters to explain what happened, what information was involved, how long the breach has been going on, what the entity is doing about the problem, what the breach victim can do, and who to contact for additional information. Uniform breach notification requirements across state lines can ease compliance for multistate companies that experience a breach.

Data Breach: Enforceability

Wisconsin is an outlier in that its breach notification law lacks an enforcement provision. Any modernization of this law should include the ability of the government to enforce it with appropriate penalties for a violation. This is essential for the law to be effective at ensuring those impacted by a data breach are duly informed. For instance, DATCP enforces consumer regulations such as unfair billing; product safety; and untrue, deceptive and misleading representations in Chapter 100 of Wisconsin statutes. However, DATCP does not have legal authority to enforce the data breach laws in Chapter 134.

In California, the CCPA tasks the Attorney General's office with rulemaking and investigation. In Wisconsin, other agencies have the authority for rulemaking and investigation. Those agencies in turn refer appropriate cases to the Department of Justice for adjudication. Any bills the legislature considers should account for the roles and discretion of the appropriate agency.

Private Right of Action

Private rights of action can be a mechanism for enhanced enforcement of consumer data laws. Take, for example, the enforcement of a data breach law. Breaches can be both large and small, impacting a handful of people or as the case with Equifax, millions. Government enforcement typically occurs when a breach is egregious and/or there is significant harm. This is because the number of cases that prosecutors may pursue is limited (in both time and resources). Smaller cases, with limited harm, often are not pursued by law enforcement. For this reason, allowing individual consumers to pursue action independently may provide relief where none would otherwise be available. Private rights of action can put an undue burden on business, however, leading to significant expenses in litigation or other mitigation efforts. Lawmakers will need to strike a balance between these competing interests.

Consumer Autonomy of Data: Opt-In vs Opt-Out

In order to conduct business, some amount of data sharing must occur. At the very least, if a person pays with a credit card, financial data must be shared. In a brick and mortar store, a consumer may shop without leaving behind information about purchases they considered but did not make. Online, however, these would-be purchases can be part of an algorithm. While businesses may find this data to be vital, consumers may not agree. For this reason, discussions have been held nationwide about whether

consumers should have the option of opting in or opting out of the collection of their data. The adoption of the CCPA and the GDPR has forced this question into law and public policy.

Opting in means a consumer must affirmatively consent to their data being collected. Online, such action typically requires a checkbox to agree to a privacy policy, accept cookies, or create an account to receive newsletters. In contrast, opting out means a consumer takes an action to deny their consent. For example, a promotional email may contain a link to "unsubscribe."

> *"…Practically every company (website) entry and contract says they have the right to share your information with others, and their third party partners. No they don't. That shouldn't be allowed…."*
>
> *Colleen, Lake Geneva, WI*

While GDPR leans in favor of allowing consumers to opt in to having their data used, CCPA utilizes an opt out framework. Since Europe is a large market and California is the largest state in the United States, many of their decisions impact multistate and multinational businesses already operating in Wisconsin.

While such policies are attractive to many, there are a number of considerations that could complicate their effective implementation. For instance, a consumer may find benefit in sharing information that results in discounts at their favorite store, but may understandably be less eager to share details about their online medical inquiries. Stricter guidelines could also inadvertently tie the hands of businesses. For instance, a health care facility may need to release certain information to third-party billing authorities. A bank may need to release certain financial information as well. However, if the consumer does not authorize such a release, the bank may not be able to share data—possibly to the detriment of the consumer, or even in violation of other laws. While opt-in may work for specific circumstances, many believe an across-the-board opt-in approach would not work.

The approach set by Nevada could be considered, where a verified opt-out would simply exempt consumer data from targeted advertising.[50] CCPA became fully operational on July 1, 2020, and Wisconsin should monitor their successes and failures in this context. As one of the public comments that the Advisory Committee received stated, "… (D)ata privacy and security laws are complex, and any regulatory scheme must weigh the preferences of consumers against the needs of businesses that process personal data." (Appendix C).

Self-Regulation by Business

Both consumers and businesses agree that the technology of data collection changes rapidly. By the time a law is enacted, that law itself may no longer be relevant.

Professor Hirsch stated in his presentation that privacy laws may start a conversation, but true help for consumers may come through what he calls "big data ethics." He warns that current data privacy laws are insufficient to address the ethics of manipulating the consumer data collected, stored and shared by businesses. He posed the question of whether data collectors have a fiduciary duty to consider human rights, bioethics, or philosophical ethics when storing and manipulating consumer data. Professor Hirsch reported that leading companies are taking these ethical complexities seriously and are going beyond compliance to mitigate these risks. He suggested that businesses need to consider what corporate data ethics should mean to them and how they can deliver best practices to consumers. Even in the absence of laws and government mandates, businesses can enhance their reputations by being known as good

[50] NRS 603A (Nevada).

stewards of data. This added prestige may also assist in the recruitment and retention of employees. Engaging in corporate data ethics could also preempt government efforts to regulate in ways that may be counterproductive to both businesses and consumers. Simply put, Hirsch stated, "Corporate data ethics is beyond compliance risk mitigation; it is corporate social responsibility for data."[51]

In addition to Hirsch's comments, at an industry panel conducted at the January meeting, five Wisconsin data professionals who work intimately with consumer data attested that being good data custodians actually benefitted them with more satisfied customers. Generally, people want to trust that businesses will do what is right for consumers.

As more businesses begin to explore self-regulation and adherence to "big data ethics," Consumer Reports and other consumer advocates recommend that states instead incorporate the Digital Standard they devised when drafting legislation. The Digital Standard provides a set of criteria for consumers to use when evaluating a business' data privacy standards:

- I can see and control everything the company knows about me.
- I can easily find, read, and understand the privacy policy and/or terms of service. My account and information are deleted when I leave the service.
- I know how long the company keeps my information. Every piece of data I share brings me a benefit and does not just help the company.
- I know what user information this company is collecting.
- The only information the company requests from me is what's needed to make the product or service work correctly.
- The default settings in this product prioritize my privacy. To give up privacy, I actually need to change the settings.
- The company explicitly discloses every way in which it uses my data.[52]

Need for a Federal Approach

Some question whether there is a need for a federal approach. Differing laws in differing states can and do cause confusion for both businesses and consumers. Several public comments demonstrated a desire for the federal government to take a more active role in both legislation and in regulation.

However, similar to the consideration for a private right of action, the federal government's limited resources may result in limited enforcement. This could mean many violations go unaddressed. For this reason, some members of the committee agreed that individual states should have the ability, through their own state laws or enforcement of federal law, to pursue an action independently in order to seek relief for the citizens of its states.

Currently numerous federal laws impact data privacy and security including the Health Insurance Portability and Accountability Act (HIPAA), the Fair Credit Reporting Act (FCRA), and the Gramm-Leach-Bliley Act (GLBA). While some bills have been introduced on the national level that would address certain concerns, there remains no comprehensive package related to consumer data privacy, security and breach to protect consumers. Of course, Wisconsin continues to have an obligation to address the needs of its citizenry as they relate to data privacy and security, with or without federal action.

---

[51] Hirsch, Dennis. "Big Data Analytics: Risks, Ethics and Regulation." DATCP Data Privacy and Security Advisory Committee, April meeting, 21 Apr 2020, WebEx Meeting, Madison, WI.

[52] *The Digital Standard*: https://www.thedigitalstandard.org/. Accessed July 2, 2020.

CONCLUSION

Regulation of data privacy, security and breach presents a whole host of complex and important issues. The decision of whether, who, what, and how to regulate will have significant impacts on the residents of Wisconsin and its economy for years to come. This report outlined the work of the Data Privacy and Security Advisory Committee and presented information as Wisconsin considers its next steps to move forward in protecting consumers' data. It is not a directive, nor is it an exhaustive summary of all the steps that should be taken to address challenges of data privacy, security, and breach. In fact, this report should be merely the first of many steps. Addressing those next steps effectively will require the sustained involvement of multiple parties, including consumers, businesses, industry leaders, industry standards organizations, legislators, and regulators alike, to meet the challenges of a data driven economy.

Wisconsin Privacy Survey

2020 Online Survey

Prepared by CR Survey Research Department

February, 2020

INTRODUCTION

In January 2020, Consumer Reports conducted an online survey of Wisconsin residents. The purpose of this survey was to assess Wisconsin residents' expectations, concerns, and experiences with companies collecting, storing, and sharing their personal data.

Ipsos Public Affairs (Ipsos) administered the survey through its KnowledgePanel® to a representative sample of 649 adult Wisconsin residents.

HIGHLIGHTS

Companies Should be REQUIRED by Law to Keep Wisconsinites' Personal Data Secure

- MOST **(94%)** Wisconsinites say **companies should be REQUIRED by law to keep their personal data secure** (i.e., protected from unauthorized access).

Notifications that Should be Required in a Data Breach

- Nearly ALL Wisconsinites **agree that companies should be required to provide notifications in the event of a data breach.**
    - 97% of Wisconsin residents AGREE that companies should be REQUIRED to notify them if their data has been breached.
    - 96% of Wisconsin residents AGREE that companies should be REQUIRED to notify them if their data has been breached, EVEN if it does NOT create any financial risk such as identity theft or fraud.

Experienced a Data Breach

- **Forty-six percent of Wisconsin residents say they have experienced a data breach** where their personal information was stolen or exposed.

Concern about the Collection and Storage of Personal Data

- **Forty-six percent of Wisconsinites** say they are **"extremely/very concerned" about HOW MUCH data** companies collect and store about them and an additional 36% are moderately concerned.

- More than half **57% of Wisconsin residents are "extremely/very concerned" about the SECURITY and PRIVACY of their own personal data** that companies collect and store about them and an additional 29% are moderately concerned.

Worry About Companies Tracking Online Behavior

- **Eight in 10 Wisconsinites** say they are **worried** (20% very worried and 61% somewhat worried) about companies tracking their day-to-day online activities and **14%** say they are '**not at all worried.'**

Confidence in the Security of Personal Data

- More than a third **(35%)** of Wisconsinites say they are **'not at all confident'** that their personal data, such as their social security number, finances, or other personal information, is kept secure and not accessed without authorization.

Companies Sharing Personal Data

- Wisconsin residents say that companies SHOULD NOT BE ALLOWED to share their data **at all or at least without some restriction.**
    - **Half of the Wisconsin residents** we surveyed say companies **should not be allowed to share their personal data** and more than a third (**36%) say companies can do this as long as they get permission each time.**
- **Zero percent of Wisconsin residents** say companies should be able to **share their personal data without any restrictions.**

Control Over Personal Data

- **Seven in 10** Wisconsin residents say they **'strongly disagree/disagree'** that they feel in control of their personal data that companies collect about them.

Personal Data Security Now, Compared to Five Years Ago

- More than half **(55%)** of Wisconsin residents say they believe their data is **much less secure (17%) or less secure (38%) than it was five years ago.**

NOTIFICATIONS THAT SHOULD BE REQUIRED IN A DATA BREACH

Nearly ALL Wisconsinites **agree that companies should be required to provide notifications in the event of a data breach.**

97%

OF WISCONSIN RESIDENTS
AGREE COMPANIES SHOULD BE **REQUIRED** TO NOTIFY
THEM IF THEIR DATA HAS BEEN BREACHED

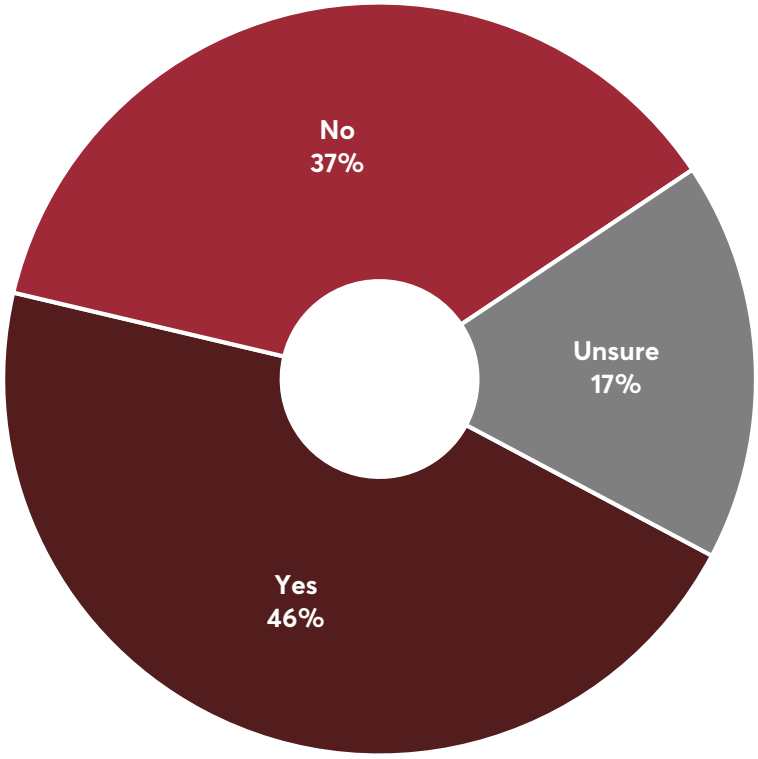
96%

OF WISCONSIN RESIDENTS
AGREE COMPANIES SHOULD BE **REQUIRED** TO NOTIFY THEM
IF THEIR DATA HAS BEEN BREACHED
EVEN IF IT DOES NOT CREATE ANY FINANCIAL RISK SUCH AS IDENTITY THEFT OR FRAUD

EXPERIENCED A DATA BREACH

Forty-six percent of Wisconsin residents say they have experienced a data breach where their personal information was stolen or exposed. Seventeen percent say they are 'unsure' if they have experienced a data breach. A larger percentage of males (22%) than females (12%) say they are unsure.

HAVE YOU EVER PERSONALLY **EXPERIENCED A DATA BREACH?**



Base: Wisconsin residents

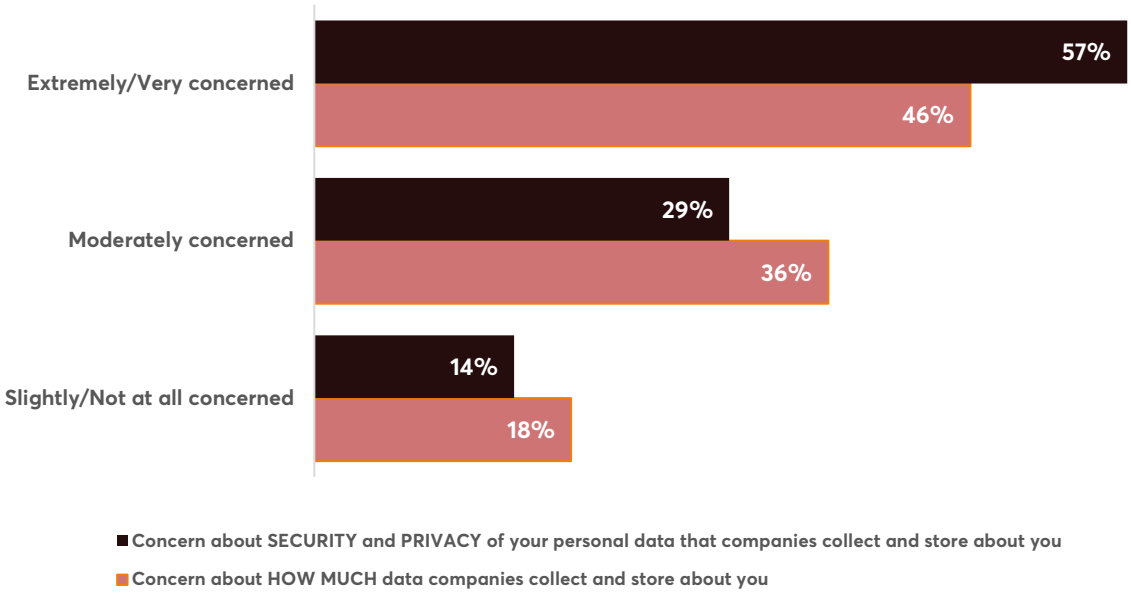
CONCERN ABOUT COLLECTION AND STORAGE OF PERSONAL DATA

We asked Wisconsin residents first about their **concern regarding HOW MUCH** data companies collect and store about them and second, their **concern about the SECURITY and PRIVACY** of the personal data that companies collect and store about them.

Forty-six percent of Wisconsinites say they are **"extremely/very concerned" about HOW MUCH data** companies collect and store about them and an additional 36% are moderately concerned. More than half **of Wisconsin residents (57%) are "extremely/very concerned" about the SECURITY and PRIVACY of their own personal data** that companies collect and store about them and an additional 29% are moderately concerned.

Millennials are less likely than Baby Boomers or the Silent Generation to be concerned about how much data is collected about them and less likely to be concerned about their security and privacy of their personal data that companies collect and store about them.

CONCERN ABOUT **DATA COLLECTION AND STORAGE**



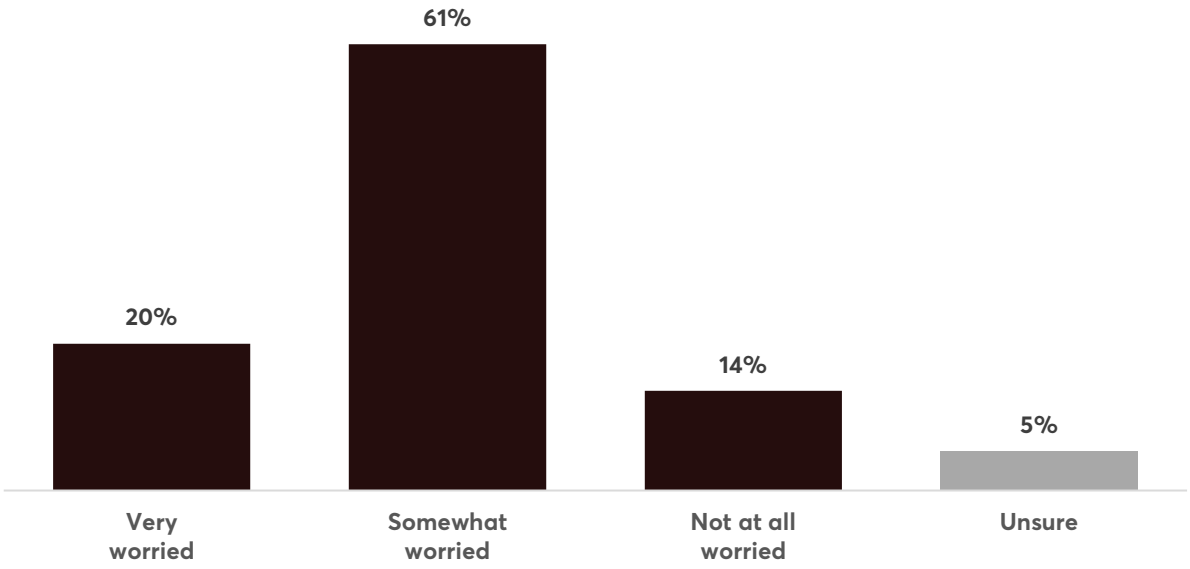
Base: Wisconsin residents

A larger percentage of Wisconsin residents **who have personally experienced a data breach (62%)** than those who **have not (50%),** say they are **"extremely/very concerned" about the security and privacy of their personal data that companies** collect and store about them.

WORRY ABOUT COMPANIES TRACKING ONLINE ACTIVITIES

Eight in 10 Wisconsinites say they are **worried** (20% very worried and 61% somewhat worried) about companies tracking their day-to-day online activities while **14%** say they are '**not at all worried.'**

HOW WORRIED ARE YOU ABOUT COMPANIES **TRACKING YOUR BEHAVIOR** DURING YOUR DAY-TO-DAY ONLINE ACTIVITIES?



Base: Wisconsin residents

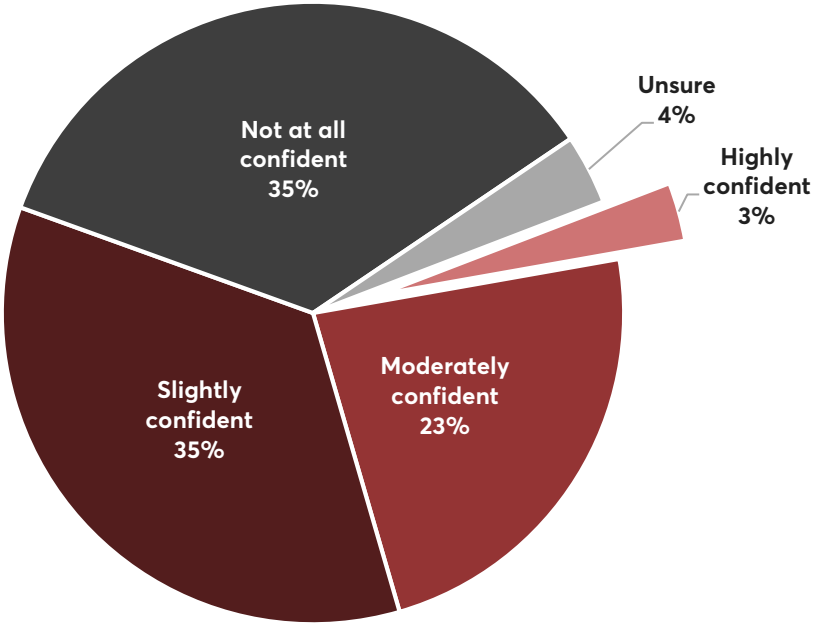
A larger percentage of Wisconsin residents **who have personally experienced a data breach (25%)** than those who **have not (15%)** say they are **"very worried"** about **companies tracking their day-to-day online activities.**

CONFIDENCE IN SECURITY OF PERSONAL DATA

More than a third **(35%)** of Wisconsinites say they are **'not at all confident'** that their **personal data**, such as their social security number, finances, or other personal information, **is kept secure** and not accessed without authorization.

A larger percentage of Wisconsin residents with household incomes less than $30,000 (12%) than those with household incomes 30,000+ (1%) say they are 'highly confident' that their personal data is kept secure.

HOW **CONFIDENT** ARE YOU THAT YOUR **PERSONAL DATA** IS **KEPT SECURE AND NOT ACCESSED WITHOUT AUTHORIZATION**?



Base: Wisconsin residents

A larger percentage of Wisconsin residents **who have personally experienced a data breach (43%)** than those who **have not (25%)** say they are **"not at all confident" that their personal data is kept secure and not accessed without authorization.**

COMPANIES SHARING PERSONAL DATA

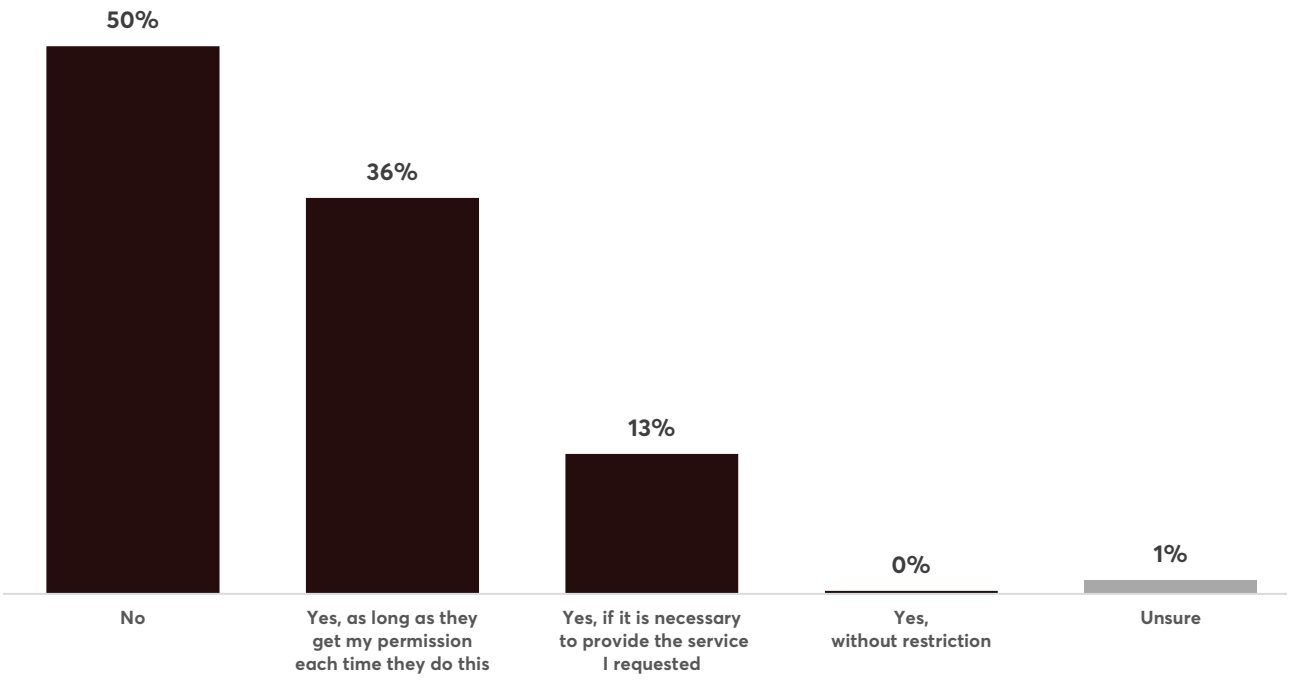
Wisconsin residents say that companies SHOULD NOT BE ALLOWED to share their data **at all or at least without some restriction.** Half of the Wisconsin residents we surveyed say companies should not be allowed to share their personal data and more than a third (36%) say companies can do this as long as they get permission each time.

0%

OF WISCONSIN RESIDENTS

Say companies **should be able to share their data without any restrictions.**

SHOULD COMPANIES BE ALLOWED TO **SHARE YOUR PERSONAL DATA?**



Base: Wisconsin residents

CONTROL OVER PERSONAL DATA

We asked Wisconsinites if they agree or disagree with the following statement:

"I feel I am in control of my personal data that companies collect about me"

Two in 10 Wisconsinites said they **neither agree nor disagree with the statement.**

7%

OF WISCONSIN RESIDENTS SAY THEY **STRONGLY AGREE (1%) OR AGREE (6%)** THEY FEEL IN CONTROL OF THEIR PERSONAL DATA THAT COMPANIES COLLECT ABOUT THEM

3%

WHO **HAVE EXPERIENCED A DATA BREACH** SAY THEY **STRONGLY AGREE/AGREE** THAT THEY FEEL IN CONTROL OF THEIR PERSONAL DATA

8%

WHO **HAVE NOT EXPERIENCED A DATA BREACH** SAY THEY **STRONGLY AGREE/AGREE** THAT THEY FEEL IN CONTROL OF THEIR PERSONAL DATA

70%

OF WISCONSIN RESIDENTS SAY THEY **STRONGLY DISAGREE (28%) OR DISAGREE (42%)** THAT THEY FEEL IN CONTROL OF THEIR PERSONAL DATA THAT COMPANIES COLLECT ABOUT THEM

82%

WHO **HAVE EXPERIENCED A DATA BREACH** SAY THEY **STRONGLY DISAGREE/DISAGREE** THAT THEY FEEL IN CONTROL OF THEIR PERSONAL DATA

64%

WHO **HAVE NOT EXPERIENCED A DATA BREACH** SAY THEY **STRONGLY DISAGREE/DISAGREE** THAT THEY FEEL IN CONTROL OF THEIR PERSONAL DATA

PERSONAL DATA SECURITY NOW, COMPARED TO 5 YEARS AGO

We asked Wisconsinites "**Would you say you believe your personal data is MORE or LESS SECURE (i.e., protected from unauthorized access) today than it was five years ago?"**

55%

OF WISCONSIN RESIDENTS

SAY THEY BELIEVE THEIR PERSONAL DATA IS **MUCH LESS SECURE (17%) OR LESS SECURE (38%)** THAN IT WAS FIVE YEARS AGO

18%

OF WISCONSIN RESIDENTS

SAY THEY BELIEVE THEIR PERSONAL DATA IS **MUCH MORE SECURE (1%) OR MORE SECURE (17%)** THAN IT WAS FIVE YEARS AGO

27%

OF WISCONSIN RESIDENTS

SAY THEY ARE **'NEUTRAL' (23%) OR 'UNSURE' (4%)** IF THEIR PERSONAL DATA IS MORE OR LESS SECURE THAN IT WAS FIVE YEARS AGO

Regardless of how much more or less secure Wisconsin residents believe their personal data is now compared to the past,

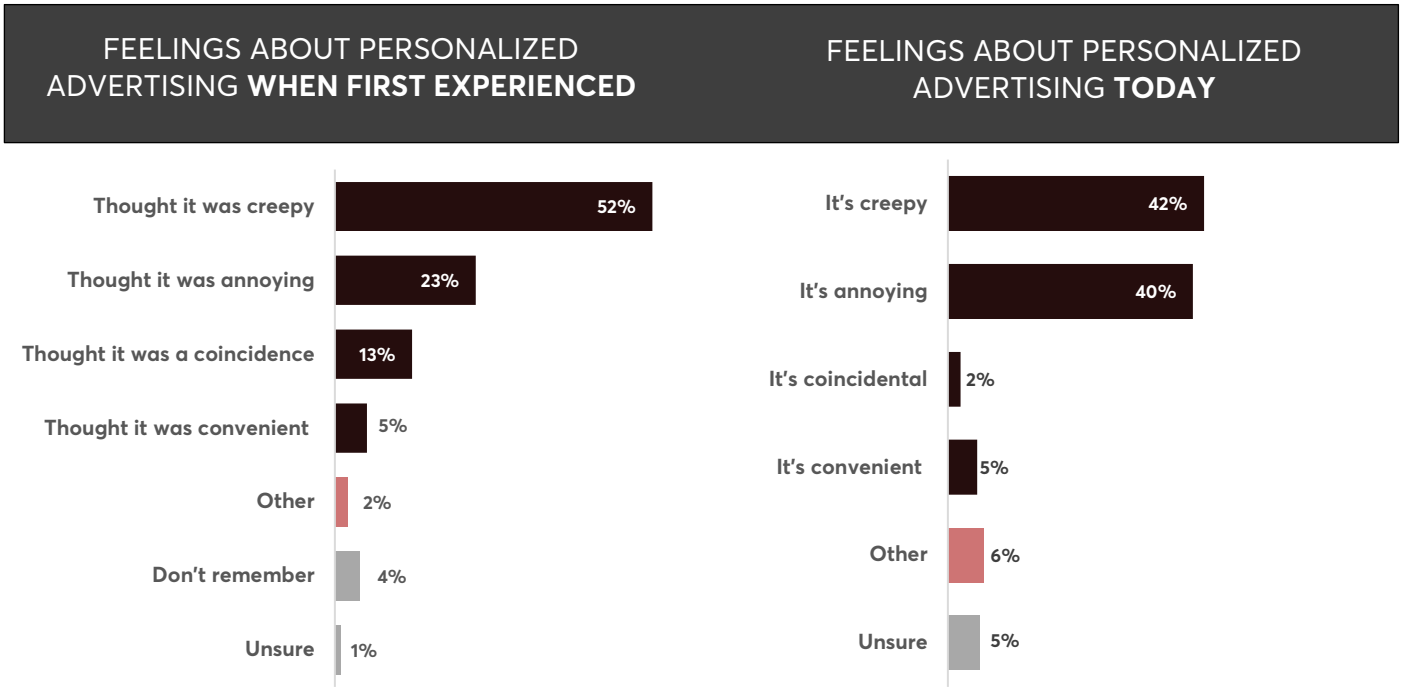
MOST (94%) Wisconsinites say **companies should be REQUIRED by law to keep their personal data secure (**i.e., protected from unauthorized access).

FEELINGS ABOUT PERSONALIZED ONLINE ADVERTISING – THEN AND NOW

More than eight in 10 (83%) Wisconsin residents say they have seen online advertising that is personalized based on their online searches or purchases. We asked Wisconsinites to tell us which statement BEST describes how they felt about this personalized advertising the FIRST TIME they experienced it and how they feel about it TODAY.

There has been a bit of a shift in perspective on the matter. While more than half (52%) of Wisconsinites felt it was creepy when they first experienced it, about four in 10 (42%) feel that way now. More Wisconsin residents find it annoying today (40%) than in the past (23%) but most likely because it is part of their daily life now compared to the first time, where they were more likely to say they just thought it was just a coincidence (13%).

One thing remains the same —only one in 20 say they think it is convenient.



Base: Wisconsin residents who say that they have seen online advertising that is personalized based on their online searches or purchases

82%

OF WISCONSIN RESIDENTS WHO HAVE **SEEN ONLINE ADVERTISING THAT IS PERSONALIZED BASED ON THEIR ONLINE SEARCHES OR PURCHASES**

Say they currently think it is **CREEPY OR ANNOYING**

SUMMARY

Overall, Wisconsinites are concerned about how much data companies collect and store about them, specifically when it comes to the security and privacy of their own personal data. They worry about companies tracking their habits when they are online but they acknowledge they do not have control over their personal data that companies collect. Wisconsin residents are not confident their data is secure— nor should they be when nearly half of those surveyed say they have experienced a data breach.

Wisconsinites do seem to have one voice when it comes to regulation…

- Nearly all Wisconsinites we surveyed say companies should be **REQUIRED by law** to keep their personal data secure.

- However, if a data breach does take place, nearly all Wisconsin residents say **companies** should be REQUIRED to notify them about the breach even if it does not create any financial risk such as identity theft or fraud.

METHODOLOGY

This online survey was fielded by Ipsos from January 8-13, 2020 to 649 Wisconsin residents. The target population consists of non-institutionalized adults age 18 and older residing in Wisconsin. To sample the population, Ipsos sampled households from its KnowledgePanel®, l, a probability-based web panel designed to be representative of the U.S. Ipsos invited one adult each from a representative sample of households to take this survey. Selected panel members received an email invitation to complete the survey and were asked to do so at their earliest convenience.

Once all survey data have been collected and processed, design weights are adjusted to account for any differential nonresponse that may have occurred. Depending on the specific target population for a given study, geodemographic distributions for the corresponding population are obtained from the CPS, the U.S. Census Bureau's American Community Survey (ACS), or in certain instances from the weighted KnowledgePanel® profile data. For this purpose an iterative proportional fitting (raking) procedure is used to produce the final weights. In the final step, calculated weights are examined to identify and, if necessary, trim outliers at the extreme upper and lower tails of the weight distribution. The resulting weights are then scaled to aggregate to the total sample size of all eligible respondents.

For this study, Ipsos weighed all respondents back to 18 and over adult Wisconsin population from ACS 2018.

Weighting variables include the followings:

- Gender (Male, Female) by Age (18-29, 30-44, 45-59, 60+)
- Race-ethnicity (White/Non-Hispanic, Black/Non-Hispanic, Other/Non-Hispanic, Hispanic, 2+ Races/Non-Hispanic)
- Education (Less than High School, High School, Some College, Bachelor or Higher)
- Household Income (under $25K, $25K-$49,999, $50K-$74,999, $75K-$99,999, $100K-$149,999, $150K+)

To avoid extreme values, the resulting weights were trimmed and then scaled to sum to the unweighted sample size of total respondents (weight).

In total, Ipsos interviewed 649 Wisconsin residents. The margin of error on the weighted data is +/- 4.8 percentage points at the 95% confidence level for the full sample. Findings presented in this report represent analyses of data after weighting was applied to respondent data to approximate Wisconsin population-based estimates.

Key demographic characteristics (after weighting is applied) of this sample are presented below:

- 51% female
- Average age of 50 years old
- 86% White, Non-Hispanic
- 30% 4-year college graduates
- 58% have a household income of $60,000 or more

APPENDIX: STRAIGHT TABS

2020 Wisconsin Privacy Survey

TABULATIONS

Q1 How concerned or not concerned are you about how much data companies collect and store about you?

		Total
		%
	Extremely concerned	18
	Very concerned	27
	Moderately concerned	36
	Slightly concerned	15
	Not at all concerned	4
	Base: Respondents who know that companies collect and store data about them	632

Q2 How concerned or not concerned are you about the security and privacy of your personal data that companies collect and store about you?

		Total
		%
	Extremely concerned	27
	Very concerned	29
	Moderately concerned	29
	Slightly concerned	11
	Not at all concerned	3
	Base: All respondents	640

Q3 Should companies be allowed to share your personal data?

		Total
		%
	No	50
	Yes, as long as they get my permission each time they do this	36
	Yes, if it is necessary to provide the service I requested	13
	Yes, without restriction	0
	Unsure	1
	Base: All respondents	647

Q4	Do you agree or disagree with the following statement: *"I feel I am in control of my personal data that companies collect about me"*	
		Total
		%
	Strongly agree	1
	Agree	6
	Neither agree nor disagree	20
	Disagree	42
	Strongly disagree	28
	Unsure	3
	Base: All respondents	647

Q5	How confident are you that your personal data, such as social security number, finances, or other personal information, is kept secure and not accessed without authorization?	
		Total
		%
	Highly confident	3
	Moderately confident	23
	Slightly confident	35
	Not at all confident	35
	Unsure	4
	Base: All respondents	647

Q6	Would you say you believe your personal data is more or less secure (i.e., protected from unauthorized access) today than it was five years ago?	
		Total
		%
	Much more secure	1
	More secure	17
	Neutral	23
	Less secure	38
	Much less secure	17
	Unsure	4
	Base: All respondents	646

Q7	Should companies be REQUIRED by law to keep your personal data secure (i.e., protected from unauthorized access)?	
		Total
		%
	Yes	94
	No	2
	Unsure	4
	Base: All respondents	646

Q8	Have you EVER personally experienced a data breach (i.e., when your personal information was stolen or exposed)?	
		Total
		%
	Yes	46
	No	37
	Unsure	17
	Base: All respondents	647

Q9	Should companies be REQUIRED to notify you if your data has been breached?	
		Total
		%
	Yes	97
	No	1
	Unsure	1
	Base: All respondents	643

Q10	Should companies be REQUIRED to notify you if your personal data has been breached, even if it does not create any financial risk such as identity theft or fraud?	
		Total
		%
	Yes	96
	No	1
	Unsure	3
	Base: All respondents	638

Q11	Have you seen online advertising that is personalized based on your online searches or purchases? (For example, an advertisement for auto insurance after searching for insurance.)	
		Total
		%
	Yes	83
	No	7
	Unsure	10
	Base: All respondents	647

Q12	Thinking back to the FIRST TIME you experienced this personalized advertising, which, if any, of the following statements BEST describes how you felt about it? (We will ask you about your current feelings about it shortly.)	
		Total
		%
	You thought it was creepy	52
	You thought it was annoying	23
	You thought it was a coincidence	13
	You thought it was convenient (e.g., you see ads for things you'd like to purchase)	5
	Other	2
	Don't remember	4
	Unsure	1
	Base: Respondents who say that they've seen online advertising that is personalized based on their online searches or purchases	542

Q13	Which, if any, of the following statements BEST describes how you feel about this personalized advertising TODAY?	
		Total
		%
	It's creepy	42
	It's annoying	40
	It's convenient (e.g., you see ads for things you'd like to purchase)	5
	It's coincidental	2
	Other	6
	Unsure	5
	Base: Respondents who say that they've seen online advertising that is personalized based on their online searches or purchases	543

Q14	When thinking about the ONLINE activities you do in your day-to-day life, would you say you are very worried, somewhat worried, or not at all worried about companies tracking your habits?	
		Total
		%
	Very worried	20
	Somewhat worried	61
	Not at all worried	14
	Unsure	5
	Base: All respondents	648

PUBLIC COMMENTS

In the interest of capturing the thoughts, opinions, and concerns of Wisconsin residents, the Advisory Committee sought public comment by holding a public comment period before three of the meetings and promoting a dedicated e-mail address (DATCPDataAdvisory@wisconsin.gov). The Advisory Committee received a few e-mails, and redacted versions are included in this Appendix.

The following people provided comment at the public hearings.

Green Bay, WI – Meeting #2 held in November 2019

Doug Raasch of Clintonville

Mr. Raasch had a data breach that led to identity theft recently. He has found it hard to get information from companies and stores. He does not have a computer which makes it harder—going to a public library to use a public computer provides more chance for identity theft. There should be stiffer laws, and it should be a felony to steal someone's identity.

David Dorn of Fond du Lac

He made a purchase off Facebook, and he was defrauded for about $170. He complained to the state, the federal government, and the credit card company. Zuckerberg does not vet his vendors unlike Amazon and others. There should be stringent measures to prevent fraud. The Internet is impossible to police, and the fake notices add to the defrauding.

Sheila Berndt of Denmark

She has a company called Net V Pro to help small businesses avoid hacking. She encourages offsite and onsite backup of your data, and they help identify people trying to hack you. The problem is international.

Curt Esser of Appleton

He is a computer consultant with Esser Consulting, and he has been in the business for 20 years. As such, he tries to educate the public about risk. Until you become a victim, you frequently are unaware. Lots of areas need to be addressed. Consumer education (social media, cell phones, and televisions/smart devices). Unfortunately, a lot of conveniences benefit the elderly, and it opens them up for problems. The advent of the Internet of Things, where security can be an afterthought. Smart cars, Bluetooths, and Onstars can be hacked or provide information that can be stolen and turned against consumers. He helps people with recovery from identity theft—lots of resources. Also, a person may not even know they have been hacked. People need antivirus and patching software. Password managers and ad blocker software help. A single typo can also send you to a Website that can compromise your machine. Tech support scams can particularly annoy, and we should have strong state laws in that regard. Ransomware has been on the increase for businesses, governments, and health care systems. A postponed surgery could lead to serious health problems. Data privacy and security can be a cat and mouse game where the software improves, and scammers find new ways around it. Wireless routers can be hacked. Because some data does not change (Social Security Numbers), one year of credit monitoring can be a joke. Credit recovery should be longer.

Robert Defnet of Green Bay

What people go through is scary. Why should people have to opt out or lose the convenience of modern devices? Why should opt in be the default option?

Madison, WI – Meeting #3 held in December 2019

No constituents testified.

Milwaukee, WI – Meeting #4 held in January 2020

Mary Lynn Center Strack of Milwaukee

She believed that identity theft was also an issue for businesses. She also stated Wisconsin should consider the provisions of the California Consumer Privacy Act that provide the possibility of opting out of shared data.

Sheila Berndt of Denmark

She talked about the 3-2-1 backup. She talked about difficulty she had with Amazon related to an unauthorized $400 gift card that could not be stopped due to authentication issues on their end.

Luke Rollins of Sun Prairie

He works for Lexis-Nexis. Having attended previous meetings, he saw the Advisory Committee pursuing three major areas: CCPA, Data Breaches, and Data Brokers. He thinks the state's breach law is pretty good, but it could be tweaked to include notification of the attorney general. All states now have a data breach law. The time component can be complicated; Lexis-Nexis has a war room for attacks, but they get attacked a few thousand times a day. They sometimes involve law enforcement in their efforts, so if the notification is too short, it can be unsafe to consumers in the long term. Due to market forces, it can be hard for government to have the resources or information technology staff for certain crises. Since Facebook and Google do not need to register, the Vermont data broker law may not be the best model. California's laws may be more comprehensive, but the law has now entered the rulemaking portion, and there are already 2,000 pages of comments. Lexis-Nexis fully complies with both CCPA and Europe's General Data Protection Regulation (GDPR). The California law started out as an initiative but then the legislature acted. Lexis-Nexis builds law enforcement databases, and early versions of the California law would have permitted criminals to opt out. In late 2020, people will have a better perspective of how the California law shapes the discussions. Washington State has a current bill (SB 6281), but they would prefer a Federal law. Rep. Shannon Zimmerman from River Falls plans to introduce bills tomorrow. Facebook decided that the CCPA does not apply to them. Three bills have been introduced in Illinois. He suggested the Advisory Committee consider the meaning of the word "sell" in any legislation.

[redacted]

From: [redacted]
Sent: Tuesday, November 12, 2019 9:09 AM
To: DATCP Data Advisory

Hi my name is [redacted]. I want to make you aware of an incident that happened to me in October 2019. I was in [redacted]. I was exchanging a defective product that I had bought there. The check out lady asked to see my driver's license. She reached out her hand to look at it. I gave it to her to LOOK at it. She immediately scanned my driver's license into the computer at the checkout. I said what are you doing scanning my license into your computer. She said that's what I'm supposed to do. I asked to see her supervisor. A man came and talked to me at the checkout. He said it's a new policy they put in a month ago. To scan people's driver license into the computer for exchanges. I told him she NEVER asked me for permission to do that. If I would have known she was going to do that I wouldn't have exchanged the product. Now they have my driver's license scanned into their system. I feel there should be a law to protect me from this happening again. This really upset me because of all the computer hacking that's going on out there. Now there's another computer that has my identity in it! And it was for just exchanging a product and not asking for my permission!!!! Thank you for having this committee to look at changing the laws for our protection!

[redacted]

[redacted]

[redacted]

Through my church I'm assisting someone with developing a budget and becoming more self-reliant. This process has made me aware of an identity theft and data breach threat that I had not considered before and wanted to make sure you are aware of and might be a concern for this committee.

The potential threat is that people who do not have their own internet service, may not have a secure connection to do financial and other online transactions. For example, if someone is using an eatery's wifi or a library's wifi connection, those are generally public, unsecure connections. I realized this because I want to look at my church member's online banking but if we meet at the library as we have, we will not have a secure connection there. So we will have to do that elsewhere.

While this is a concern for individuals, it's also a concern for businesses who may be at greater risk to a hacker who is already beyond the initial firewalls with a stolen login and password.

I came to this realization this morning and then I saw this email so I thought I'd share.

[redacted]

[redacted]

[redacted]

Sent: Saturday, December 21, 2019 8:36 PM
To: DATCP Data Advisory
Subject: Comment about the sharing of personal data.

One comment – I think is down right improper to allow businesses to sell our personal information to those that are interested in buying that information to help them make contacts. (Example – [redacted] selling my phone number/ email to companies that then turn around and try to seek money for their cause. Please realize that maybe some companies have great intentions and then you have those that will try to use techniques to scam!!!!

[redacted]
Oshkosh, WI

From: Sheila Berndt [redacted]
Sent: Wednesday, May 27, 2020 5:31 PM
To: Woldseth, David A - DATCP
Subject: [redacted]
Attachments: Color Coding Emails 03.26.2020.pdf; Security Tips 04.20.2020.pdf; Resilience Capabilities 05.26.2020.docx

"Never doubt that a small group of thoughtful, committed, citizens can change the world. Indeed, it is the only thing that ever has."

I should've googled this first. I almost had it right.

Sheila Berndt
[redacted]
Help People. Solve Problems. Add Value

From: Sheila Berndt
Sent: Wednesday, May 27, 2020 5:25 PM
To: Woldseth, David A - DATCP [redacted]
Subject: RE: DATCP Webinar Questions?

Hello,
I have been very impressed with the level of honest, thoughtful public discourse I've heard in viewing your meetings. I believe Margaret Mead said, "Never doubt a small group of thoughtful committed citizens can change the world. It's usually how it happens."

My biggest concern is a statement I saw which said something about we need to have enough money to keep up with the hackers. We don't need to keep up with the hackers, we need to thwart them. We need to deny them the benefits they are currently receiving with their mischief of ransomware and cryptolocking and other such nonsense. This is from the Cyberspace Solarium Commission who say 80% of the mischief can be taken off the table by doing 20% of things that can easily be done.

Users can do this by color coding their emails, using MFA everywhere including Health accounts and ALL online buying and email, hovering over links to See the path where it is taking them, using strong security passphrases and locking their credit reports.

Operating Systems personnel can do this by practicing POLP, MFA on all credentials, 3 2 1 back up rules, testing their backup, inventorying their assets, having a DR plan or even an outline and testing that outline by running mini drills, threat mitigation through patching protocols, closing RDP's and a good security stack which provides Endpoint Security along with the rest of the NIST framework. We promote Protection without Detection, which doesn't need to Identify threats, and by being resilient. We also love the idea of enacting Law to force companies to make data ephemeral after 7 years. If there's nothing to steal, then there's nothing to steal.

It has been interesting viewing the discussions regarding defining PII. From the first meeting I went to at NWTC last October, Jason, one of the committee members, said we should have other identifiers than what's on our DL or SS#, which I thought was brilliant! Do That!

Regarding the Ohio Safe Harbor bills they define that with the Prudent Man clause, as this being loosely defined as to what a

[redacted]

“Prudent Man” would have done to keep their data secure. To my knowledge, the definition of what “Prudent Men” do is still unclear.

Please let me know if there are any questions or clarifications needed on any of this information, and Thank You All for what you are doing here, I believe Wisconsin will definitely get it’s number to a 5 once you have completed your task!

Sheila

Sheila Berndt
[redacted]
Help People. Solve Problems. Add Value

Adding Red Flags to your **Inbox** by color coding and/or CHANGING FONTS in Settings will alert you to potential email scams.

Internal emails do not have the @ sign and this rule will expose an imposter domain name with a **MASQUERADE** such as a **0** instead of an **O**, which could easily be overlooked.

- In Outlook O365
- Go to the View tab.
- Select View Settings.
- Choose Conditional Formatting.
- Click Add.
- Name your rule in Properties of rule – i.e. "external email"
- Click on Font and pick a color or font you like then hit OK.
- Click on Condition.
- In the **From**... Box enter @ and hit OK all the way back through.
- After leaving settings then every email from an external domain will be the color/font you chose earlier

  - This can also be done separating out specific domain names like @netvpro.com with a different color or **font** to make those emails stand out. If they're not the color you selected, it's an automatic **Red Flag**!

Google Mail has the use of color coding labels to make emails more distinct.

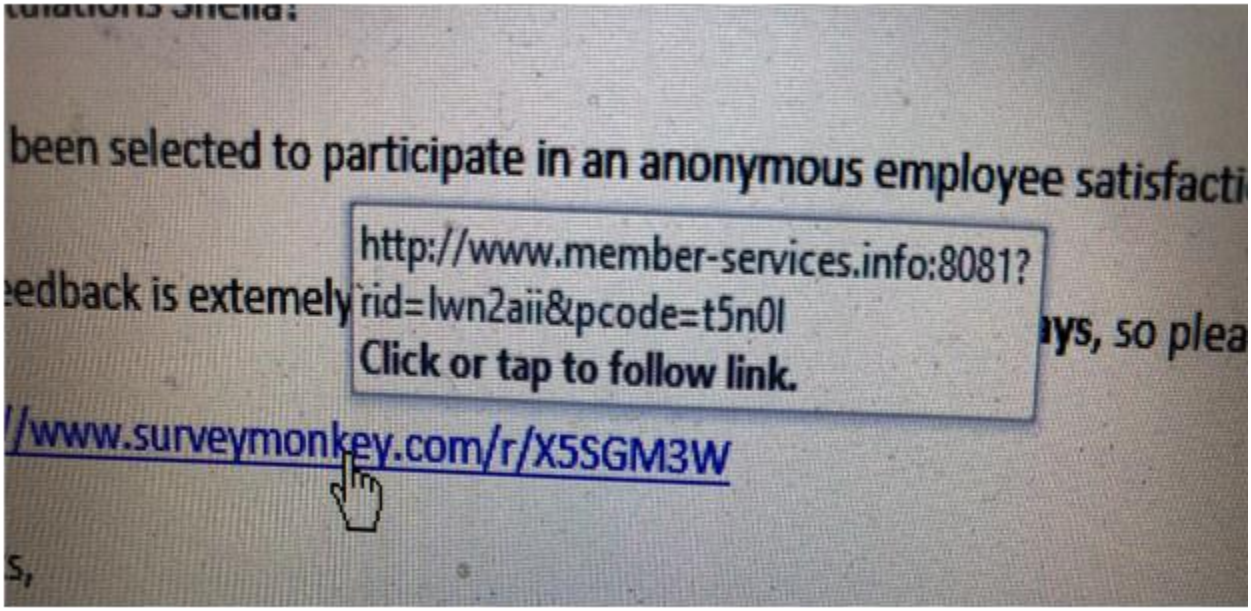
#colorcodeemails #cybersecurity #security #emailscams #emailsecurity #office365

Sheila Berndt
[redacted]
Help People. Solve Problems. Add Value.

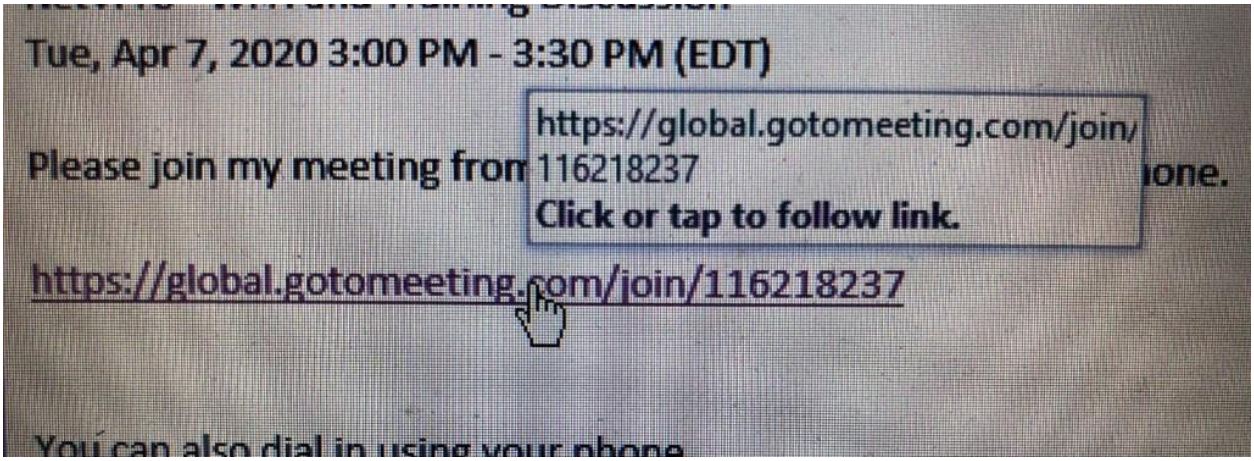
Sheila Berndt
Account Executive
[redacted]

User Controls: For Forward Defending

Example of Scam Link: See how when hovering over the link it shows a different path than the one listed?



Example of Legitimate Link: See how when hovering over the link it shows EXACTLY the same path as the one listed?



Sheila Berndt
Account Executive
[redacted]

https:// Stands for **Hypertext Transfer Protocol Secure** so if a website DOESN'T begin with **https,** only saying http, without the **S** – It means the website is not secure and could potentially be a Scam. You may also recognize an unsecured website by the lack of the Locked Padlock picture with the word Secured in front of the website address.

Turn on Multi Factor (2 Factor) Authentication on Email, Financial Institutions, online buying, Health Accounts, and anything else which can identify You as You and authenticate someone isn't masquerading as You.

Use Strong Passwords with a symbol and a number such as **%6** with a pass phrase
using upper & lower case letters, symbols and numbers and end the password with the opposite **6%** for safety.
Such as **%6M@Du$p6%** - Standing for **%6Making a difference using strong passwords6%**

Color Code Your emails BY CHANGING FONT AND COLOR to 1) Recognize External vs. Internal Emails. Internal Emails do not have the @ sign, so if someone is masquerading as an internal emails, this will alert you immediately and 2) It will alert you to an email where you may not notice the address is slightly altered, for instance an O (Capital O) instead of a 0 (Zero), and Block Domain names known to be malicious.

Operating System Controls: For Forward Defending

3 2 1 Backup Plan – 3 Types of Backup, 2 potentially on Premise in different Media and 1 offsite back up method, whether Virtualized or otherwise.

Practice Principles of Least Privilege (POLP)

Practice Meaningful Segmentation

Delete all delinquent passwords and email addresses

Close all Remote Desktop Protocols

Do an Inventory on Your Existing Assets

Patch Management

TO: Members of the Data Privacy & Security Advisory Committee
Wisconsin Department of Trade, Agriculture & Consumer Protection

Lara Sutherlin	Michelle Reinen	David Woldseth
Administrator	Policy Initiatives Advisor	Policy Analyst

Division of Trade & Consumer Protection
Wisconsin Department of Agriculture, Trade & Consumer Protection

FROM: Luke Rollins
Director of State Government Affairs
RELX (Reed, Elsevier & LexisNexis)

DATE: May 19, 2020

RE: RELX Feedback on Possible Draft Policy Recommendations

Data Privacy & Security Advisory Committee:

Thank you for the opportunities since the Fall to observe the Advisory Committee's proceedings.

RELX is a stakeholder and interested party in policy regarding data, data security, privacy and technology. We have worked on policy in these areas around the country.

Below, we would like to share some notes that you all may want to consider during the deliberations of the possible recommendations.

By way of background, RELX is the parent organization of Reed, Elsevier, LexisNexis and Reed Exhibitions. LexisNexis is a recognized leader in providing authoritative legal, public records and business information. LexisNexis plays a vital role in supporting government, law enforcement and business customers who use our information services for important uses including: detecting and preventing identity theft and fraud, supporting law enforcement and locating suspects, supporting the insurance markets, finding missing children and preventing and investigating criminal and terrorist activities. Data is our lifeblood and being good stewards of data is something RELX and LexisNexis task seriously.

LexisNexis produces a variety of solutions from data and being sincere and strong stewards of data is paramount and we take privacy seriously.

In Wisconsin we work to prevent fraud via identity verification and authentication with the Wisconsin Department of Health Service's Medicaid program and the Wisconsin Department of Workforce Development. As well, we provide front line law enforcement and regulatory investigators with the research tools they need to gather intelligence and solve cases.

Data Broker:

- I do not recommend Vermont as a model because due lobbying by big social media companies resulted a very narrowly crafted bills impact just a small set of businesses that use data while not pertaining to the biggest data collectors (big technology, big social media, big retailers that you would expect).
- The Council of State Governments (CSG) Suggested State Legislature (SSL) process rejected Vermont data broker as a model in December 2019 at their national meeting.
- If the Task Force desires to include a data broker recommendation in their report I would encourage the Task Force look at the California data broker statute which is not as narrow as Vermont.
- As well, the Task Force may want to explore that a company that qualifies for the data broker registry should be exempt from an omnibus privacy proposal.
- There are only two data broker registries in the USA as those policy proposals have become old news because omnibus privacy proposals are more encompassing of all types of data collectors and users.
- We recommend an omnibus privacy proposal approach over a data broker approach.
- If you are to look at the Vermont data broker list, only a few company names are recognizable and it leaves many to wonder where are all the big retailers, big technology and big social media companies.

Exemptions:

- We strongly encourage any omnibus privacy recommendations recognize the sets of data and data practices that are already regulated under Federal rule: Fair Credit Reporting Act (FCRA), Gramm Leach Bliley Act (GLBA), Health Insurance Portability & Accountability Act (HIPAA) and Drivers Privacy Protection Act (DPPA).
- We strongly encourage any omnibus privacy proposal protects access and use of public records and that public records remain public.
- We strongly recommend exemptions for law enforcement, law enforcement support organizations and anti-fraud/identity verification and authentication initiatives. The scenario of bad actors opting in or opting out law enforcement or anti-fraud databases would be troublesome.

Omnibus privacy policy:

- We strongly encourage the committee look at 2020 Washington State Senate passed as a thoughtful model to develop omnibus privacy recommendations.
- We also encourage the committee look at a narrow policy bill in Nevada (2019 NV S 220) that specifically addresses the universe of “online data” and a “right to know”.
- CCPA passed in 2018 and no other omnibus privacy bill has passed in the United States. California had to pass several bills to address concerns and issues with their quickly passed CCPA. Although CCPA was effective January 1, 2020, there still are no administrative rules implementing that law. The CA AG has received over 2,000 pages of comments. There are still clarifications needed for CCPA. Business compliance with CCPA is reported to be over $55 billion. Amendment bills to CCPA are still being filed and heard. As well, the proponent behind CCPA is already moving forward with a CCPA 2.0 via a ballot initiative.
- We appreciate the thought, time and effort put behind the Representative Zimmerman Bills (2020 WI AB 870, 871 & 872).
- We appreciated having the February hearing and the teeing up discussions to prepare for legislate in 2021 because we can then see how CCAP implementation is going, with enforcement and recognize what does work, does not work and recognize the pain points.

- We appreciate exemption considerations being given for data that already has Federal regulatory regimes: FCRA, DPPA, HIPAA & GLBA. We understand there will need to be some work on the FCRA definition to bring it in line with other proposals. Public records and law enforcement also have exemptions in Zimmerman.
- Our concerns with Zimmerman include: ensuring a strong exception for purposes of fraud prevention and supporting law enforcement use; the need for clarity that this bill does not allow for a private right of action; the 4% of annual revenue is extraordinary; confusion if a definition or exemption in one of the bills carries through to all three bills and the possible need for one bill; opt-in versus opt-out and questions regarding operational consistency with other state laws including around providing notices to consumers.
- Zimmerman pulls heavily from GDPR. For a global company, GDPR only applies to its European lines of business and not its US lines of business so it would still be a significant effort to bring US lines of business into compliance. To date, US lines of business that utilize CA data need to have a compliance program with CCPA. This will be a completely new regulatory regime for Wisconsin businesses unless they have European or California lines of business.
- Zimmerman plans on holding stakeholder meetings later this year.

Security Breach:

- We strongly encourage that any notification of security breach to be based upon "determination" or "confirmation" of a breach. We do not want to announce to early while a system may be vulnerable, the breach needs to be investigated, stopped, patched, identify and determine the scope of the breach, possible law enforcement engagement and then preparations for notifications.
- Attorney General and Consumer Protection notifications after determination of a breach would be just fine.
- Omnibus privacy bills do not necessarily need to contain a breach provision. Security breach laws have been around for a long time, they are mature policy that is tweaked over the years. All 50 states of a security breach law. Omnibus privacy laws are brand new with only one state California having passed an omnibus privacy bill.
- Senator Larson's bill copied CCPA prior to several of the 2019-2020 amendments that were passed in California prior to the January 1, 2020 effective date. California has a robust security breach statute thus the CCPA did not have to include security breach policy.
- We advocate for security breach and omnibus privacy bills to be standalone bills given one is completely new policy and one is mature policy. Tweaks to an existing breach statute may receive considerable less opposition and may be easier to pass than a CCPA or GDPR style bill.
- Representative Zimmerman's Assembly Bill 870 does have security breach provisions in Section 1 (4):

> **(4)** Personal data breach notification. (a) 1. Except as provided in subd. 2., if a controller is aware of a personal data breach of personal data maintained by the controller, the controller shall notify the department of justice of the personal data breach without undue delay. If feasible, the controller shall notify the department within 30 days of becoming aware of the personal data breach. If the controller does not notify the department within 30 days of becoming aware of the personal data breach, the controller shall provide a reason for not notifying within 30 days. The notification shall do all of the following:
>
> a. Describe the nature of the personal data breach including, if known, the categories and approximate number of consumers involved and the categories and approximate number of personal data records involved.
>
> b. Describe the likely consequences of the personal data breach.
>
> c. Describe the measures taken or proposed by the controller to address the personal data breach, including, if appropriate, measures to mitigate the possible adverse effects.

2. A controller is not required to make a notification under this paragraph if the personal data breach is unlikely to result in a risk to the rights and freedoms of consumers.

3. If it is not possible to provide the information required under subd. 1. at the same time, the controller may provide the information in stages without undue delay.

4. If a processor is aware of a personal data breach of personal data that the processor maintains on behalf of a controller, the processor shall notify the controller without undue delay.

(b) 1. Except as provided in subd. 2., if a controller is aware of a personal data breach of personal data maintained by the controller and the personal data breach is likely to result in a high risk to the rights and freedoms of consumers, the controller shall notify the consumers whose personal data is involved in the personal data breach. The notification shall describe in clear and plain language the nature of the personal data breach and contain the information described in par. (a) 1. b. and c.

2. A controller is not required to make a notification under this paragraph if any of the following applies:

a. The controller has implemented appropriate technical and organizational protection measures to the personal data involved in the personal data breach that render the personal data unintelligible to any person who is not authorized to access it.

b. The controller takes measures after the personal data breach that ensure that a high risk to the rights and freedoms of consumers is not likely to exist.

c. Making the notification involves unreasonable effort. If this subd. 2. c. applies, the controller shall publicly communicate about the personal data breach to consumers in an effective manner.

Attorney General versus Private Right of Action:

- We would recommend empowering the Attorney General with an enforcement role.
- We would strongly oppose, as would many industry associations, any private right of action.
- A private right of action instantly creates a non-business friendly and adversarial business environment.
- That last two years in Washington State, the Senate passed a strong omnibus privacy bill with attorney general enforcement. But two years in a row the bill died in great part due to the House wanting to add in a private right of action.

Citizen Cyber Security Force:

- I recommend the Task Force also considers the 2018 Ohio House Bill 747 “Ohio Cyber Reserve”.
- I recommend not mixing a citizen cyber security force with other policy recommendation as it really is its own unique concept to help states respond to cyber-attacks.

Safe Harbor:

- The Ohio safe harbor bill is fine to base recommendations upon but we strongly encourage more clarity in language, drafting and definitions.

Please feel free to reach out to me with any questions or requests for additional information.

Take care,
Luke Rollins
Director of State Government Affairs
RELX

[redacted]

TO: Members of the Data Privacy & Security Advisory Committee
Wisconsin Department of Trade, Agriculture & Consumer Protection

Lara Sutherlin	Michelle Reinen	David Woldseth
Administrator	Policy Initiatives Advisor	Policy Analyst

Division of Trade & Consumer Protection
Wisconsin Department of Agriculture, Trade & Consumer Protection

FROM: Luke Rollins
Director of State Government Affairs
RELX (Reed, Elsevier & LexisNexis)

DATE: June 12, 2020

RE: RELX Feedback on Possible Draft Policy Recommendations

Data Privacy & Security Advisory Committee:

Thank you for the opportunities since the Fall to observe the Advisory Committee's proceedings. As well, thank you for allowing me the opportunity to submit my memo raising questions and concerns and relaying information on data brokers, breach, omnibus privacy, etc.

After observing several workgroup sessions and the last general committee meeting I had some additional thoughts that may be of interest to the committee.

Opt-in vs. Opt-out:

- To date no state in the national has created an opt-in version of omnibus privacy laws.
- CCPA, 2020 Washington State Senate passed and Nevada (online data) are all opt-out.
- With certain products/solutions/platforms there, like automobile driving telematics for insurance purposes are opt-in relationship between a customer and a business.
- Opt-in may work for some specific circumstances but in mass it would not. Given LexisNexis' databases for law enforcement, missing children, identity verification/authentication, anti-fraud or insurance…..the bad actors would not opt-in. Many the markets LexisNexis serves would be harmed by an opt-in model.

Fines/Forfeitures for breaches:

- Fines and forfeitures need to be limited in scope to proven negligence and harm.
- Do you get fined if your house gets broken into and a theft occurs?
- You are proposing fines and forfeitures for victims of theft.
- Businesses do not want to get broken into and have data stolen.

- The fines structure in the Zimmerman bills would be devastating to many companies large and small.

Breach Compensation Fund:

- We are struggling how this operationalization would look and work.
- Many national and multinational companies have breach insurance. How could the State of Wisconsin grab a slice of the breach premium pie for all the breach insurance policies already in existence, around the county and globe, to finance a Wisconsin fund?

Right to Cure:

- The committee should consider a right to cure.
- There could be a circumstance where a business may unknowingly make a mistake. With each state pursuing different privacy laws, the regulatory field is confusing and cumbersome.

Federal legislation:

- The committee should consider a recommendation that encourages the Wisconsin delegation to advance a comprehensive national data privacy pan for the USA.
- The patchwork of state privacy laws is confusing and cumbersome for businesses of all sizes.

Do Not Call & Do Not Collect:

- The committee should reject any notion of a "do not call" type solution for "do not collect".
- First, the state could then hold so much data they may not want any part of having.
- Second, such a system would have a considerable cost to build, staff and manage.

"The Hub":

- We would advise Wisconsin continue the approach of crafting a narrow scope to the hub concept.
- The Indiana hub is fairly complex in its function as it is a central point to manage data flow, data output, data analysis and data connectedness amongst state agencies. From the discussions we do not think that is the workgroup's intent.

Recapping Exemptions:

- We strongly encourage any omnibus privacy recommendations recognize the sets of data and data practices that are already regulated under Federal rule: Fair Credit Reporting Act (FCRA), Gramm Leach Bliley Act (GLBA), Health Insurance Portability & Accountability Act (HIPAA) and Drivers Privacy Protection Act (DPPA).
- We strongly encourage any omnibus privacy proposal protects access and use of public records and that public records remain public.
- We strongly recommend exemptions for law enforcement, law enforcement support organizations and anti-fraud/identity verification and authentication initiatives. The scenario of bad actors opting in or opting out law enforcement or anti-fraud databases would be troublesome.

Recapping Vermont Data Broker:

- The last New Ideas Workgroup began a discussion to have a broader scope to the data broker recommendation. We encourage that broader scope as data collected and use is not limited to a very narrow set of companies.
- The Vermont Data Broker statute is drafted so narrow that it impacts a very small set of companies with only a few recognizable.

- The nation's largest brokers of data that one would expect to see on this list do not qualify for registration under the Vermont statute.
- Vermont data broker was passed prior to CCPA and is now obsolete to CCPA or to Nevada or to the Washington State Senate passed version of omnibus privacy.

Recapping Omnibus privacy:

- We strongly encourage building out an omnibus privacy proposal from 2020 Washington State Senate passed or Nevada.

Please feel free to reach out to me with any questions or requests for additional information.

Take care,

Luke Rollins
Director of State Government Affairs
RELX

[redacted]

TO: Members of the Data Privacy & Security Advisory Committee
Wisconsin Department of Trade, Agriculture & Consumer Protection

Lara Sutherlin	Michelle Reinen	David Woldseth
Administrator	Policy Initiatives Advisor	Policy Analyst

Division of Trade & Consumer Protection
Wisconsin Department of Agriculture, Trade & Consumer Protection

FROM: Luke Rollins
Director of State Government Affairs
RELX (Reed, Elsevier & LexisNexis)

DATE: July 1, 2020

RE: RELX Feedback on Possible Draft Policy Recommendations

Data Privacy & Security Advisory Committee:

Thank you for the time and consideration of my comments over the last several months. I would like to submit the following thoughts regarding the "Privacy Pal" concept.

Privacy Pal:

- The concept of a "Privacy Pal" seemed to be based upon an existing online retailer's privacy settings panel that a customer could access and adjust.
- The application of an online retailer's privacy settings panel across other sectors and industries needs to be carefully vetted and considered.
- The Privacy Pal concept appeared to evolve from the discussion about the creation of a privacy "do not call" (marketing) type initiative. This would be a first in the nation.
- The Privacy Pal concept seems most applicable to an online consumer-to-business relationship/transaction relationship, where data is collected on a consumer at a point-of-sale.
- A broad application of Privacy Pal could be harmful for a variety of industries supporting law enforcement, insurance, credit, and anti-fraud solutions.
- A Privacy Pal concept would need to consider exemptions to sets of data that already have federal regulatory regimes including: Fair Credit Reporting Act (FCRA), Gramm Leach Bliley Act (GLBA), Health Insurance Portability & Accountability Act (HIPAA) and Drivers Privacy Protection Act (DPPA).
- We strongly encourage any Privacy Pal recommendation also exempts public records so that public records indeed remain public.
- The creation, maintenance and security needs of a Privacy Pal initiative would have a significant FTE and financial implication upon the state.

- Presumedly, a Privacy Pal program would need to house a fair amount of individual level consumer data thus the security concerns and protection of that data has to be considered.
- A Privacy Pal program would have to have a way to deliver details concerning a consumer's privacy settings to businesses around the USA and even globally.
- Privacy Pal would also need to verify the identities of the consumers making the privacy setting requests to ensure people are who they say they are and other people, including bad actors, could not adjust another person's privacy settings.

Please reach out with any questions.

Take care,

Luke Rollins
Director of State Government Affairs
RELX

[redacted]

American Council of Life Insurers
American Property Casualty Insurance Association
Independent Insurance Agents of Wisconsin
National Association of Insurance and Financial Advisors - Wisconsin
National Association of Mutual Insurance Companies
Professional Insurance Agents of Wisconsin
Wisconsin Bankers Association
Wisconsin Council of Life Insurers
Wisconsin Credit Union League
Wisconsin Insurance Alliance

June 12, 2020

Data Privacy and Security Advisory Committee
Wisconsin Department of Agriculture, Trade, & Consumer Protection
2811 Agriculture Drive
P.O. Box 8911
Madison, WI 53708-8911

Dear Committee Members:

We greatly appreciate the opportunity to comment on the work of the Data Privacy and Security Advisory Committee ("DPSAC") established by the Department of Agriculture, Trade and Consumer Protection. As trade associations representing the insurance and financial services industries, our members have decades of experience operating in highly regulated environments and maintaining consumer data in a secure and confidential manner.

It is our desire and intent to continue working with state policymakers to improve data privacy and security laws. There is no doubt that the evolution of technology has given rise to legitimate privacy concerns for individuals, and state policymakers should address this issue by clearly defining expectations for consumer privacy and requiring adequate security measures to protect private and personal information.

That being said, data privacy and security laws are complex, and any regulatory scheme must weigh the preferences of consumers against the needs of businesses that process personal data. New regulations in this ever-evolving area must be developed and implemented in a manner that does not stifle innovation or frustrate consumers. Additional regulation of data privacy and security must not unnecessarily add to the already large regulatory burden imposed on Wisconsin businesses. Any significant additional regulations risk making the state less attractive for investment and growth.

Our concern is that at this point the committee may be heading toward recommendations that—while certainly well intended—may negatively impact businesses and consumers. We ask that you consider delaying recommendations for highly regulated industries or deferring to industry-specific regulators where appropriate. If action is necessary, ensure it is targeted and consistent with the existing framework.

We submit this letter to identify three important principles for future data privacy and security measures recommended by the DPSAC and other state policymakers, all with the goal of reducing harms to both businesses and consumers:

(1) **Ensure harmonization** between existing regulatory structures and requirements;

(2) **Retain and expand risk-based regulations**, which balance consumer expectations with the ability of businesses to effectively operate and innovate; and

(3) **Proceed incrementally** so that Wisconsin businesses and consumers have time to adapt and do not suddenly find themselves at a significant disadvantage.

If the DPSAC and other state policymakers respect those three important principles, they can ensure Wisconsin develops a coherent and workable data privacy and security scheme that is both business- and consumer-friendly. To provide context, we begin by describing the current state of the law, as applicable to our members, then offer our suggestions on how to best achieve these principles going forward.

I. Background: The insurance and financial services sectors are already subject to significant data privacy and security regulations.

The financial services sector already complies with many different laws regarding data breach notification, privacy, and security. Specifically, insurers and other financial institutions have been subject to comprehensive federal and state laws and regulations for many years, with additional laws currently under consideration. Prudential regulatory agencies with jurisdiction over these sectors regularly examine insurers and financial services providers to determine their compliance with these laws and regulations and test how they manage information security risk. The already-existing regulatory structure has two important effects, both of which emphasize the need for the DSPAC and other state policymakers to ensure that any new laws or regulations complement what is already in place.

First, the existing structure ensures that businesses—including our members—are already subject to a high baseline for data privacy and protection. That baseline strikes an important and delicate balance between privacy concerns and the proper use of personal information for the benefit of consumers. It is also tailored to specific industries, based on an understanding of the types of data collected and maintained by businesses, as well as the legitimate and illegitimate uses for that data.

Second, given the existing structure, any *additional* laws and regulations may cause significant confusion if not implemented carefully. As it exists now, the structure is complex. Adding more complexity amplifies the possibility that laws will conflict, either substantively (if, for instance, two laws impose different obligations) or across jurisdictions (if, for instance, Wisconsin adopts a law that is different from federal or another state's law, or subjects companies to regulation by multiple agencies within the same state).

We hope that this perspective will provide additional context for the committee regarding how certain information and industries are already regulated, so that it can understand that additional regulation may not be necessary or should respect the existing boundaries. However, in the event that the committee ultimately decides to recommend new data security and privacy measures, this information should also be valuable to ensure that new measures do not conflict with what is already in place and, instead, are consistent with other successful and similar measures across new types of information and industries.

There are three already-existing federal laws, which—when combined with related state-level regulations—impose significant data privacy and security obligations on financial services companies:

- **Fair Credit Reporting Act ("FCRA") –** FCRA imposes strict limitations on the use and sharing of intimate details of consumers' creditworthiness, reputation, and customer relationships with other companies. In general, no one is permitted to access, and reporting agencies are not permitted to disclose, such information without specific "permissible purposes." Over decades since FCRA's enactment, the Federal Trade Commission has issued guidance to enforce these limitations, such as by generally prohibiting the disclosure and use of consumer reports for marketing purposes. The Consumer Financial Protection Bureau (CFPB) now shares FCRA jurisdiction with the FTC, and it is responsible for FCRA implementing regulations, Reg. V. Fifteen (15) years ago, FCRA was amended by the Fair and Accurate Credit Transactions Act (the "FACT Act") to ensure that regulated entities implement "red flags" programs to protect against, detect, and mitigate the effects of identity theft. In addition, FCRA affords rights to consumers who have been adversely affected by information in their consumer reports. Insurers, depository institutions, non-bank lenders, and other financial services companies often use credit reports in making underwriting decisions. Accordingly, these companies are keenly aware of the limits on how consumer information may be used and are required to provide adverse action notices to individuals when a denial, cancellation, increase in charge, or adverse or unfavorable change in terms in the underwriting results from a consumer report.

- **Health Insurance Portability and Accountability Act of 1996 ("HIPAA")/ Health Information Technology for Economic and Clinical Health ("HITECH") Act –** HIPAA and HITECH protect health information maintained by covered entities, including certain insurers, along with their business associates. Among other things, it: (1) limits disclosure except in prescribed situations or with an individual's consent; (2) includes rights for individuals to request access to, amendment of, accounting of, disclosure of, and restriction on the use or disclosure of protected health information; and requires data breach notification for unauthorized disclosure of protected health information ("PHI"). Insurers are also subject to similar requirements under Wis. Admin. Code INS Chapter 25.

- **Gramm-Leach-Bliley Act ("GLBA") –** GLBA imposes privacy and security standards on financial institutions. The act broadly includes any institution which is engaged in activities that are financial in nature or incidental to such financial activities and specifically directs state insurance commissioners to adopt data privacy and data security regulations. This federal action led to the development of NAIC Model #672, which was addressed by Wisconsin in Wis. Admin. Code INS Chapter 25. The CFPB's Regulation P, which implements GLBA at the federal level, and the Office of the Insurance Commissioner's regulations in Chapter 25 require financial institutions and insurers to: (1) provide notice to consumers about privacy policies and practices; (2) describe the conditions under which nonpublic personal health information and nonpublic personal financial information about individuals may be disclosed to affiliates and nonaffiliated third parties; and (3) give individuals the opportunity to prevent a financial institution from disclosing that information to nonaffiliated third parties, specifically mandating an "opt out" option for financial information (thus allowing an individual to elect not to have their financial information shared). In addition, Chapter 25 provides consumers an "opt in" option for disclosure of health information (thus prohibiting disclosure of the individual's health information without express consent). Over the years, federal banking regulators have issued extensive guidance in response to GLBA, including requiring financial institutions to implement robust information security procedures.

- **Right of Financial Privacy Act ("RFPA") -** The RFPA establishes specific procedures that federal government authorities must follow in order to obtain information from a financial institution about a customer's financial records. Customers affected by the RFPA include individuals and partnerships of five or fewer individuals. Unless the customer has specifically consented to the release of information, such information generally can only be provided to federal law enforcement pursuant to an administrative subpoena or summons, a judicial subpoena, a search warrant, or a formal written request. A customer's consent cannot be required by the financial institution as a condition to receiving products or services. Financial institutions generally may not release financial information relating to a customer unless the government agency requesting information has provided a written certification of compliance with the RFPA. Financial institutions also must keep records of all instances in which the customer's information is disclosed to a federal government authority, including the identity of the governmental authority and a copy of the request.

II. Principle 1: Ensure harmony in the law, by focusing new recommendations on gap-filling, while also avoiding duplicative or contradictory requirements.

As the committee considers recommendations to data privacy and security laws in Wisconsin, it should harmonize those efforts with the existing framework to the maximum extent possible. The current framework provides a valuable starting point, offering the committee two benefits.

First, harmonizing any recommendations with the existing framework spares the committee from having to "reinvent the wheel." Consumers and companies already understand the existing framework. Indeed, they have years of experience and clear expectations for the treatment of sensitive data. In practice, the existing structure creates "concentric circles" of regulation—providing greater protection and control over the most sensitive information, with those protections and controls scaling down as the level of sensitivity is reduced or where the consumer has consented to use.

This model has become the accepted—and expected—approach for protecting data. Thus, future efforts to expand data privacy regulations for the financial services sector should build upon this existing structure, so that both consumers and businesses know what to expect; to the extent that any new law is necessary, it should only fill existing and identifiable gaps in that structure. Similarly, if there are new industries or specific trade practices that are of particular concern to policymakers, narrowly tailored regulations addressing those gaps should be developed. To the extent existing frameworks already exist, new regulations should be crafted within those existing structures.

Second, consideration and use of the existing framework will avoid unintended downstream confusion. There is no doubt that data-privacy regulation has important benefits to consumers and society as a whole—but *over*-regulation will be a net negative. Specifically, we want to ensure that state policymakers avoid: (1) creating duplicative requirements enforced by multiple state agencies; and (2) contradicting currently existing requirements. Complying with inconsistent laws and/or reporting to more than one state agency is a concerning possibility for business, as it risks uncertainty in expectations and enforcement while also increasing compliance costs.

In short, recommendations the committee ultimately makes should be consistent with what already exists, vesting clear authority for oversight and enforcement in the single regulatory agency for that industry as possible.

In light of the already-existing regulations, together with our hope that any additional regulations will be targeted to fill gaps and consistent with what is already in place, we specifically make the following requests of the committee:

- **Consider delaying recommendations for highly regulated industries or deferring to industry-specific regulators where appropriate.** There are several bases on which the committee may choose this path.

  - *The already-existing framework imposes significant data-protection responsibilities on businesses, including insurers.* Financial institutions already comply with the FCRA, GLBA, and RFPA, along with implementing regulations and regulatory guidance. For insurers, the Wisconsin Privacy of Consumer Financial and Health Information Regulation, adopted in response to GLBA and HIPAA, requires insurers to disclose privacy policies and practices and allows consumers to prevent disclosure of their information.

  - *Financial institutions and insurers are subject to other laws that limit their use of data.* Aside from the general protection of data, other laws also control the *use* of personal data by a financial institution or insurer. Examples include unfair discrimination and other underwriting or rating statutes regulating insurance companies, and equal credit and anti-discrimination statutes relating to the extension of credit by financial institutions. In this sense, financial institutions and insurers are prohibited from using data in certain ways. Generally, financial institutions and insurers may not take certain adverse actions solely on the basis of an individual's past criminal record, physical condition or developmental disability, age, marital status, sexual preference, or "moral" character.

  - *It is likely that additional data security and privacy safeguards may soon be effective, including a new data security statute for the insurance industry.* Prior to the COVID-19 pandemic, the Legislature was set to approve an industry-supported, Wisconsin-specific version of the National Association of Insurance Commissioners ("NAIC") Insurance Data Security Model Law, adopted in 2017.[1] This legislation was developed through a deliberate process involving regulators, insurers, and consumer advocates, and relies on the Office of the Commissioner of Insurance's (OCI) regulatory authority. Separately, through the NAIC, state insurance regulators are also currently considering whether improvements to data privacy are appropriate. That effort may lead to further revisions within the existing regulatory structure – which could be implemented in Wisconsin for the insurance industry and others.

  - *Wisconsin's insurers and financial institutions are already subject to significant and targeted regulatory oversight of data privacy and security.* Insurance regulators take a proactive approach in monitoring insurer compliance with already-existing data security and privacy requirements. The NAIC Financial Examiner Handbook and the Market Regulation Handbook provide guidance on examining information technology controls to help ensure entities are taking reasonable and necessary steps to protect consumers from theft or loss of personal information. In addition, the federal Interagency Guidelines Establishing Information Security Standards requires financial institutions to assess the risks posed to sensitive customer information and implement procedures to protect against those risks on an ongoing basis, with boards of directors and management oversight. The Federal Financial Institutions Examination Council recently released its Cybersecurity Assessment Tool to provide a concrete framework for determining the strength of an institution's security protocols. By focusing on risk assessments and governance, the guidance allows data security practices to be developed commensurate with an institution's risk profile, without a one-size-fits-all solution, and evolve as technology changes.

[1] If the legislature convenes in July this legislation may pass. If the legislature does not convene, we expect the legislation will be approved early in the 2021-22 legislative session.

- **If action is necessary, ensure it is targeted and consistent with the existing framework.**

  - *Work only within "gaps."* If the committee believes that further action is necessary, despite the already-existing regulatory framework, it should avoid duplicating any of the above-described laws and regulations. Rather, it should clearly identify what "gap" needs to be filled and limit its actions to addressing that limited need.

  - *Identify a single license-issuing regulatory body as the exclusive regulator for insurers and financial institutions already operating under the existing framework.* As the number of regulators overseeing an industry increases, costs and uncertainty increase as well. The potential for conflicting interpretations also increases. Any marginal benefit of increased oversight by a second regulator will be of particularly little value in already highly-regulated industries like insurance and financial services, which are subject to the oversight of their respective regulators.[2] The laws and regulations governing insurers and financial institutions already balance data privacy with other important considerations, including solvency, safety and soundness, and market conduct. These regulatory agencies also possess a unique understanding of the business practices and processes within these industries.

  - *Provide exemptions to entities that are subject to the already-existing framework.* For maximum consumer clarity, the committee should specify that businesses that already comply with HIPAA, GLBA, and state counterparts do not need to comply with any new, additional regulations that may be imposed. This is the approach the current framework has adopted, consumers expect it, and it should not be changed. Indeed, the California Consumer Privacy Act ("CCPA") took this approach in large part, by exempting personal information that constitutes PHI or non-public personal information from the data privacy requirements of CCPA, and the recently proposed Wisconsin Data Privacy Act, while not ideal, included similar exemptions for those categories of data (as well as other categories subject to regulation, including data subject to FCRA). Unfortunately, merely exempting data, as opposed to entities, caused additional confusion under CCPA. We support entity-level exemptions, as opposed to complicated data-based exemptions, which are hard for consumers to understand and difficult for businesses to operationalize in practice.

III. Principle 2: Retain and expand the risk-based approach to data privacy laws.

As already described, the existing regulatory framework relies on a concept of concentric circles, with the most sensitive personal data subject to the highest level of protections and less sensitive data subject to fewer requirements. The Advisory Committee should maintain this risk-based model for data privacy and security laws because it is consistent with consumer expectations. Indeed, one of the major challenges with CCPA, because of its broad definition of "personal information," is determining what exact information is subject to the law. For instance, should a name and address – information you can easily find online – be accorded protection equal to social security numbers, credit cards, and other sensitive personal information?

Lessons can be learned from the existing opt-in/opt-out structure for health and personal financial data in INS Chapter 25, which draws a distinction between various types of data and consumers' expectations for privacy. Under current law, Wisconsin has already enacted a regulatory

[2] We have provided a copy of this communication to Commissioner of Insurance Mark Afable and Department of Financial Institutions Secretary Kathy Blumenfeld with the hope that their firsthand knowledge and experience with the data privacy and security laws may also support these efforts to develop effective, industry-specific regulations.

structure that requires explicit approval for the release of health information ("opt-in"), given its extreme sensitivity. The same regulatory structure gives consumers the ability to actively prevent financial information from being shared ("opt-out") with non-affiliated third parties, given the less significant concerns surrounding that information. In other situations, providing notice to customers of how a business may use data is appropriate.

It is important to note that obtaining consent from consumers can be incredibly difficult, especially when businesses collect personal information over the phone, in person, and online. Businesses continue to struggle with CCPA's requirement to provide notice at the time of collection, especially when collection may occur on the phone, in a restaurant, at a football game, at a convention, or other offline locales. Subjecting all classes of data to these requirements would create a scenario where consumers were being constantly inundated with privacy policies, checkboxes, pop-ups, cookie consents, browser banners, and opt-in requests. Think about the number of times you have been asked recently to agree to a "click-wrap" agreement; now imagine having to take a similar action every time you visit a website, sign up for an email list, drop your business card in a jar at a convention, or provide your credit card to pay for food. The average consumer does not desire the additional transaction friction for every potential disclosure of information.

Wisconsin's existing data breach notification law respects consumer expectations, taking a reasonable position by requiring notification to consumers only when sensitive personal information has been accessed or disclosed. CCPA includes a similarly restrictive definition of personal information with respect to data breaches, such that notifications are required only when certain sensitive information is accessed or disclosed, and not when personal information such as IP address, address, or phone number are accidentally disclosed. Both the Wisconsin and California approaches match consumer expectations, leading to disclosures only when there has been a data breach or disclosure with increased potential for actual resulting harm.

The Wisconsin Data Privacy Act ("WDPA")—which was proposed but not passed earlier this year—stands in stark contrast to Wisconsin's current scheme. It defined the term "personal data" broadly to include information such as email address. As introduced, the law would have required breach notification to consumers every time such information was disclosed to a third party unless disclosure was "unlikely to result in a risk to the rights and freedoms of consumers."

Under the WDPA, Wisconsin businesses would also be required to notify consumers if they receive a consumer's personal information from another party, even for a legitimate business purposes—like a referral.[3] These requirements in WDPA would have caused a massive influx of emails and written notices to consumers, subverting the privacy protection component of the law in favor of nuisance communications. Moreover, the WDPA would have implemented a default opt-in system for practically all data—requiring affirmative consent for businesses to process any personal information, including names and addresses, except in certain limited and vague circumstances. The WDPA's one-size-fits-all regulation of personal data is not: (a) consistent with the expectations of consumers, (b) realistic in a technology-driven world, and (c) conducive to business innovation. The WDPA fails to make any attempt to fit within the existing regulatory scheme, except for exemptions regarding certain types of information subject to other regulatory schemes.

[3] Similarly, if an insurance agent was provided the name, email address, and telephone number of a prospect from a friend, the insurance agent would need to contact the prospect and provide a disclosure about how the insurance agent received that personal information, even if the prospect provided their information for that specific purpose. A final example is worthwhile. If an attorney received an email from a client that said company ABC wanted to fire Sally, under the WDPA the attorney would need to email Sally and let her know within thirty (30) days how the attorney obtained her information—that could be a problem if Sally doesn't know she will be fired.

The WDPA also proposed fines up to $20 million dollars for violations of its provisions. This number that is guaranteed to scare off businesses of all sizes and shapes from entering Wisconsin's business community and is unnecessary to provide an incentive to financial services companies to protect consumer information. In the event consumer information is compromised, financial services companies often bear the brunt of expenses associated with the breach. For example, credit and debit card issuers may be subject to fines from the card brand associations (such as Visa and Mastercard). Depository institutions may be liable to their customers for unauthorized transactions conducted under the card brands' zero liability programs and the Electronic Funds Transfer Act and Regulation E, regardless of whether the institution was at fault. Financial services companies suffering data breaches incur the second highest per record cost of responding to and remediating a breach, behind only the healthcare industry.

Beyond hard dollar losses, financial services companies can be exposed to serious reputational harm following a breach, which can contribute to lost revenue from customer attrition. The WDPA deficiencies noted above will subject businesses to vastly greater regulatory costs and burdens if enacted. Any benefits the law could bring to consumers may be outweighed by consumer exhaustion and apathy, and the law would almost assuredly reduce the effectiveness of data breach notifications. If the committee is looking to impose additional regulations, the WDPA model is not supported, as it is overly broad without commensurate consumer benefits.

IV. Principle 3: Proceed in an incremental fashion and do not place Wisconsin businesses and consumers at a disadvantage.

We urge state policymakers to take a measured and incremental approach to data privacy and security legislation, given the potential costs to and impacts on Wisconsin businesses.

Wisconsin should not be an outlier, a likely result if the committee adopted something similar to the WDPA. Wisconsin must maintain its status as an attractive place for businesses to locate and operate. This does not need to come at the cost of consumer protection as the two values are not mutually exclusive. The WDPA would have placed Wisconsin on a "regulatory island," making the state less attractive for all businesses—even exceeding California's prohibitive CCPA. We would strongly encourage the committee to not emulate CCPA or GDPR, but learn from the mistakes that have challenged the implementation of each law, and the struggles that businesses (including many in Wisconsin) have endured in trying to comply with the new regulatory schemes.

For example, the rollout of the CCPA was flawed, involving last-minute amendments passed by the California legislature that materially changed the law. Although CCPA went into effect on January 1, 2020, the California Attorney General just released final implementing regulations for the law on June 1, 2020—six *months* after CCPA took effect. The final regulations follow the release of three previous iterations of regulations, each with vastly differing interpretations of the law. Adding a further level of uncertainty, the law is likely to be significantly altered once again by the California Privacy Rights and Enforcement Act (CPREA) ballot measure. The instability with the underlying law has meant that regulators in California have struggled to provide guidance for businesses to comply with the complex regulatory schemes. Many businesses and commentators would agree that California still does not have it right. While regulators, legislators, commentators, and attorneys try to determine what CCPA requires, businesses are expending significant resources to materially comply with an uncertain, complex, and burdensome law which includes some facially contradictory regulations.

It is our hope the committee will continue in a deliberative fashion, and not rush recommendations that may benefit from incorporating the experiences of other jurisdictions. This

includes both the procedural implementation of those new standards as well as the efficacy of regulations in meeting consumer expectations.

The work of this committee is a first step in avoiding the same implementation challenges in Wisconsin; but other lessons can also be gleaned from the CCPA and GDPR processes. One lesson to be learned from CCPA is the massive cost it has had to date on California businesses. Initial compliance costs to businesses in California from CCPA is predicted to be $55 billion according to a study commissioned by the California Attorney General's Office and the California Department of Justice.[4] Another lesson to be learned from both CCPA and GDPR is that businesses have actively withdrawn from those markets in response to their restrictive data privacy regimes[5], proving that flawed data privacy regulations can impact not only businesses forced to comply with those regulations, but the economic activity and attractiveness of Wisconsin as a business-friendly state.

Undoubtedly, data privacy and security legislation will require Wisconsin companies of all sizes to contribute significant resources to attorneys, consultants, and new software products – costs that will surely be passed on to consumers and lead to an increase in the price of products and services.

We urge the Advisory Committee to keep the costs of the regulations top-of-mind. An incremental approach, building off existing structures and the principles discussed here can defray much of that cost while providing consumers with substantial protections. This approach will also increase the likelihood that these recommendations are enacted into law in the upcoming legislative session.

V. Conclusion

In summary, we encourage the Advisory Committee to embrace the following recommendations as it continues its deliberations on these important issues:

- Promote harmonization with existing data regulatory requirements and regulatory agencies to promote a more tailored approach that avoids duplicative or potentially inconsistent requirements.

- Adopt a risk-based structure for regulation of data that appropriately balances the burden of implementation with consumer expectations for privacy and the harm that attaches from unauthorized disclosure.

[4] *See* Standardized Regulatory Impact Assessment: California Consumer Privacy Act of 2018 Regulations, California Department of Justice by Berkeley Economic Advising and Research, LLC (August 2019), *available at* http://www.dof.ca.gov/Forecasting/Economics/Major_Regulations/Major_Regulations_Table/documents/CCPA_Regulations-SRIA-DOF.pdf; Lauren Feiner, *California's New Privacy Law Could Cost Companies a Total of $55 Billion To Get In Compliance*, CNBC (Oct. 8, 2019), *available at* https://www.cnbc.com/2019/10/05/california-consumer-privacy-act-ccpa-could-cost-companies-55-billion.html. The study also stated that compliance costs for the next decade could range from $467 million to over $16 billion. Most importantly, the study also found that the initial compliance cost to small businesses under 20 employees could be $50,000, $100,000 for companies up to 100 employees, $450,000 for companies up to 500 employees, and $2 million for companies over 500 employees.

[5] *See European Readers Still Blocked From Some US News Sites*, BBC News (June 26, 2018), *available at https://www.bbc.com/news/technology-44614885*; Hannah Kuchler, *US small businesses drop EU customers over new data rule*, Financial Times (May 23, 2018), *available at* https://www.ft.com/content/3f079b6c-5ec8-11e8-9334-2218e7146b04.

- Consistent with the risk-based approach, the definition of PII should be tied to some potential for harm from the disclosure. There are many innovative uses for data that benefit consumers. Recommendations of the committee should not stifle that innovation.

- Also consistent with the risk-based approach, Advisory Committee recommendations should follow existing opt-in/opt-out/disclosure structures. Different types of data should be subject to different levels of control based on the sensitivity and potential harm associated with the data.

- Proceed in an incremental fashion. Data laws are complex – ranging from breach notification to privacy to security. The Advisory Committee should avoid a one-size-fits-all omnibus piece of legislation, in favor of incremental progress, addressing a single issue at a time.

Thank you for your efforts to address these important issues. We look forward to continuing working collaboratively to develop an effective data privacy and security framework for Wisconsin residents and businesses.

Respectfully,

American Council of Life Insurers
American Property Casualty Insurance Association
Independent Insurance Agents of Wisconsin
National Association of Insurance and Financial Advisors - Wisconsin
National Association of Mutual Insurance Companies
Professional Insurance Agents of Wisconsin
Wisconsin Bankers Association
Wisconsin Council of Life Insurers
Wisconsin Credit Union League
Wisconsin Insurance Alliance

cc: Secretary-designee Randy Romanski, Department of Agriculture, Trade and Consumer Protection
Commissioner Mark Afable, Office of the Commissioner of Insurance
Secretary Kathy Blumenfeld, Department of Financial Institutions

22410356.11

August 10, 2020

Data Privacy and Security Advisory Committee
Wisconsin Department of Agriculture, Trade, & Consumer Protection
2811 Agriculture Drive
P.O. Box 8911
Madison, WI 53708-8911

Dear Committee Members:

Thank you for the opportunity to comment on the Data Privacy and Security Advisory Committee (Advisory Committee) created by the Wisconsin Department of Agriculture, Trade and Consumer Protection.

WSTA joins other comments sent to the Advisory Committee by sharing the concern the group may be heading toward recommendations that—while well intended—may negatively impact businesses and consumers. Productive data security and privacy legislation should support and protect both business and consumers, or it will fail to support and protect both.

In addition, we support the following concepts with respect to data privacy and security:

- Retention and expansion of risk-based regulation. Any other basis for regulation makes compliance little more than exercise in "checking the box." A risk-based approach develops security and privacy priorities for companies where actual risk or gaps exist.
- Avoidance of prescriptive requirements that are inflexible, quickly outdated, and inhibit security innovation and creativity.
- Consistency in regulation through federal legislative solutions, rather than state by state solutions. A patchwork of regulation across the country promotes confusion and gaps in protection.

Again, thank you for the opportunity to comment on the work of the Advisory Committee.

Please contact me directly if there are any questions or comments.

Sincerely,

/s/ William C. Esbeck
William C. Esbeck
WSTA Executive Director

PUTTING DREAMS to WORK
Since 1987
WWBIC

Greater Milwaukee
1533 N. RiverCenter Drive
Milwaukee, WI 53212
Phone: 414.263.5450

South Central
2300 S. Park Street, Suite 103
Madison, WI 53713
Phone: 608.257.5450

Southeast
600 52nd Street, Suite 130
Kenosha, WI 53140
Phone: 262.925.2850

245 Main Street, Suite 102
Racine, WI 53403
Phone 262.898.5000

Northeast
1191 N. Casaloma Drive
Appleton, WI 54913
Phone: 920.944.2700

info@wwbic.com
wwbic.com

August 31, 2020

Thank you to the Department of Agriculture, Trade and Consumer Protection (DATCP) agency for the opportunity to have Wisconsin Women's Business Initiative Corporation (WWBIC) be a part of the Data Privacy and Security Advisory Committee.

WWBIC, as a Community Development Financial Institution (CDFI), has been the leader in advancing economic development for the past 33 years impacting micro businesses across the State of Wisconsin. It is our hope that small businesses remain as a forethought as our policy leaders advance legislative regulations and procedural components to ensure protection and oversight around the areas of data privacy, security, and cybersecurity. Small businesses, unlike big box companies, do not have the funding to advance sophisticated technological platforms to protect against breaches that are now becoming the norm in our society. We request a careful and prudent review of any legislation that is put forward to assure that small businesses are not left from consideration as exemptions limits that may be set in the future, such has been provided in the GDPR and CCPA regulations.

Furthermore, a comprehensive plan around education will be most imperative as we look to ensure clear and concise understanding of protection under the law throughout the community. Simplification of language, a robust and user-friendly platform, and subject-matter experts to lead these training components will be most advantageous, not only to the community, but overarchingly to all stakeholders.

WWBIC also recommends the agency to partner with the Opportunity Finance Network (OFN) and the Association for Enterprise Opportunity (AEO). OFN is a national association of Community Development Financial Institutions (CDFIs); AEO assists entrepreneurs to access resources and services to contribute to economic growth nationally – WWBIC is a member with both entities. CDFIs create impact through the rural, urban and Native communities – nationally. These partnerships will provide benefits in fully grasping what may be at stake for small businesses (i.e. reputation, write-offs, etc.) should a comprehensive legislation is not secured.

WWBIC appreciates the opportunity to have been part of this very rich discussion and would be pleased to serve in whatever capacity the agency may feel will help propel this legislation forward.

Best wishes,

Kamaljit K. Jackson, MBA
Vice President for Programs and Operations