10.48047/jocaaa.2025.34.12.29

Data Privacy Regulations and Their Impact on Information Security: A Technical Analysis

Zubairuddin Mohammed
Independent Researcher, USA

Abstract

The modern digital environment has radically changed how organizations handle personal information, and there is an immediate need to establish robust privacy and security models. Privacy laws such as the General Data Protection Regulation, the California Consumer Privacy Act, the Health Insurance Portability and Accountability Act, and the Personal Information Protection and Electronic Documents Act have established extensive legal requirements that mandate technical data protection across all data processing procedures. These frameworks require the use of encryption protocols, multi-factor authentication systems, role-based access controls, breach detection systems, and the concept of privacy by design that would be ingrained into the system's architecture since the inception of the architecture. Companies are experiencing significant technical problems, such as integration of legacy systems, the complexity of cross-border data transfer, and the ongoing trade between technical rigor and usability. Industry-focused applications within healthcare, retail, financial services, and technology industries indicate that compliance is not only successful in relation to minimum regulatory requirements but also in relation to strategic differentiation of privacy promises. Health care providers should put up extensive measures to ensure that the electronic health records have up-to-date security, as well as making sure that the systems are available when needed in critical patient care. Financial institutions and retail companies roll out open-source consumer management interfaces and fraud detection systems that provide protection against advanced threats. Privacy-improving technologies are integrated by technology firms, which allow them to control their data and safely delete their accounts. Patterns of enforcement show that there are severe penalties meant to be imposed in the case of violation, and therefore, organizations must make compliance a strategic requirement. But organizations that have mature security programs enjoy quantifiable returns, such as reduced cost of breaches, timely response to incidents, and customer trust in the form of competitive advantages. The intersection of privacy compliance and information security symbolizes a core business need that has promoted organizational resiliency within a more data-centric landscape in which digital trust is the core element of sustainable customer relationships and market differentiation.

Keywords: Data Privacy Regulations, Information Security Compliance, Encryption Protocols, Breach Detection Systems, Privacy-By-Design Architecture

1. Introduction

With the digital revolution, there has been a condition where personal data is transferred across untold networks and systems within a single second. The laws that relate to privacy have become the foundation of the way business should be conducted and have altered the nature of the relationship existing between businesses and the information they are entrusted with. The compliance requirements and security practices have come together at all levels of operation in the organization.

10.48047/jocaaa.2025.34.12.29

The current cyber threats have formed a web of challenges that is difficult to solve. The attackers are continuously improving their skills, and they are exploring the vulnerabilities of every possible point of entry. Recent research shows that enterprises are pouring resources into cybersecurity infrastructure, with technology budgets clearly reflecting how seriously leadership takes these threats [1]. When defenses crumble, the aftermath extends far beyond the initial incident. Financial losses pile up from multiple sources: emergency response costs, fines from regulators, halted operations, and a tarnished reputation that can take years to rebuild [2].

This examination delves into the major privacy frameworks shaping today's business environment, explores their security implications, and presents concrete examples from various industries. This has led to a significant level of regulatory implementation, as government agencies have become more advanced in terms of control systems and imposing fines that attract the interest of executive management. Privacy has ceased to be a mere compliance issue, but a fundamental strategic issue. The change requires the security thinking to permeate all business processes at the grassroots and not be added at the end. The following sections include the different sectors that address these needs as they develop security systems that are strong enough to address the threats in the future.

2. Data Privacy Regulations and Their Technical Requirements

2.1 General Data Protection Regulation (GDPR)

The origin of the then-European-Ultra personalized approach to information began with the unveiling of GDPR, which began in May 2018 and marked the point of departure of the attitude towards personal data by the organizations. This legislation establishes highly rigorous requirements regarding each phase of information processing, including original acquisition to ultimate destruction. The technical mandate calls for security measures matching the actual risks involved, abandoning cookie-cutter approaches in favor of thoughtful risk assessment.

Patterns emerging from enforcement actions paint a clear picture of regulatory priorities. Authorities across Europe have levied substantial fines for a spectrum of violations [3]. Such issues as encryption only on paper, access controls that are too porous to allow unauthorized personnel to regularly access sensitive data, and notices of breaches that take days or weeks to reach required personnel, rather than within the time limit that is already seventy-two hours. Such instances become costly lessons to the rest of the business society.

The framework encourages organisations to invest in privacy protection in their system at its inception instead of attempting to incorporate security later on. This conceptual base would mean that an architect and a developer have to grapple with the issue of data security as they brainstorm in their preliminary brainstorming. Requirements touch all aspects of the data lifecycle: keeping comprehensive documentation of data processing, developing automated software to respond to data access or deletion requests, and developing retention schedules that automatically delete old data.

When doing business across borders, the complexity is further compounded more especially in the transfer of data into and out of international borders. Firms should design advanced architecture that complies with the data residency requirements, and may implement geographically distributed infrastructure, coordinate encryption keys through jurisdiction, and integrate vendor-contractual safeguards in each agreement. The regulation reaches beyond Europe's borders, pulling in any organization that processes EU citizen data, regardless of where the company plants its headquarters.

10.48047/jocaaa.2025.34.12.29

2.2 California Consumer Privacy Act (CCPA) and Healthcare Regulations

California's entry into privacy legislation in January 2020 handed state residents meaningful control over their personal information. Though it shares DNA with GDPR, CCPA brings its own flavor shaped by American business culture. The technical heavy lifting involves building transparent systems that document what data gets collected, how it gets processed, and who receives it, all made accessible through interfaces regular people can actually use [4].

The regulatory guidance has sealed the gaps concerning the definition of what constitutes reasonable security measures. The sensitivity of the data requires the companies to be safeguarded accordingly: the truly sensitive data must be encrypted, the access controls have to be linked with the actual job needs, and the monitoring tools must notify the companies that something is amiss. The law casts a wide net defining personal information, forcing careful system design to track and protect a diverse range of data types.

Healthcare operates in its own regulatory universe under HIPAA, which wraps medical information in specialized protections. The recent statistics of breaches paint a concerning picture as the incidents targeting providers, insurers, and their partners occur with an alarming frequency [5]. Advanced hackers who attack electronic health records, ransomware that takes over key systems, and insiders who access areas they are not required to are also adding to the issue.

Compliance in healthcare requires a three-prong approach to compliance namely, physical infrastructure to protect computer hardware and facilities, technical compliance such as encryption of electronic medical data when sitting in databases or when in transit through the networks, fine-grained access control of who has access to what patient information, exhaustive audit trail whereby all access to a medical record is documented and, lastly, administrative compliance where policy documentation through administrative rules govern all policy-related documents and training of the staff as well as response to incidents. There is a special pressure in the healthcare world since security measures cannot interfere with providing urgent care. This tension requires the security architectures that do not jeopardise the clinical workflow and will not slow down the treatment that could have saved a life.

10.48047/jocaaa.2025.34.12.29

Regulation	Jurisdiction	Primary Technical Requirements	Key Compliance Obligations
General Data Protection Regulation (GDPR)	European Union	Encryption, access controls, breach notification within 72 hours, and automated data retention policies	Data protection by design and default, processing records, cross-border transfer safeguards, and data subject rights automation
California Consumer Privacy Act (CCPA)	California, USA	Data inventory systems, encryption for sensitive data, access management, and security monitoring	Transparency mechanisms, consumer-facing interfaces, opt-out capabilities, automated deletion workflows
Health Insurance Portability and Accountability Act (HIPAA)	United States	Multi-factor authentication, encryption for ePHI, audit logging, and role-based access controls	Physical, technical, and administrative safeguards, breach reporting, and workforce training programs
Personal Information Protection and Electronic Documents Act (PIPEDA)	Canada	Consent management systems, proportionate security safeguards, breach notification mechanisms	Data collection transparency, security measures matching sensitivity, and regulatory breach reporting

Table 1: Major Data Privacy Regulations and Core Requirements [3, 4]

3. Information Security Implementation Requirements

The current privacy laws all create high-tech expectations of security that extend well beyond the creation of online walls. Access control systems establish the base, which is a combination of multi-factor authentication, job-based access, and minimal access control to ensure that only the correct individuals access data that they actually require to do their job. The identity verification of authentication systems needs to be confirmed by a number of independent ways, a combination of things known to people, such as passwords, things possessed by people, such as security tokens or phones, and more and more things known by people, such as fingerprints or face scans.

Job-based access control allows organizations to set specific permissions according to what is actually needed, such that individuals do not stumble into data that is not their duty. This design also slows down attackers during security incidents, preventing stolen credentials from opening every door in the building. Recent studies spotlight serious risks from insiders holding legitimate credentials, whether acting with malicious intent or simply being careless [6]. Monetary loss due to insider cases can be crippling since the

10.48047/jocaaa.2025.34.12.29

granted accessibility is a freeway to stealing information, destroying systems, or accidentally revealing information owing to haphazard treatment. These results drive the point home on why behavioral monitoring is important, with odd patterns detected such as strange access requests, huge data downloads, or even logins at odd times, providing the security team with an opportunity to investigate before damage is actually done.

Encryption requirements apply to data at all locations. Data on the move is secured by the use of protocols such as the Transport Layer Security version 1.3, whereas stationary data requires the use of Advanced Encryption Standard version 256-bit keys or higher standard across databases and file systems, and backup storage. Extensive auditing and tracking systems ensure that all contacts between data are monitored so that abnormal activity can be identified and be able to facilitate investigations following security incidents. Security information and event management platforms pull together logs from firewalls, intrusion detection gear, authentication servers, and applications, running correlation rules and machine learning algorithms to catch threat signatures like repeated login failures, unauthorized privilege grabs, or suspicious data extraction.

Analysis of breach patterns shows that organizations with well-developed security operations catch intrusions much faster than those waiting for someone outside to sound the alarm [7]. Speed of detection directly connects to limiting damage because quick identification enables rapid containment, cutting down how long attackers lurk inside networks and shrinking the volume of stolen data. Breach response requires both the appropriate technology and clear-cut procedures that outline the process of telling the right people the right thing to do in a way that allows fixing the situation right. The regulations on data minimization mandate technical architectures to facilitate automated obligation policies, gathering necessary data, and eliminating documents when their authorized intent concludes, reducing the attack area and simplifying the process of adhering to when an individual requests his or her data to be deleted.

10.48047/jocaaa.2025.34.12.29

Security Component	Implementation Method	Primary Function	Regulatory Alignment
Multi-factor Authentication	Knowledge factors (passwords), possession factors (tokens/mobile devices), biometric factors (fingerprints/facial recognition)	Verify user identity through multiple independent factors, and prevent unauthorized access	GDPR, CCPA, HIPAA, PIPEDA
Role-based Access Control	Job function permissions, least privilege principles, and granular access definitions	Restrict data access to authorized personnel based on legitimate business needs, limit lateral movement	GDPR, HIPAA, PIPEDA
Encryption Standards	TLS 1.3 for data in transit, AES-256 for data at rest	Protect data confidentiality during transmission and storage, render information unreadable without cryptographic keys	GDPR, CCPA, HIPAA, PIPEDA
Audit and Monitoring Systems	SIEM platforms, intrusion detection systems, behavioral analytics, log aggregation, and correlation	Track data access and modifications, detect anomalous activities, and support forensic investigations	GDPR, CCPA, HIPAA, PIPEDA
Breach Detection and Response	Automated threat detection, incident response protocols, forensic capabilities, and notification procedures	Identify security incidents rapidly, contain breaches, limit attacker dwell time, and comply with notification requirements	GDPR, CCPA, HIPAA, PIPAA
Data Minimization and Retention	Automated retention policies, scheduled deletion mechanisms, and data lifecycle management	Collect only necessary information, delete data upon legitimate period expiration, and reduce the attack surface	GDPR, CCPA, PIPEDA

Table 2: Technical Security Implementation Components [5, 6]

4. Industry-Specific Technical Applications

4.1 Healthcare Sector Technical Implementations

Healthcare providers wrestle with distinctive security puzzles given how sensitive medical information is and how critical it is that patient care systems stay running no matter what. Electronic health record platforms need strict controls: multi-factor authentication blocking unwanted visitors, automated audit trails watching every data interaction for accountability and detective work after incidents, and encryption protecting patient details during transmission between facilities and while stored in clinical databases.

10.48047/jocaaa.2025.34.12.29

Recent cybersecurity research covering healthcare reveals troubling gaps in preparedness [8]. Plenty of institutions complain about not having enough security staff to handle their workload, budgets too tight to afford cutting-edge protective technology, and real struggles getting clinical personnel engaged with security awareness programs. Medical professionals naturally put immediate patient needs first over security procedures, creating cultural friction when security teams try to implement protective measures that might slow down workflows.

The healthcare threat picture shows stubborn vulnerabilities despite regulatory requirements. The medical providers are targeted by criminals in particular due to the fact that health records command a high price in black markets, the urgent care patients are usually under stress and thus in urgent need of a ransom, and the infrastructure is often outdated in most facilities, and thus not fitted with the latest security protocols. Successful implementations follow holistic strategies that address both technical controls and the organizational culture concurrently and ensure that clinical staff understand their protective mandate, identify social engineering techniques such as fake emails purportedly sent by colleagues, and follow safe practices when accessing records or sharing confidential information.

High-tech security resources can provide a quantifiable mitigation of risk when implemented in an appropriate manner. Behavioral analytics systems identify unusual authentication patterns, inappropriate access attempts, or unusual data access volumes that may indicate compromised credentials or insider threats. Automated monitoring also allows the security operations center to identify ransomware warning signs such as the rapid encryption of files, the presence of network telemetry that may indicate remote control communication, or privilege escalation, which precedes the release of ransomware. With proper setups and staffing, the early warning systems can quarantine the affected systems, close down the compromised accounts, and lock things down prior to the virus spreading.

Healthcare organizations also face medical device security headaches. Countless connected devices from medication pumps to imaging machines frequently run ancient operating systems, never get security updates from manufacturers, and offer convenient entry points for attackers trying to break into clinical networks. Detailed network segmentation isolates medical device access to administrative systems, so that damaged devices cannot spread as much, and the attackers are not able to use vulnerable medical devices to leap to the electronic health records or other sensitive systems. Effective technical controls combined with thorough employee education and frequent security inspections help providers to maintain information in confidence, integrity, and access within regulatory compliance and their main mandate of providing quality patient care.

4.2 Retail, Financial, and Technology Sector Applications

The challenges encountered by retail organizations in the implementation of privacy regulations, particularly transparency requirements and management of consumer rights, are unique. Technical solutions need customer-facing interfaces enabling data access requests, preference management for opt-out choices, and secure deletion workflows that scrub information across scattered systems, including transaction databases, marketing platforms, customer relationship tools, and backup archives.

Recent research looking at privacy control user experiences shows that interface design makes a huge difference in whether consumers actually exercise their rights [9]. Complicated or buried privacy settings produce dismal engagement, while intuitive, accessible controls encourage active preference management. Retailers are walking a fine line between full privacy functionality and effortless shopping operations due to the fact that too much checkout antagonism or disorganized account maintenance is enough to drive away customers to other companies.

10.48047/jocaaa.2025.34.12.29

Technical implementation involves end-to-end encrypted transactions to ensure data on customer devices, within the banking applications, and with the processing systems, secure access protocols with a high level of authentication that may include biometrics or hardware tokens to facilitate risky transactions, and frequent security tests that may be in the form of penetration exercise and vulnerability scanning to identify vulnerabilities before bad actors can exploit them. Organizations must have extensive fraud detection technologies that examine transaction patterns immediately to identify anomalies that indicate unauthorized access or fraudulent transfer, so that suspicious transactions can be automatically blocked suspicious transactions under additional authentication or investigation.

The technology sector faces distinctive puzzles of privacy implementation due to the overwhelming volume and intricacy of the placement of information in cloud platforms, social networks, and software-as-a-service applications. Privacy-by-design thinking asks the architects to consider the privacy implication when developing a product, as they build features such as fine-grained controls that allow users to manage their data privacy, the inclusion of portability tools that allow users to transfer their information to standard formats in case they want to switch to other services, and deletion processes that ensure that all production systems, analytics services, and backups collections destroy all the information when a user closes their account. These implementations have to scale to enormous volume, crunching through millions of privacy requests and maintaining the quality of system performance and customer experience at par with the bloodthroat markets where privacy practices are becoming a dominant consumer decision factor and brand loyalty factor.

10.48047/jocaaa.2025.34.12.29

Industry Sector	Primary Regulations	Core Technical Implementations	Specific Challenges	Demonstrated Benefits
Healthcare	HIPAA	EHR systems with multi-factor authentication, automated audit trails, encryption for ePHI, and network segmentation for medical devices	Aging infrastructure, balancing security with clinical workflow continuity, medical device vulnerabilities, and ransomware targeting	Reduced breach frequency, protected patient information, and maintained system availability for care delivery
Retail	CCPA	Customer data portals, preference management systems, secure deletion workflows, automated privacy request processing	Cross-system data purging, balancing privacy controls with shopping experience, and high-volume request handling	Enhanced customer trust, improved satisfaction scores, and competitive differentiation through privacy commitments
Financial Services	GDPR, CCPA	End-to-end transaction encryption, fraud detection systems, penetration testing, vulnerability scanning, risk-based authentication	Account takeover threats, payment fraud, real-time anomaly detection requirements, and cross-border transfer complexity	Reduced fraud incidents, enhanced customer confidence, regulatory compliance, and operational efficiency improvements
Technology	GDPR, PIPEDA	Privacy-by-design architectures, granular privacy controls, data portability mechanisms, and account deletion workflows at scale	Massive scale processing requirements, cross-jurisdictional compliance, and balancing personalization with privacy	Increased user engagement, enhanced brand reputation, and competitive advantage in privacy-conscious markets

Table 3: Industry-Specific Technical Applications and Challenges [7, 8]

5. Technical Challenges and Best Practices

The compliance of privacy regulations presents significant technical challenges that extend far beyond the mere implementation of new technology, that organizations to change, as the old infrastructure is a headache, and security versus operating efficiency as a tradeoff that will persist. Integration of legacy systems is the most prevalent problem; there are thousands of active firms with important applications created decades ago that have not been revised in regard to security. Those dinosaur systems are unable to generate detailed audit trails recording access and modifications, cannot offer fine-grained access controls suited to give job-specific permissions, and often store information in forms undecipherable utilizing present encryption systems.

10.48047/jocaaa.2025.34.12.29

Organizations must deploy compensating controls like database activity monitoring, capturing queries and transactions when applications can't natively log activities, encryption proxies protecting data traveling to and from legacy applications, and wrapper applications tacking authentication and authorization layers onto older systems. However, compensating controls bring complexity, potential performance hits, and maintenance overhead, demanding careful management. Projects of system modernization provide long-term solutions with the replacement of old applications by modern ones created on a secure platform and designed with security in mind at the initial stage, but these projects require colossal investments, careful planning that does not disrupt business, and gradual migration strategies that would stepwise move data and functionality but leave business operations running.

Another significant technical challenge that is raised by cross-border data transfers is encountered by multinational organizations operating in jurisdictions with incompatible or conflicting regulatory requirements. The technical solutions should address the data localization requirements that require some sets of information to remain within a defined geographic region, and therefore, the distributed architecture will need regional data centers that operate and store information that is subject to localization requirements. Organizations build data residency architectures chopping up customer information based on citizenship or residence, steering processing activities to compliant infrastructure while keeping global service delivery capabilities intact.

Encryption and tokenization tricks enable some data flows across borders by scrambling information so it's unreadable without cryptographic keys staying within authorized jurisdictions, though regulatory interpretations of whether encrypted data counts as a transfer vary wildly across jurisdictions. Compliance solution scalability is a challenge that continues to grow with the size of the organization because security architectures must manage the increased volumes of data, larger counts of users, and changing business processes without compromising compliance postures. Security solutions built on the cloud and automation platforms provide scalable compliance through providing elastic infrastructure elastic to demand, ongoing compliance checks performed automatically as configurations are observed against policy requirements, and the ability to orchestrate the implementation of consistent security controls across sprawling environments.

Companies also have to balance security needs and usability needs as undue friction irritates legitimate users, slows down production, and even invites workarounds, which are likely to open security holes. Risk-based authentication policies are strategies that look at contextual indicators such as location of the user, device fingerprints, network reputation, and transaction risks to implement an appropriate authentication rigor, with little additional verification required in the case of low-risk conditions and additional authentication required in the case of high-risk behaviors. The winning practices to successful implementation are the running of regular security checks that identify vulnerabilities prior to exploitation, implementation of automated compliance monitoring that provides real time visibility of security postures, development of comprehensive data governance frameworks that detail clear policies and procedures, and the rollout of privacy-enhancing technologies that make it possible to perform calculations on encrypted data, maintaining a sharp incident response capability, and investing resources in ongoing employee education programs that develop security awareness and ensure workforce understand privacy obligations and individual accountability in safeguarding organizational and customer information.

10.48047/jocaaa.2025.34.12.29

Challenge Category	Specific Issues	Compensating Controls	Long-term Solutions	Expected Outcomes
Legacy System Integration	Outdated operating systems, incompatible encryption formats, a lack of audit logging, and insufficient access controls	Database activity monitoring, encryption proxies, wrapper applications, and adding authentication layers	Phased system modernization, replacement with contemporary platforms incorporating security by design	Reduced technical debt, improved compliance posture, enhanced security capabilities
Cross-border Data Transfers	Data localization requirements, conflicting jurisdictional mandates, and adequacy determinations	Regional data centers, data residency architectures, encryption, and tokenization for international flows	Distributed processing architectures, jurisdiction-specific key management, contractual safeguards	Compliant global operations, maintained service delivery, and avoided regulatory penalties
Scalability of Compliance	Growing data volumes, expanding user populations, evolving business processes	Cloud-native security solutions, automated compliance verification, and orchestration platforms	Elastic infrastructure, continuous configuration monitoring, consistent control deployment	Maintained compliance during growth, reduced verification time, and efficient resource utilization
Security vs. Usability Balance	User friction, productivity impacts, workaround behaviors, and creating risks	Risk-based authentication, contextual security controls, and adaptive authentication rigor	User experience optimization, behavioral analytics, and intelligent authentication systems	Reduced user frustration, maintained security effectiveness, minimized support overhead
General Best Practices	Vulnerability identification, compliance drift, policy enforcement gaps	Regular security assessments, automated monitoring tools, and comprehensive data governance	Privacy-enhancing technologies, tested incident response, and continuous workforce training	Proactive threat detection, real-time compliance visibility, and reduced security incidents

Table 4: Technical Challenges and Implementation Best Practices [9, 10]

10.48047/jocaaa.2025.34.12.29

Conclusion

The development of privacy laws has essentially reshaped the definition of information security as a business strategic requirement, not as a supporting compliance role. The General Data Protection Regulation, California Consumer Privacy Act, Health Insurance Portability and Accountability Act, and Personal Information Protection and Electronic Documents Act all define detailed structures that require complex technical implementations on encryption, access management, breach detection, and privacy-by-design architectures. The patterns of enforcement across jurisdiction reflect dedication to regulation by high penalties for non-conformance and make privacy no longer a benevolence, but a dire business necessity. Nevertheless, organizations that adopt mature security programs have found that the benefits are much more than regulatory compliance, and include lower cost of breaches, faster response to incidents, and increased customer confidence that leads to competitive benefits that are quantifiable. Experts in the industrial application can be seen through the use of healthcare, retail, financial services, and technology industries through the implementation of privacy commitments to strategic applications that distinguish organizations in more privacy-conscious markets. Healthcare organizations that use end-to-end protection and safeguards keep the sensitive data of patients and ensure continuous operation that is vital to the care delivery process. The retail and financial institutions that have invested in open customer controls and fraud mitigation technologies note improved customer contentment and loyalty. Technology firms that implement privacy-enhancing capabilities at the early phases of the product development capture the attention of users who value meaningful data controls over the shrouds. A variety of technical implementation issues, such as limitations of legacy systems, complex cross-border transfers, scalability, and security-usability balancing, need advanced solutions, integrating compensating controls, system modernization, distributed architectures, and risk-based authentication techniques. With regulatory frameworks advancing around the world with the expansion of jurisdictional adoption, fine-tuned enforcement, and new guidance, organizations need to adopt proactive security postures that use flexible technical frameworks, an executive-responsible governance scheme, and a culture of privacy protection as an essential business value. The intersection between privacy compliance and information security forms a fundamental basis for organizational integrity in data-intensive settings in which digital trust forms the cornerstone to sustainable customer relationships, effective business collaborations, and sustainable competitive distinction in markets where privacy practices contribute growingly to consumer behavior and buying choices.

References

[1] PwC, "2023 Global Digital Trust Insights". [Online]. Available: https://www.pwc.in/assets/pdfs/consulting/cyber-security/2023-global-digital-trust-insights-v1.pdf

[2] IBM Security, "Cost of a Data Breach Report 2025". [Online]. Available: https://www.ibm.com/reports/data-breach

[3] Enforcement Tracker, "GDPR Enforcement Tracker". [Online]. Available: https://www.enforcementtracker.com/

[4] OAG, "California Consumer Privacy Act (CCPA)" 2024. [Online]. Available: https://oag.ca.gov/privacy/ccpa

[5] Steve Alder, "Healthcare Data Breach Statistics," HIPAA Journal, 2025. [Online]. Available: https://www.hipaajournal.com/healthcare-data-breach-statistics/

10.48047/jocaaa.2025.34.12.29

[6] Data Patrol, "Insider Threats Cost Companies $17.4M Annually – What You Need to Know," 2025. [Online]. Available: https://datapatrol.com/insider-threats-cost-companies-17-4m-annually/

[7] Philippe Langlois et al., "DBIR 2023 Data Breach Investigations Report 10K 20K 30K About the cover," 2023. [Online]. Available: https://www.researchgate.net/publication/371445421_DBIR_2023_Data_Breach_Investigations_Report_10K_20K_30K_About_the_cover

[8] Healthcare Information and Management Systems Society (HIMSS), "2023 HIMSS Survey: Healthcare Cybersecurity survey", 2024. [Online]. Available: https://www.himss.org/sites/hde/files/media/file/2024/03/01/2023-himss-cybersecurity-survey-x.pdf

[9] Van Hong Tran et al., "Measuring Compliance with the California Consumer Privacy Act Over Space and Time," Proceedings of the CHI Conference on Human Factors in Computing Systems, 2024. [Online]. Available: https://dl.acm.org/doi/fullHtml/10.1145/3613904.3642597

[10] Office of the Privacy Commissioner of Canada, "Protecting and promoting privacy in a digital world". [Online]. Available: https://www.priv.gc.ca/media/5996/annual-report-2022-23.pdf