International Journal of Multidisciplinary Research and Publications
ISSN (Online): 2581-6187

Strengthening U.S. Data Privacy Policies

Xuan Huong Ngo[1], Beverly Grace Clapano Oblina[2]
[1]Student, Vinschool Central Park, Ho Chi Minh City, Vietnam, 700000
[2]AP Seminar, Academic Writing, & ESL Teacher, ESL Standard Department, Vinschool Central Park, Ho Chi Minh City, Vietnam, 700000
Email address: beverlygrace90210@gmail.com

Abstract*—Amidst growing public concern and frequent data breaches, research highlights the inadequacy of the current U.S. data protection framework, characterized by a fragmented legal landscape and reliance on often ineffective consent-based approaches. Analyzing federal law, tech company practices, and user behavior, this paper argues that the absence of a unified federal privacy law, coupled with manipulative design of consent interfaces and user misunderstanding, undermines meaningful data privacy. Specifically, the analysis reveals how sector-specific regulations create inconsistencies, tech companies exploit loopholes in consent mechanisms leading to invasive tracking, and users are frequently overwhelmed or misinformed by privacy policies. Enhancing data privacy requires comprehensive reforms, including the implementation of a baseline federal privacy law, greater corporate accountability in consent practices, improved transparency of data handling, and enhanced user education to foster a more privacy-conscious digital environment in the U.S*.

***Keywords*—** *Cybersecurity, Data Security, Data Privacy Policy, Notice and Consent Framework, U.S. Data Protection Laws*.

I. Introduction

"Most [Americans] believe they have little to no control over what companies (73%) or the government (79%) do with their data." (McClain, Faverio, Anderson, & Park, 2023). This statistic reflects growing public anxiety over data privacy as breaches and misuse of personal information continue to make headlines. The vulnerabilities in the U.S. data protection framework are evident from the Equifax breach in 2017 to Yahoo's admission that billions of accounts were compromised (O'Connor, 2018). The issue of unauthorized data collection, sharing, and usage has become a topic of intense public scrutiny, raising critical questions about the effectiveness of current policies designed to safeguard personal information and secure user consent.

In the U.S., the lack of cohesive federal legislation governing data privacy exacerbates the problem, leaving gaps that tech companies often exploit while users remain largely uninformed or powerless. This paper investigates the effectiveness of U.S. data privacy policies from legal and technological perspectives, focusing on the roles of federal law, tech companies, and users. While some argue that existing sector-specific regulations like HIPAA and FERPA offer sufficient protection, the fragmented and inconsistent nature of these policies suggests otherwise. Current consent-based mechanisms are largely ineffective and comprehensive reforms, technological improvements, and increased public awareness are crucial to enhancing data privacy.

II. Federal Law: Fragmented and Inadequate

The absence of a unified federal data privacy law in the U.S. is one of the primary reasons for systemic weaknesses in protecting user information. Existing regulations, such as the Health Insurance Portability and Accountability Act (HIPAA) and the Family Educational Rights and Privacy Act (FERPA), offer protection only within specific sectors, creating inconsistencies across industries. The Federal Trade Commission (FTC), tasked with enforcing privacy standards, faces significant limitations in its legal authority, often resulting in incomplete enforcement and leaving companies with minimal accountability (O'Connor, 2018).

One of the fundamental issues lies in the traditional approach of relying on notice and consent mechanisms, rooted in the Fair Information Practices (FIPs) established in the 1960s. This framework assumes that users can make informed decisions if provided with clear notices. However, as technology evolves, this premise has become increasingly unrealistic. Modern data collection is complex, involving numerous small data fragments that are often pieced together to create comprehensive user profiles. A study in 2008 revealed that reading privacy policies for all websites visited annually would require an average of 244 hours (Landau, 2015). This impracticality renders the current model ineffective, as users frequently consent without fully understanding the implications.

III. Tech Companies and Website Providers: Exploiting Loopholes

On the technological front, issues arise from the practices of tech companies and website providers. Although consent-based policies are intended to give users control, they often produce unintended consequences that undermine user privacy such as increased data sharing with third parties as demonstrated by Gopal et al. (2023). This happens as smaller websites are driven out of the market due to the costs associated with compliance, leaving only larger, data-rich companies to dominate, reducing user surplus and harming competition. Additionally, web tracking becomes significantly more widespread after users accept consent policies. Jha et al. (2021) report that the number of trackers embedded in websites can increase by as much as four times post-consent, particularly on ad-heavy platforms like news and sports sites. This increase in tracking highlights a critical flaw in the consent process: users may believe they are protecting their privacy through consent, yet they are often subjected to more

Xuan Huong Ngo and Beverly Grace Clapano Oblina, "Strengthening U.S. Data Privacy Policies," *International Journal of Multidisciplinary Research and Publications (IJMRAP)*, Volume 7, Issue 10, pp. 14-16, 2025.

invasive tracking practices.

Moreover, privacy banners frequently prioritize obtaining consent over genuinely informing users about data practices. Fassl, Gröber, & Krombholz (2021) note that this approach often leads to uninformed acceptance of terms, as users may not fully understand what they are agreeing to. The manipulative design of privacy banners significantly impacts user consent rates. Jha et al. (2024) illustrate that a simple "one-click reject-all" option led to over 60% of users denying consent, while requiring more than one click to opt out resulted in about 90% of users granting consent. Some websites' privacy choices were rendered unusable due to missing or unhelpful information, or broken links, as proven by a paper analyzing 150 websites (Habib et al., 2019).

Furthermore, some websites completely disregard user consent decisions, rendering the consent process effectively meaningless. As highlighted by Liu, Iqbal, and Saxena (2024), websites typically incorporate Consent Management Platforms (CMPs) like OneTrust and CookieBot to solicit and convey user consent to embedded advertisers, expecting that this consent will be respected. However, neither the websites nor the regulators have mechanisms in place to audit advertisers' compliance with user consent, raising concerns about accountability in data practices. This lack of oversight is particularly troubling in light of the fact that privacy policies often misrepresent data collection and sharing practices. Okoyomon et al. (2019) reveal alarming statistics, such as the fact that 9.1% of apps directed at children claim they are not for children, while 30.6% assert ignorance regarding whether the data they collect is from minors. Additionally, 10.5% of apps share personal identifiers with third-party service providers without disclosing this in their privacy policies, and only 22.2% explicitly name third parties. Such discrepancies further erode trust in privacy policies and underscore the need for improved transparency and accountability in data practices.

IV. Users: Misunderstanding and Inattention

Users themselves play a crucial role in the data privacy landscape, but their lack of understanding often contributes to the ineffectiveness of consent policies. Many users misinterpret privacy policies, believing them to be more privacy-friendly than they actually are. Research indicates that American users often misinterpret the meaning of privacy policies due to ambiguous wording, causing confusion even among experts (college-level participants) (Reidenberg et al., 2014). This misconception fosters a false sense of security (Turow et al., 2018), leading users to upload more information than intended.

Another significant issue is the annoyance caused by consent banners. Many users accept privacy policies not out of informed decision-making but to eliminate disruptive pop-ups, as proven by Jha et al. (2024); the number is specified to be 69% by Pew Research Center (2023). This behavior, driven by convenience, weakens the effectiveness of consent mechanisms and perpetuates uninformed data sharing. The repetitive nature of these consent prompts further discourages users from carefully evaluating their choices, leading to inattentive acceptance of terms (Landau, 2015).

V. Potential Solutions

The solution lies in implementing a baseline privacy law that harmonizes regulations across sectors, ensuring more uniform protections. The Fair Credit Reporting Act (FCRA) serves as an example, strictly limiting access to credit information only to essential causes like employment and court orders (Landau, 2015). Legislation can refer to pieces evaluating the effectiveness of privacy policies, such as Vail et al. (2008) findings, to identify and address systematic setbacks. Additionally, subsidizing websites to adopt stronger privacy practices could enhance protection without sacrificing user experience (Gopal et al., 2023). Such measures would address inconsistencies and create a more robust legal framework to safeguard user data.

Another solution is to improve Consent Management Platforms (CMPs) – the channels by which users and advertisers exchange data. CMPs are better at implementing user consent than others but no one is able to check whether or not advertisers are following these preferences (Liu, Iqbal, & Saxena, 2024). A framework of auditing that keeps track of bidding activity and detects consent violations would give third-party advertisers more responsibility. And robust enforcement of data protection policies along with open communication can help prevent the misuse of consent mechanisms by tech companies.

Education and awareness campaigns can empower users to make informed decisions, fostering a more privacy-conscious culture. Additionally, technological solutions like Shibboleth, which allows users to access resources without revealing personal information, could provide greater control over data sharing (Landau, 2015). By promoting such tools and enhancing digital literacy, users can become active participants in protecting their privacy.

VI. Conclusion

The ineffectiveness of data privacy policies and consent mechanisms in the U.S. stems from a combination of fragmented federal regulations, exploitative practices by tech companies, and user misunderstanding. Federal law remains inconsistent, tech companies manipulate consent processes for profit, and users often lack the knowledge to protect their data effectively. Addressing these systemic failures requires comprehensive legislative reform, improved corporate accountability, and enhanced public education. By fostering a more informed and privacy-conscious society, the U.S. can move towards a digital environment that respects user autonomy and safeguards personal information.

References

[1]. Fassl, M., Gröber, L., & Krombholz, K. (2021). Stop the consent theater. CHI EA '21: Extended Abstracts of the 2021 CHI Conference on Human Factors in Computing Systems, Article No. 35, 1–7. ACM Digital Library. https://doi.org/10.1145/3411763.3451230

[2]. Gopal, R. D., Hidaji, H., Kutlu, S. N., Patterson, R. A., & Yaraghi, N. (2023) Law, Economics, and Privacy: Implications of Government Policies on Website and Third-Party Information Sharing. Information

Systems Research, 34(4), 1375–1397. https://doi.org/10.1287/isre.2022.1178

[3]. Habib, H., Zou, Y., Jannu, A., Sridhar, N., Swoopes, C., Acquisti, A., Cranor, L.F., Sadeh, N.M., & Schaub, F. (2019). An Empirical Analysis of Data Deletion and Opt-Out Choices on 150 Websites. SOUPS @ USENIX Security Symposium. https://www.usenix.org/conference/soups2019/presentation/habib

[4]. Jha, N., Trevisan, M., Vassio, L., & Mellia, M. (2021). The Internet with Privacy Policies: Measuring The Web Upon Consent. ACM Transactions on the Web (TWEB), 16(3), Article 15, 1–24. https://doi.org/10.1145/3555352

[5]. Jha, N., Trevisan, M., Mellia, M., Fernandez, D., & Irarr, R. (2024). Privacy policies and consent management platforms: Growth and users' interactions over time. arXiv preprint arXiv:2402.18321v2 [cs.CY]. https://doi.org/10.48550/arXiv.2402.18321

[6]. Landau, S.M. (2015). Control use of data to protect privacy. Science, 347, 504–506. https://www.science.org/doi/10.1126/science.aaa4961

[7]. Liu, Z., Iqbal, U., & Saxena, N. (2024). Opted Out, Yet Tracked: Are Regulations Enough to Protect Your Privacy? https://doi.org/10.56553/popets-2024-0016

[8]. McClain, C., Faverio, M., Anderson, M., & Park, E. (2023). How Americans view data privacy. Pew Research Center. https://www.pewresearch.org/internet/2023/10/18/how-americans-view-data-privacy/

[9]. O'Connor, N. (2018). Reforming the U.S. approach to data protection and privacy. Council on Foreign Relations. https://www.cfr.org/report/reforming-us-approach-data-protection

[10]. Okoyomon, E., Samarin, N., Wijesekera, P., On, A.E.B., Vallina-Rodriguez, N., Reyes, I., Feal, Á., & Egelman, S. (2019). On the ridiculousness of notice and consent: Contradictions in app privacy policies. IEEE Computer Society's Technical Community on Security and Privacy. https://www.ieee-security.org/TC/SPW2019/ConPro/papers/okoyomon-conpro19.pdf

[11]. Reidenberg, J. R., Breaux, T., Cranor, L. F., French, B., Grannis, A., Graves, J., Liu, F., McDonald, A., Norton, T., Ramanath, R., Russell, N. C., Sadeh, N., & Schaub, F. (2014). Disagreeable Privacy Policies: Mismatches between Meaning and Userss Understanding. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.2418297

[12]. Turow, J., Hennessy, M., & Draper, N. (2018). Persistent misperceptions: Americans' misplaced confidence in privacy policies, 2003–2015. Journal of Broadcasting & Electronic Media, 62(3), 461–478. https://doi.org/10.1080/08838151.2018.1451867

[13]. Vail, M. W., Earp, J. B., & AntÓn, A. I. (2008). An empirical study of consumer perceptions and comprehension of website privacy policies. IEEE Transactions on Engineering Management, 55(3), 442–454. https://doi.org/10.1109/tem.2008.922634