# The Balancing Act: Navigating the Tight Rope of Online Privacy

An STS Research Paper
presented to the faculty of the
School of Engineering and Applied Science
University of Virginia

by

Caleb Stoltz

March 14, 2024

On my honor as a University student, I have neither given nor received unauthorized aid on this assignment as defined by the Honor Guidelines for Thesis-Related Assignments.

*Caleb Stoltz*

STS Advisor: Peter Norton

## Introduction

In the internet age, policymakers are engaged in a balancing act between open communication and personal data privacy. To data collectors, user data is lucrative; many users, however, regard such data as personal and private information. According to the US Census Bureau, "in 2013, 74.4 percent of all households reported Internet use, with 73.4 percent reporting a high-speed connection" (File, Ryan, 2014). Ecommerce enterprises, data collectors, and privacy advocacies compete to draw the line between legitimate and proscribed collection of personal data online. In 2021, Mckinsey & Company asserted that "data-driven campaigns" were "poised to increase sales in a core product by more than 10 percent" (Bibby et al., 2021).

By conducting an in-depth analysis of existing research, published information on online data collection, current controversies, and legal actions, I aim to further delineate a boundary and establish a balanced perspective on the conflicting dynamics of data acquisition practices and the preservation of personal privacy. For current statistics and better results, I will use only research from the year 2000 and forward. The research done in the earlier stages of the internet could skew results due to the lack of research at the time and outlier data. This research argues that the future delineation between legitimate and verboten online personal data collection will hinge not only on the tactics and efforts of e-commerce enterprises and data collectors but critically on the united efforts of privacy advocacies and the creation of sturdy legislative frameworks. Examining a broad scope of research, this will portray that a sustainable equilibrium can be achieved through transparent data practices, informed consumers, and adaptive regulatory policies, ensuring that the digital age's connective potential does not come at the cost of individual online privacy.

**Review of Published Research**

To further contour the line between legitimate and illicit collection of personal data, the examination of previous research on data privacy within e-commerce will aid new positions and conclusions. Beginning with a similarly structured study done on "Legal Protection of E-Commerce Consumers Through Privacy Data Security" in Indonesia in by Sugeng and Fitria, the 2020 study contends that:

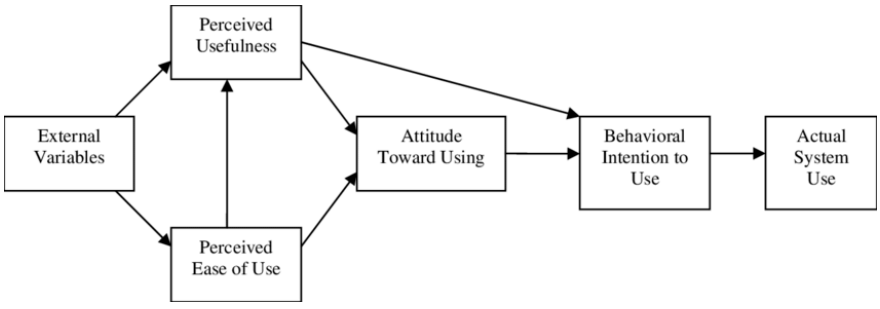
> To protect the rights of e-commerce consumers, comprehensive regulations regarding the protection of personal data are needed. In addition, to resolve consumer disputes, it is necessary to strengthen the online dispute resolution mechanism and personal data security as a Consumer Protection Instrument. This study recommends further research that can compare the application of the PDP Law in several countries, especially regarding supervisory agencies that can control the use of consumer personal data by electronic system administrators and marketplace companies. (Sugeng & Fitria, 2021, p. 283)

Sugeng and Fitria assert the pressing need for "comprehensive regulations regarding the protection of personal data" and the desire to "strengthen the online dispute resolution mechanism and personal data security" in their conclusion. This call to action not only highlights the lack of consumer protection laws globally but also underscores the effectiveness of online dispute resolution methods with a rapidly growing online economy and transactions. While providing insights into safeguarding consumer data, particularly within Indonesia, it also opens up pathways of further exploration on how to implement complex regulations across diverse legal and cultural environments. Further research into building a "foundational framework" by

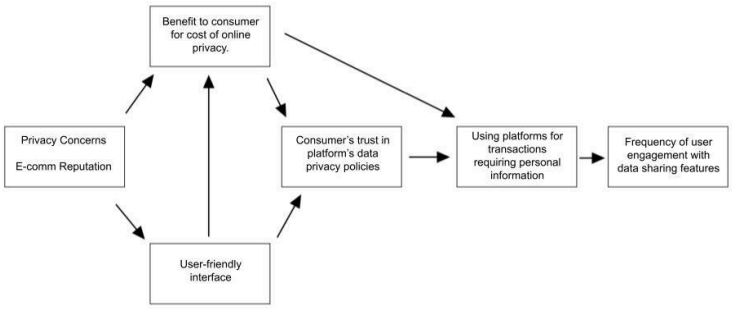
comparing current laws across various jurisdictions would help locate the best practices for a universally applicable standard.

Furthermore, the research by Sugeng and Fitria identifies many vulnerabilities within e-commerce transactions as highlighted by the insistence on the growing digital economy and its reliance on "informal trade or social trade which is driven by small business actors" using popular social media platforms for business transactions. (Sugeng & Fitria, 2021, p. 276) However, the study does not extensively explore consumer behavior or education on data privacy. Addressing these research gaps not only complements past research but will aid the development of a more holistic approach to the faced challenges and the protection of online consumers.

Along with current research, the knowledge of certain methodologies, models, and theories could be beneficial to a stronger understanding and framework for legal personal data collection. In regards to the previous conclusion reached by Sugeng and Fitria, the use of the Technology Acceptance Model, or TAM. The technology acceptance model "proposes that perceived ease of use and perceived usefulness predict the acceptance of information technology (Liu & Ma, 2004, p. 59)." The model was originally created in 1989 by Fred Davis but has adapted along with the current level of technology. Building on the foundational insights Sugeng and Fitria brought, the incorporation of the TAM could deepen the understanding of consumer interactions within digital marketplaces and build legislation upon those interactions. As stated earlier, Indonesia's



digital economy is heavily reliant on small businesses that complete transactions over large social platforms with ease of use (Liu & Ma, 2004, p. 59). In Figure 2, we can see the use of the technology acceptance model in regard to the specific topic of consumer data privacy. The model could uncover valuable insights into the efficacy of privacy assurances and legislative protections in shaping these perceptions.




In a similar light to the Technology Acceptance Model, the Privacy Calculus Theory offers a complementary lens through which to understand consumer behavior. This theory states that "people will self-disclose personal information when perceived benefits exceed perceived negative consequences" (Dienlin & Metzger, 2016). The Privacy Calculus Theory would similarly aid Sugeng and Fitria's argument, offering a theoretical framework to dissect decisions consumers make when navigating e-commerce platforms.

Dienlin and Metzger's research, "An Extended Privacy Calculus Model for SNSs," expands upon the Privacy Calculus Theory by integrating self-withdrawal behaviors and privacy self-efficacy. Within their results, they discovered that:

> Moreover, both privacy concerns and privacy self-efficacy positively predicted use of self-withdrawal. With regard to predicting self-disclosure in SNSs, benefits outweigh privacy concerns; regarding self-withdrawal, privacy concerns outweighed both privacy self-efficacy and benefits (Dienlin & Metzger, 2016).

This provides a more holistic view of a consumer's thought process for social networking services (SNS), a large portion of e-commerce. Not only do they manage their online presence through information they choose to share, but also what they choose to withhold by account deletion and data removal requests.

In the context of my thesis, the extended Privacy Calculus theory that Dienlin & Metzger propose offers a valuable framework for analyzing consumer behavior in e-commerce platforms. Just as SNS users weigh the benefits of self-disclosure against privacy risks, e-commerce consumers weigh the advantages of personalized shopping experiences against the potential misuse of data. The concept of self-withdrawal that Dienlin and Metzger discover resonates with increasing consumer demand for control over personal data, shown in behaviors like account deletion or the removal of personal information.

In unifying insights from existing research, notably the work of Sugeng and Fitria (2021), and integrating the suggested models of the Technology Acceptance Model and the Privacy Calculus Theory, this research sets the stage for a deeper understanding of consumer behavior, technological adaptations, and data privacy within the e-commerce landscape. While previous studies have laid the legal frameworks, this research seeks to build upon these problems by exploring the psychological and behavioral dimensions that govern consumer engagement with platforms.

**Navigating the Frontier: Balancing E-Commerce Innovation and Personal Data Privacy**

E-commerce websites and apps are intricately designed to not only contain seamless user interfaces but also strategically collect and analyze consumer data. The rapid growth of the internet in the twenty-first century, especially during the COVID-19 pandemic, has significantly

impacted e-commerce sales. According to Brewster (2022) with the United States Census Bureau: “According to the most recent 2020 ARTS release, e-commerce sales increased by $244.2 billion or 43% in 2020, the first year of the pandemic, rising from $571.2 billion in 2019 to $815.4 billion in 2020.” As e-commerce sales continue to rise, the growth not only expands the digital marketplace but the volume of consumer data generated through these platforms. According to a General Electric (2013) study 81% of e-commerce consumers research products before making purchases, providing an ample amount of data for companies to analyze and insert into individual user interfaces. E-commerce behaviors are shifting towards smartphones and other mobile platforms, with mobile e-commerce expected to account for 42.9% of total e-commerce sales by 2024 in a forecast from Insider Intelligence (2022). This emphasizes the importance of mobile device consumer data collection for companies in the near future. These highlight the extensive efforts and resources e-commerce platforms invest in gathering and analyzing consumer data to enhance their strategies, offerings, and profitability.

**Current Landscape of Global Data Privacy Legislation**

The current landscape of data privacy legislation reveals a patchwork of laws that vary significantly across jurisdictions. Notable regulatory frameworks currently include the European Union’s tight-knit General Data Protection Regulation (GDPR) and the United States California Consumer Privacy Act (CCPA) being the first state-level legislation on online privacy. Despite these advanced frameworks, critical gaps in data privacy legislation provide an overarching law neither on the national or international scale. This regulatory shortfall is highlighted by the Federal Trade Commission (FTC), the primary body overseeing data privacy in the United States. The FTC reported that there were more than 10 billion dollars reported lost in 2023, with

e-commerce ranking as the second most affected sector following human imposter fraud (FTC, 2024). Further emphasizing the point, the United States Government Accountability Office, who advises Congress directly, stated that the FTC, “has not issued regulations for Internet privacy other than ones protecting the privacy of children.” The office advocated for a comprehensive Internet privacy law, suggesting that such a measure would significantly bolster consumer protection by constructing clear fences against certain behaviors. (U.S. GAO, 2019)

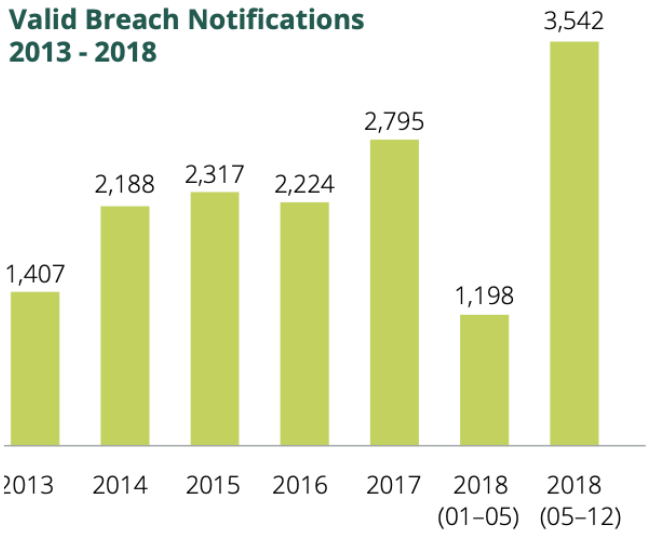
This fragmented regulatory system is further complicated by the recent legislation aimed at large platforms, such as the case of TikTok. The US House of Representatives recently passed a bill looking for a nationwide ban on TikTok unless separated from ByteDance, the parent company. With potential endorsement from President Joe Biden himself, the bill's passage derives from a broader challenge: the outdated legal frameworks that do not fully address the risks of the digital age. A privacy advocacy group, the Center for Strategic and International Studies (CSIS), states that:

> The national security risk of using TikTok is easily exaggerated. Intelligence agencies routinely scrape social media to collect biographical information and do not need ownership of TikTok (or any other social media platform) to do this. The question is, how much more does China obtain by having access to TikTok data that is not publicly available? There is probably some benefit, but it is likely small. (Lewis, 2022)

The CSIS perspective that the national security risks associated with TikTok might be overstated does not diminish the importance of scrutinizing data handling practices by foreign-owned companies. The ongoing problem reflects the complexity of data privacy in a world where digital platforms transcend national boundaries. It also reflects how the current legislation efforts fall short and the need for a cohesive international strategy for digital privacy and security. A call for

enhanced interaction among nations, big tech e-commerce companies, and privacy advocates to establish user privacy norms in acknowledgment of the global nature of the internet.

Building off the foundational contention about the current fragmented landscape of data privacy legislation, it is evident some overarching policies have had an effect on their jurisdiction like the General Data Protection Regulation (GDPR) in the European Union. The GDPR not only provides extensive descriptions of the data privacy rights of individuals, but also provides foundational rules for e-commerce businesses, data controllers, and consumers. Data from the Data Protection Commission of Ireland (2019) illustrates a marked uptick in the reporting of valid data breaches within just 7 months of GDPR's implementation in the graph, a stark contrast to the years preceding its enforcement. This surge in breach notifications not only points to the inadequacies of prior regulations in detecting breaches but also enhances transparency for consumers regarding the security of their data.




A report presented to Congress by a seasoned expert in economic relations advocates for a GDPR-like framework to be adopted in the US, highlighting its global impact and the robust enforcement mechanisms it embodies. Chase (2019) commends the enforcement efforts the GDPR offers on US and European companies, stating that “lawyers abound and compliance departments have serious clout, not complying with the strictest interpretation of the law as

written is not an option." Specifically, Article 83, paragraph 6 of the GDPR (2018) stipulates that:

> Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.

These rigorous enforcement measures compel e-commerce companies and big tech to significantly bolster their data privacy budgets and enhance transparency with their user base. This scenario underscores the potential of overarching legislation across multiple countries to delineate the boundary between permissible and prohibited personal data collection practices, ensuring a clearer and more enforceable framework for data privacy.

**The Impact of Privacy Advocacies On Data Privacy Legislation**

After examining globally known regulatory frameworks, it's evident that privacy advocacies are crucial in shaping these frameworks. These groups catalyze the evolution of data privacy through awareness campaigns, legislative testimonies, and public engagement. The Electronic Frontier Foundation(EFF) in the United States "fights in the courts and Congress to maintain your privacy rights in the digital world, and works with partners around the globe to support the development of privacy-protecting technologies. (EFF, 2022)"

For instance, the EFF and the Asian American Liberation Network challenged the Sacramento Municipal Utility District and the City of Sacramento. They filed a lawsuit against local authorities for unlawfully searching residential energy usage data to locate cannabis cultivation, selectively targeting Asian-owned households while sparing predominantly white

neighborhoods. This presents not only a problem with corporate businesses but also with the local governments and their abuse of consumer data. The EFF (2022) stated that “national governments must put legal checks in place to prevent abuse of state powers, and international bodies need to consider how a changing technological environment shapes security agencies’ best practices.”

The work of privacy advocates extends beyond the courtroom; The International Association of Privacy Professionals reported that 2022 saw an increase in user privacy complaints and fines towards corporations globally, highlighting the efforts of advocacies in consumer protection (Bryant et al., 2022). Furthermore, Privacy International (PI) has had a major role in the exposure of complaints against AdTech with the implementation of the GDPR. PI (2021) aided “noyb”, a non-profit organization that defends consumer digital rights in Europe, in releasing over 500 complaints to companies relating to data cookie banner's non-compliance with the GDPR.

A comparative study by Varone et al. (2020) across California and Switzerland quantified the effectiveness of advocacy groups, assigning them a success score of 0.67. The large-scale study, including 898 unique groups, influenced six policy processes between California and Switzerland in their respective regions. This indicates that advocacy groups frequently achieve at least part of their policy objectives, influencing policy decisions and ensuring consumer interests are adequately represented and protected. This illustrates that the presence of advocacy groups leads to more effective policy making and reinforces consumer protection, supporting their inclusion in the idea of a well-regulated legislative boundary that defines data protection laws.

**E-Commerce Data Practices and Consumer Trust**

Navigating through the intricacies of regulatory frameworks and advocacy influences in the digital marketplace, the importance of data practices in e-commerce and their effects on consumers becomes clear. The value of consumer data is underscored by Anant et al. (2020), who estimated the personalized advertising and marketing industry to be worth over $300 billion. Despite some consumer hesitance to input data for programs like rewards, there is implicit consent to data collection, often overshadowed by concerns about how data is tracked and used. Tools such as web cookies, app usage data, and web beacons frequently raise concerns due to their opaque purposes. Fazlioglu (2023) from the IAPP reported that "Nearly 68% of consumers throughout the world said they are either somewhat or very concerned about their online privacy."

This widespread fear significantly impacts consumer trust in online corporations. Amazon (2022) released an article on maintaining customer trust through data privacy that claims to employ transparent data usage practices. This includes a clear privacy policy and options for users to control their data to maintain a high level of trust. As a leading e-commerce giant, Amazon exemplifies the proactive approach to handling customer data with transparency, user control, and privacy as core principles. Conversely, the case of Morele.net, as studied by Strzelecki and Rizun (2022), illustrates the detrimental impact of inadequate data security measures. Following a severe data breach exposing the personal data of their customers, a loss of approximately 33% of customers followed, showcasing the crucial role of trust in maintaining consumer relationships. Moreover, the perception gap between corporate executives and consumers concerning data is stark. Narula's (2014) Deloitte Consulting study found that while

50% of business executives believe their privacy efforts suffice, only 37% of consumers share that sentiment, signaling a critical disconnect that influences consumer loyalty and behavior.

**Conclusion**

This study has ventured deep into the fight where e-commerce enterprises, data collectors, and privacy advocacies compete to define the boundaries between permissible and impermissible personal data collection practices online. The problem in this competition not only lies in the act of data collection but also in what constitutes ethical use and transparent handling of personal data. The research revealed that while technological innovations provide a plethora of opportunities for business growth, the escalation of personal privacy risks demands a more dynamic regulatory framework.

Privacy advocates emerge as a pivotal member in the narrative, driving toward more stringent and transparent regulatory frameworks. Groups like Privacy International and the Electronic Frontier Foundation haven't only persuaded legislation like the GDPR in Europe, but provide public and corporate awareness of the need for data privacy. Moreover, the contrast in data handling and consumer trust between companies like Amazon and the case study of Morele.net provides a stark illustration of how privacy policy perceptions affect consumer trust and corporate reputation. This discrepancy highlights the need for businesses to align more closely with consumer privacy values and potentially redefine corporate strategies toward data handling.

This use of this research extends beyond the realm of e-commerce businesses and consumer data privacy; Many principles expanded on could lead to broader discussions in cybersecurity, digital rights, and global digital policy-making. As the digital landscape evolves,

further research is needed to explore these topics in greater detail, particularly focusing on the integration of artificial intelligence in data processing and its use in security standards.

This research not only deepens our understanding of the current state of data privacy and the wavering line of user data privacy but also sets the stage for ongoing academic, legislative, and practical debates. It calls for a conjoined effort from all competitors to forge a clear path to personal data collection and handling that respects consumer privacy while fostering innovation and economic growth. Moving forward, the journey to creating a fair equilibrium of legitimate and verboten collection of personal data between competing interests of the people and e-commerce businesses will be crucial to the future of digital society.

## References


Amazon. (2022, January 28). Amazon is earning and Maintaining Customer Trust through privacy. Amazon. https://www.aboutamazon.com/news/how-amazon-works/amazon-is-earning-and-maintaining-customer-trust-through-privacy

Anant, V., Donchak, L., Kaplan, J., & Soller, H. (2020, April 27). The consumer-data opportunity and the privacy imperative. McKinsey & Company. https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights%20/the-consumer-data-opportunity-and-the-privacy-imperative

Art. 83 GDPR – general conditions for imposing administrative fines. General Data Protection Regulation (GDPR). (2018, May 25). https://gdpr-info.eu/art-83-gdpr/

As Nationwide Fraud Losses Top $10 Billion in 2023, FTC Steps Up Efforts to Protect the Public. Federal Trade Commission. (2024, February 9). https://www.ftc.gov/news-events/news/press-releases/2024/02/nationwide-fraud-losses-top-10-billion-2023-ftc-steps-efforts-protect-public

Asian American Liberation Network V. Smud, et al.. Electronic Frontier Foundation. (2022, November 3). https://www.eff.org/cases/asian-american-liberation-network-v-smud-et-al

Bibby, C., Gordon, J., Schuler, G., & Stein, E. (2021, March 25). The big reset: Data-driven marketing in the next normal. McKinsey & Company. https://www.mckinsey.com/capabilities/growth-marketing-and-sales/our-insights/the-big-reset-data-driven-marketing-in-the-next-normal

Brewster, M. (2022, April 27). Annual Retail Trade Survey Shows Impact of Online Shopping on Retail Sales During COVID-19 Pandemic. Census.gov. https://www.census.gov/library/stories/2022/04/ecommerce-sales-surged-during-pandemic.html

Chain Store Age. (2013, July 7). Study: 81% research online before making big purchases. Chain Store Age. https://chainstoreage.com/news/study-81-research-online-making-big-purchases

Chase, P. H. (2019). Perspectives on the General Data Protection Regulation Of the European Union.

Dienlin, T., & Metzger, M. J. (2016). An Extended Privacy Calculus Model for SNSS: Analyzing Self-Disclosure and Self-Withdrawal in a Representative U.S. Sample. *Journal of Computer-Mediated Communication*, *21*(5). https://doi.org/10.1111/jcc4.12163

Fazlioglu, M. (2023, March). IAPP privacy and Consumer Trust Report – executive summary. IAPP Privacy and Consumer Trust Report – Executive Summary. https://iapp.org/resources/article/privacy-and-consumer-trust-summary/

File, T., & Ryan, C. (2014, November 13). Computer and Internet Use in the United States: 2013. United States Census Bureau. https://www.census.gov/library/publications/2014/acs/acs-28.html

LaCasse, A., Bryant, J., & Duball, J. (2022, December 20). A look back at privacy and data protection in 2022. https://iapp.org/news/a/a-look-back-at-privacy-and-data-protection-in-2022/

Law, T. J. (2022, November 6). 19 Powerful Ecommerce Statistics That Will Guide Your Strategy In 2023. Oberlo. https://www.oberlo.com/blog/ecommerce-statistics

Lewis, J. A. (2022, November 14). Tiktok and the First Amendment. Center for Strategic & International Studies. https://www.csis.org/analysis/tiktok-and-first-amendment

Ma, Q., & Liu, L. (2004). The Technology Acceptance Model: A Meta-Analysis of Empirical Findings. *Journal of Organizational and End User Computing*, 59–59. https://doi.org/10.4018/978-1-59140-474-3.ch006

Narula, A. (2014, November 14). Building Consumer Trust. Deloitte Insights. https://www2.deloitte.com/us/en/insights/topics/risk-management/consumer-data-privacy-strategies.html

noyb issues over 500 complaints for non-compliant cookie banners. Privacy International. (2021, May 31). https://privacyinternational.org/examples/4578/noyb-issues-over-500-complaints-non-compliant-cookie-banners

Privacy. Electronic Frontier Foundation. (n.d.). https://www.eff.org/issues/privacy

Strzelecki, A., & Rizun, M. (2022). Consumers' Change in Trust and Security after a Personal Data Breach in Online Shopping. *Sustainability*, *14*(10). https://doi.org/10.3390/su14105866

Sugeng, & Fitria, A. (2021a). Legal Protection of E-Commerce Consumers Through Privacy Data Security. *Proceedings of the 1st International Conference on Law and Human Rights 2020 (ICLHR 2020)*. https://doi.org/10.2991/assehr.k.210506.038

Varone, F., Eichenberger, S., Gava, R., Jourdain, C., & Mach, A. (2020). Business Groups and Advocacy Success: Insights from a Multi-venue Approach. *Acta Politica*, *56*(3), 477–499. https://doi.org/10.1057/s41269-020-00162-8

Your Internet Privacy. U.S. Government Accountability Office. (2019, February 19). https://www.gao.gov/blog/2019/02/19/your-internet-privacy#:~:text=Information%20resellers%3A%20No%20overarching%20federal,legislation%20has%20not%20been%20enacted