Understanding Georgia's Next Steps in Data Breach Notification Standards

Juan Camilo Castrillon Davis

Abstract— **Oklahoma and California represent two sides of the same coin in data breach notification legislation. Oklahoma, while having more laxed definition in what constitutes personal information, champions protecting businesses from undue harm. California provides clear protection for business but emphasizes consumer protection with more rigorous standards of notification and business response time. Georgia currently sits with lackluster legislation on the topic and is looking for inspiration from other states to better protect its residents.**

I. In Support of Oklahoma

The Oklahoma data breach notification law provides an exemplary demonstration in balancing consumer protection with the capabilities of businesses. It ensures that there is no undue harm done to all scales of companies, while minimizing the amount of potential harm to their users and clients.

The statute's notification standards in particular show a consideration for ensuring that consumers get the information they need on a security breach in a well-documented and need-to-know manner. The statute states that an "entity… shall provide notice of any breach of the security of the system following determination or notification of the breach," which allows companies some time and discretion to understand and fix breaches before they are released to the public [1]. This ensures that the public does not get misleading information from a company if they have not had enough time to thoroughly audit the breach and understand its scope. On average it takes ~42 days for notice to be sent to consumers from the time of a breach occurring [2]. Furthermore, research shows that stakeholders in a company tend to discount disclosures of a breach if they are too close to the actual breach due to a perceived lack of information completeness [3].

The Oklahoma statute is also forward-thinking in terms of economic impacts of forcing companies to set up infrastructure to comply. It states that companies deploying "reasonable safeguards" and providing notice are exempt from such civil penalties, and companies that do not have "reasonable safeguards" but provide notice are limited to $75,000 in penalties plus damages [1]. Historically, start-ups and Small and Medium-sized Businesses (SMBs) have trouble allocating proper resources and finding talents to implement proper security measures [4]. This clause in the bill balances providing incentive for good cybersecurity while also enabling SMBs to recover and grow from potential incidents.

An incentive for good cybersecurity is often hard to establish, and the Oklahoma statute provides this through decreasing information asymmetry through notice. In addition to providing notice after a breach, Oklahoma extends this requirement by mandating that companies provide notice "if the breach involves a person with access to the encryption key," even if the data stolen was still encrypted [1]. This ties back into the amount of information asymmetry that exists, particularly around cybersecurity. By requiring more scenarios in which a company must comply with this statute, Oklahoma increases the transparency of subtle, yet relevant, methods of causing larger data breaches. Information asymmetry is dangerous for consumers due to its ability to create markets where consumers cannot accurately assess the value of a good or service. This effort to give critical information to consumers ensures that companies deploy robust data security practices to become competitive in their respective market [5].

The issue of undue burden on businesses when it comes to information security is often hard to reconcile with the need to reduce information asymmetry in the economy but is an important topic when consumers' personal information is at stake. Oklahoma's statute in particular champions creating a competitive economy while also ensuring that consumers are informed on how their personal data is maintained. This grants the twofold benefit of informed decision making by consumers and scalable requirements to ensure the growth and financial protection of businesses.

II. In Support of California

The California statute raises the bar of transparency and provides a high standard of information delivery that empowers consumers and companies to understand and invest more in measures to protect themselves. It standardizes communication to consumers, making it easier for them to make informed decisions, and it protects companies from excess penalties already defined in separate legislation in California.

A critical distinction that the California statute has is the timeframe for reporting an incident. The statute states that notice must be given "within 30 days of discovery or notification of the data breach" [6]. This is quicker than the average notification time mentioned previously, which can lead to a lack of quality and clarity in information [3], however it does reduce the average cost to a consumer who is breached [7]. To combat the downsides of rapid notification, California added a helpful clause that standardizes the format of information. It outlines every question and piece of information that must be delivered to consumers and provides a standard template for companies to use. If universally used, it can increase user readability and overall access to information through giving consumers a consistent format to learn and understand [8][9].

California ensures business protection by actively excluding explicit penalties for non-compliance with this statute. California contains other legislation such as the California Consumer Privacy Act (CCPA). The CCPA concretely covers consequences for data breaches with fines through private right of action, so the omission of strict enforcement penalties guarantees that companies are not punished twice for the same

violation [10]. California also allows freedom for businesses to have their own notification procedures, so long as they comply with the mediums for communication established in statute [6]. This gives companies the freedom to create systems that fit their structure and resources, so long as they are meeting baseline requirements.

A reason that this statute is so avoidant of creating undue burden on companies is because of both broader and stricter requirements that it has in terms of cybersecurity. In addition to notifying consumers quicker, California also requires that businesses that do not own the data that has been breached to "notify the owner or licenser of the information of the breach of the security of the data immediately following discovery" [6]. This is a critical step in ensuring that attacks do not spread, and generally good practice in cybersecurity when looking at entire supply chains. Immediate disclosure of a new breach, although potentially misleading, has been shown to increase legitimate and effective investment by companies into cybersecurity [11]. Furthermore, the extent of what is classified as personal information is very broad, adding: medical, genetic, health insurance, and login information [6]. This creates a higher standard of data security by recognizing that there are many types of information that can be traced back to a person; studies have shown that a zip code, birthday, and sex can be enough to identify a person, which emphasizes a need to treat more data equally in the lens of information security [12].

California's progressive approach to understanding the scope of personal information and mandating quick notice allows for consumers to be more protected and informed in a consistent manner while indirectly incentivizing companies to invest in better security.

III. Amendments to Georgia Bill

In terms of amending the Georgia data breach notification law, taking an approach that is (mostly) aligned with California is best for protecting its residents without surrendering Georgia's influence as a southern economic hub. Atlanta is consistently classified among top cities nationally and globally in terms of GDP [13][14]. Additionally, entrepreneurship has been increasingly prevalent in Atlanta's economy, which means that there is a lot of venture capital flowing into the city and subsequently leading to innovation through tech start-ups [15]. This indicates how central data is becoming to business, so it is in the state's best interest to be proactive and build consumer protection and trust early.

The Georgia statute should incorporate more precise language as to what classifies as personal information, using California's definition as a baseline. Currently the statute seems to be up to the discretion of businesses for what constitutes personal information. Providing clarity would ensure that businesses know what their duties are for reporting, and it would increase consumer awareness as to what data can be harmful when compromised. Along similar lines, Georgia should include a template, and what information must be disclosed, like California's for notifying consumers. This would alleviate pressure on businesses to understand and self-assess their notifications meeting state standards and increase the readability and accessibility of the information to consumers.

Finally, Georgia should incorporate limits on penalties for failure to comply like Oklahoma. Currently there is no language in the statute about what limits there are to enforcement of the bill, which exposes businesses to potentially crippling lawsuits that reconcile the damages for a breach. Including language surrounding limits on civil penalties and scaling it to account for SMBs would protect them from undue harm while maintaining greater accountability and incentive to invest into appropriate cybersecurity measures for their business.

References

[1] Oklahoma Security Breach Notification Act, 24 Okla. Stat. §§ 161–166, Oklahoma Legislature, Title 24: Debtor and Creditor, enacted Nov. 1, 2008; amended by Laws 2025, c. 406, § 2, eff. Jan. 1, 2026. Available: https://law.justia.com/codes/oklahoma/title-24/section-24-161/ and § 24-163.

[2] M. Ser-Jan, "IAPP," *Iapp.org*, Sep. 17, 2017. https://iapp.org/news/a/from-incident-to-discovery-to-breach-notification-average-timeframes (accessed Feb. 12, 2026).

[3] M. Ashraf, J. (Xuefeng) Jiang, and I. Y. Wang, "Are There Trade-Offs with Mandating Timely Disclosure of Cybersecurity Incidents? Evidence from State-Level Data Breach Disclosure Laws," *The Journal of Finance and Data Science*, vol. 8, Sep. 2022, doi: https://doi.org/10.1016/j.jfds.2022.08.001.

[4] A. Chidukwani, S. Zander, and P. Koutsakis, "Cybersecurity Preparedness of Small-to-Medium Businesses: A Western Australia Study with Broader Implications," *Computers & Security*, vol. 145, pp. 104026–104026, Jul. 2024, doi: https://doi.org/10.1016/j.cose.2024.104026.

[5] R. Anderson and B. Schneier, "Economics of Information Security," *IEEE Security and Privacy Magazine*, vol. 3, no. 1, pp. 12–13, Jan. 2005, doi: https://doi.org/10.1109/msp.2005.14.

[6] "2024 California Code Civil Code - Section 1798.82," *Justia Law*, 2024. https://law.justia.com/codes/california/code-civ/division-3/part-4/title-1-81/section-1798-82/.

[7] S. Romanosky, R. Telang, and A. Acquisti, "Do data breach disclosure laws reduce identity theft?," *Journal of Policy Analysis and Management*, vol. 30, no. 2, pp. 256–286, Mar. 2011, doi: https://doi.org/10.1002/pam.20567.

[8] J. Versloot et. al., "June 2015 - Volume 13 - Issue 2 : JBI Evidence Implementation," *Lww.com*, 2015. https://journals.lww.com/ijebh/abstract/2015/06000/format_guidelines_to_make_them_vivid.

[9] T. Hillesund and J. E. Noring, "Digital Libraries and the Need for a Universal Digital Publication Format," *The Journal of Electronic Publishing*, vol. 9, no. 2, Aug. 2006, doi: https://doi.org/10.3998/3336451.0009.203.

[10] "California Code, Civil Code - CIV § 1798.150 | FindLaw," *FindLaw*, 2024. https://codes.findlaw.com/ca/civil-code/civ-sect-1798-150/.

[11] X. Wang, W. W. Li, A. C. M. Leung, and W. T. Yue, "To alert or alleviate? A natural experiment on the effect of anti-phishing laws on corporate IT and security investments," *Decision Support Systems*, vol. 179, p. 114173, Apr. 2024, doi: https://doi.org/10.1016/j.dss.2024.114173.

[12] L. Sweeney, “Simple Demographics Often Identify People Uniquely,” Sweeney, 2000. Available: https://privacytools.seas.harvard.edu/sites/g/files/omnuum6656/files/privacytools/files/paper1.pdf.

[13] The, “PGC Group | Employer of Record - USA & Canada,” *PGC Group | Employer of Record - USA & Canada*, Jun. 21, 2024. https://pgcgroup.com/blog/us-states-gdp-compared-to-countries.

[14] D. Wood, “These Cities Have Bigger Economies Than Entire US States,” *24/7 Wall St.*, Jan. 20, 2025. https://247wallst.com/news/2025/01/20/these-cities-have-bigger-economies-than-entire-us-states (accessed Feb. 13, 2026).

[15] P. Grover, A. Basu, and M. Ben-Yousef, “BCG -Leveling-up: unlocking the entrepreneurship growth potential in Atlanta Leveling-up: unlocking the entrepreneurship growth potential for Atlanta,” 2024. Available: https://media-publications.bcg.com/Leveling-Up-Unlocking-Entrepreneurship-Growth-Potential-for-Atlanta.pdf.