Analysis of Proposed Luetkemeyer Federal Data Breach Law

Mohammad Zaid Khaishagi

***Abstract*— This memorandum evaluates the proposed Luetkemeyer Bill which would be a federal data breach law superseding individual state laws. It would provide a single legislation which organizations would need to comply with. The various benefits of the Luetkemeyer Bill are discussed in the first section. An analysis of the drawbacks is made in the second section. In the third section, the personal views of the author are presented.**

I. Benefits of the Luetkemeyer Bill

In the current information era, the personal data collected by organizations about their users and customers is a valuable asset. As such, it needs to be protected from unlawful and unauthorized disclosure which could lead to material harm to those whose data was breached. Moreover, if the individuals are not made aware of such data breaches when they occur, it denies them the opportunity to take the necessary precautions and protect themselves against such harms as financial losses, fraud, or identity theft. For ensuring this goal, it is necessary to have a unified data breach notification law that does not exempt some organizations from its clauses and which effectively provides incentives for organizations to protect personal information as well as requires them to give prompt notification of such events to the relevant parties. Having such legislation helps to protect the personal information of individual customers, establish a strong economy, reduce compliance costs, and benefit the overall state of cybersecurity in industry.

A unified data breach notification law can help to uniformly protect the personal information of individuals that may not otherwise be protected due to weak state laws not covering many aspects of personal information. In such states like Mississippi, the definition of personal information only extends to an individual's SSN, state identification number, and financial login information [1]; this leaves out things like biometric data, medical information, health insurance information, and tracking of online activities. In Louisiana, personal information does not include medical information, or health insurance information [2]. Besides the disparities between what is covered, there are also differences in how data breach notifications are issued. For example, the California law describes in detail the requirements for the notification issued to California residents [3]. Just as with the definitions of personal information, Mississippi does not have such descriptions or requirements; the same is true for Arkansas and other states [4]. Such disparities leave the residents of some states more vulnerable and with less protection for their personal information than the residents of other states. By having a unified national law for data breach accountability and notification, it is possible to provide all individuals the same coverage and protection. The Luetkemeyer Bill ("the Bill") provides a description of the requirements of the contents of notification [5] such as with the California law, as well as details what may be considered as personal information, including biometric information, SSN, financial information, and credentials [5]. It provides a unified basis for all states to give comprehensive coverage as well as equal protection to their residents.

Enacting the Bill can also have an advantageous effect on the economy because of how it accounts for organizations of different sizes which may have different amounts of resources to allocate towards ensuring security of their systems against malicious attackers. The Bill provides for some flexibility in the applicability of the regulations that it proposes. It states that the safeguards required to be implemented by the organizations should be commensurate with the capability of the organization as well as the nature of activities that it performs [5]. This allowance means that the expectation from smaller organizations with regards to safeguards would not be the same as from a large multinational organization. This would allow smaller organizations to grow and not restrict innovation in the industry and so the industry as a whole would be able to grow. Additionally, this also prevents well established large organizations from gaining a monopoly. If the Bill had placed the same requirements upon all organizations, large or small, then it would have led to a situation where the legislation would suffocate innovation and smaller organizations.

The costs of compliance can also be mitigated by implementing a single data breach law. In having different laws for each state, those organizations that have customers across states have to comply with each of them instead of complying with a single law. This increase in costs is reduced since a single overarching law would supersede the disparate state laws.

In addition to these benefits, enacting the Bill would also help improve the general state of cybersecurity in industry and reduce the frequency and severity of security breaches. The Bill legislates the requirement of safeguards for organizations [5] as well as notification to relevant parties upon a security breach [5]. These measures ensure that organizations implement the basic security measures for personal information. Also, since organizations would be required to issue a notice upon breach which may result in potential loss of business, they would be incentivised to avoid such a situation, thus implementing the appropriate cybersecurity controls.

[1]Mohammad Zaid Khaishagi, College of Computing, Georgia Institute of Technology

II. Drawbacks of the Luetkemeyer Bill

Despite its benefits, the Bill also has its drawbacks in regards to protecting personal information, the general state of cybersecurity, and the strength of the economy and enacting the Bill may lead to undesired effects with respect to these points.

If an overarching federal data breach law is enacted which supersedes all state laws, then it could possibly be detrimental to the protection of personal information for individuals. The Bill proposes certain regulations for organizations to follow regarding the safeguards that they must implement and actions they must take when breaches occur. However, the Bill does not encompass certain things that are covered by some state laws. For example, in the California law, the personal information which is protected includes medical information, health insurance information, and information collected from automated licence plate scanning [3]. These items are not considered as personal information in the Bill [5] and thus it does not provide any protection for it. This means that this information would no longer be protected if the Bill was enacted into law. Such cases where the enacted legislation superseding state law is weaker than what was already in place damages the protection that residents of such states have. This could be improved by making the Bill stricter in terms of its safeguard and notification requirements. At the very least, it should cover all items that are already covered under state laws so that the protection enjoyed by residents of a state are not lost.

Furthermore, with a weaker federal law for data breaches, it is also possible to negatively impact the general state of cybersecurity among organizations. In the presence of a weak federal law superseding state laws, organizations would not be required to uphold the same level of security measures as they were required to under a state law that had been stronger. This leads to a situation where organizations can cut corners and try to reduce costs incurred from implementing security measures.

Another reason that the Bill can lead to poorer cybersecurity is that technology progresses at a much faster pace than the enactment or updation of legislation. So, as technology progresses, new threats are expected to arise which may be more sophisticated and which may target technology and information which the present legislation does not cover or is unable to preempt. With state laws, it is possible to have individual states implementing new laws to address advances in technology at a quicker pace [6].

For the strength of the economy, the Bill may not have any additional benefits over existing state laws. The CCPA, which is considered to be a strict law [7], already makes considerations for small and medium sized businesses [8]. This instance demonstrates that the resources and capabilities of an organization are not ignored by state laws. So, the provisions for smaller organizations with fewer resources that the Bill provides, may not offer much in terms of encouraging innovation and competition in industry.

III. Personal View on the Luetkemeyer Bill

In my personal view, the Luetkemeyer Bill should be enacted into law with some modifications. The Bill should be modified so that the requirements for safeguards, notifications and the definition for personal information are more comprehensive. Generally, the Bill should not exclude any protections that are already provided to individuals by existing state laws.

Enacting the Bill into law would help organizations by lowering the cost of compliance by requiring them to only satisfy the requirement of a single comprehensive law. Adhering to multiple laws that differ on multiple points adds to the operational costs of an organization. With a single federal law, the burden on organizations can be eased; which also enables greater investment towards innovation and developing the core services of the organization. This easing of compliance costs would not adversely affect cybersecurity if the provisions of the federal law are strong.

The protection of personal information of individuals is also benefited by the Bill provided that the clauses set forth in it are modified to be more comprehensive. If the coverage of personal information is expanded to include all the protections already provided by state laws, then a single federal law can help by providing that same level of protection to the residents of each state. This would not lead to a situation where, by providing protections for more people, the quality of the protection is reduced. This modification should include the requirements for security safeguards as well as notification requirements.

Similarly, the general state of cybersecurity can also be expected to benefit by enacting a stronger version of the Bill. Mandating a basic set of security measures and safeguards which organizations must implement would help reduce the security breaches; and providing stricter notification requirements would incentivise organizations to not let breaches happen at all. This means that organizations would like to take the appropriate measures to keep their systems and individuals' information secure.

Even though it may be true that state laws already account for the fewer resources available to smaller organizations, the Bill, as a federal superseding law would not have any detriments in this regard. The provisions made for smaller organizations ensure that smaller organizations are able to grow and innovation happens in industry. So, the fact that the Bill is not adding anything new in this regard to what the state laws already provide can be viewed as a positive characteristic in that it is imbibing in itself the merits of the state laws.

Finally, this can also be advantageous for the strength of the economy. Since the strict requirements of a federal data breach law would improve cybersecurity, it would follow that this reduces losses from the damage caused by cyberattacks. It would also reduce the costs of remediation and recovery since it can be expected that improved cybersecurity would reduce the frequency and severity of breaches.

REFERENCES

[1] "SECURITY BREACH NOTIFICATION CHART - Mississippi", *Perkins Coie*, 2020. [Online]. Available: https://www.perkinscoie.com/en/news-insights/security-breach-notification-chart-mississippi.html. [Accessed: 22-Feb-2021].

[2] "SECURITY BREACH NOTIFICATION CHART - Louisiana", *Perkins Coie*, 2020. [Online]. Available: https://www.perkinscoie.com/en/news-insights/security-breach-notification-chart-louisiana.html. [Accessed: 22-Feb-2021].

[3] "SECURITY BREACH NOTIFICATION CHART - California", *Perkins Coie*, 2020. [Online]. Available: https://www.perkinscoie.com/en/news-insights/security-breach-notification-chart-california.html. [Accessed: 22-Feb-2021].

[4] "SECURITY BREACH NOTIFICATION CHART - Arkansas", *Perkins Coie*, 2020. [Online]. Available: https://www.perkinscoie.com/en/news-insights/security-breach-notification-chart-arkansas.html. [Accessed: 22-Feb-2021].

[5] U.S. House of Representatives. 115th Congress, 2nd Session. (2018, Feb. 13). *H.R. ___, Data Acquisition and Technology Accountability and Security Act.* [Online] Available: https://gatech.instructure.com/courses/173394/files/folder/Projects/Project%201?preview=18898237.

[6] J. Sovern, "Why a U.S. federal privacy law could be worse than no law at all", *Fast Company*, 2019. [Online]. Available: https://www.fastcompany.com/90352025/why-a-u-s-federal-privacy-law-could-be-worse-than-no-law-at-all. [Accessed: 22-Feb-2021].

[7] T. Spring, "California Adopts Strictest Privacy Law in US", *Threatpost*, 2020. [Online]. Available: https://threatpost.com/california-adopts-strictest-privacy-law-in-u-s/151497/. [Accessed: 22-Feb-2021].

[8] A. Attkisson, "How California's Consumer Privacy Act Will Affect Your Business", *Business News Daily*, 2019. [Online]. Available: https://www.businessnewsdaily.com/10960-ccpa-small-business-impact.html. [Accessed: 22-Feb-2021].