**Original Research Article**

**An Evaluation of Cybersecurity Frameworks and Privacy Regulations for Companies in the Digital Age: A Legal Approach**

**ABSTRACT**

The increase in cyber threats and attacks challenges personal data protection and other digital assets. It can be translated that the complete discussion of cybersecurity cannot be had without the exposition of data protection as they go hand in hand, this is because what cybersecurity seeks to achieve is the protection of personal data, company digital assets, privileged information, money, network security and other valuables and this is what cyber attackers are after. In this age and with the risks that come with handling so much data, regulations have been put in place to ensure compliance and protection of digital assets. This article presents a legal analysis of prominent cybersecurity Laws and privacy regulations for different sectors and jurisdictions alongside the importance of compliance and the penalty of non-compliance. This research aims to provide companies with an understanding of the different regulations in place to ensure compliance and proffer an opportunity to make informed decisions that will benefit the organization.

**Keywords: Cybersecurity, Privacy, Compliance**

**1. INTRODUCTION**

Data security, also known as information security is a wide web or umbrella embodying different aspects of data protection. It is under this body that we find cybersecurity which is anything security related in the cyber realm. Cybersecurity covers the digital or online space. Due to the sophistication of cyberattacks and the increase in cyber threats, the need to ensure a critical and organized cybersecurity framework cannot be overemphasized. Cybersecurity is the practice of protecting internet connected systems such as hardware, software and data from cyber threats.[1] It ensures that there is confidentiality, availability and integrity of data. This is popularly called “the CIA triad”. The components of the triad are to be enjoyed by the owners of the data, also called data subjects. One of the importance of the cybersecurity framework is that it ensures that data are protected by following the measures and steps needed to prevent unauthorized access and use. It is in this light that the interface between cybersecurity and privacy comes into play.

**2. CYBER SECURITY AND PRIVACY**

Privacy rights encompasses the right to ensure that one's personal information, online information, physical space, correspondence, etc are protected. Just like the distinction between information security and cybersecurity, a similar distinction exists between cybersecurity and privacy. In the event that privacy right covers both online and physical privacy. In this context, we are using privacy in the online space. When there is a data breach, two things that can be identified is the unavailability of active cybersecurity frameworks or insufficiency thereof and breach of individuals data protection and privacy rights. In the early 2000s, Eli Lilly and Company (Lilly) on charges regarding the unauthorized disclosure of sensitive personal information collected from consumers through its Prozac.com website agreed to settle Federal Trade Commission and take appropriate security measures to protect consumers’ privacy.[2] In more recent times, the FHC has treated privacy and cybersecurity as sharing the same boundaries. In the event that if it opens a privacy or consumer fraud investigation, the commission may also look at the respondent's data security practices. For example, in the matter of Movie Pass, Inc., the operation of the Movie Pass subscription service agreed to settled FTC allegations for taking steps to block subscribers from using the service as advertised, while also failing to secure subscribers’ personal data.[3]

Also, if it opens a matter based on a data security problem, it may also examine a company's privacy practices. In the Matter of Cafe Press, the FTC alleges that CafePress failed to implement reasonable security measures to protect sensitive information stored on its network, including plain text social security numbers, inadequately encrypted passwords, and answers to password reset questions. The commission proposed order requires the company to bolster its data security and requires its former owner to pay a half million dollars to compensate small businesses. The FTC is sending payments totaling more than $370,000 to consumers who were harmed by the data security failures of online merchandise platform CafePress.

**2.1 Cybersecurity and Privacy Regulations**

Each country has in place cybersecurity and privacy laws that regulate the protection, monitoring, detection, prevention, mitigation and management of cyber incidents. Some of these laws are sector specific, some apply to public companies, while some are state laws. These laws form the basis of legal regulatory compliance which must be followed by companies. The aim of these laws is to ensure implementation of security measures, which when defaulted comes with penalties. For example, in the United States, all 50 states plus Washington, D.C. and three federal territories have in place data breach notification laws, and the SEC has recently adopted a final rule requiring public companies to report material cybersecurity incidents in a Form 8-K within four business days from the date the incident was determined to be material.[4] This amounts to a legal regulatory framework which must be obeyed by companies that falls within the categories listed.

Cybersecurity in the U.S. does not have a Federal law regulating it. One law that cuts across different industries and locations in the U.S is section 5(a) of the Federal Trade Commission Act which apply to unfair and deceptive practices and the Securities and Exchange Commission (“SEC”) which generally prohibits fraud in connection with securities and that explained why in the Equifax's data breach case of 2017, apart from the lawsuits by local and state governments, the company was still investigated by some federal authorities, including the FBI, the FTC and the CFPB. The Securities and Exchange Commission also conducted an additional insider trading investigation due to the sale of $2 million of Equifax stock by executives after the discovery of the breach. This led to the arrest of former Chief Information Officer, Jun Ying who was found guilty of insider trading and sentenced to four months in jail and former Equifax manager, Sudhakar Reddy Bonthu who was also found guilty of insider trading and sentenced to 8 months of home confinement. [5]

**2.2 Sector-Based Laws**

Some of the sector based laws that regulates cybersecurity include Gramm-Leach-Bliley Act (GLBA).[6] This act is both an information security law and a privacy law. It covers both physical and online measures of protection in the financial institutions. The GLBA is also known as the “Financial Modernized Act of 1999”. It is a federal law that requires that financial institutions explain how they share, handle and protect their customers’ private data. What falls under financial institutions is wide and from interpretation, it includes banks, insurance underwriters and agents, securities brokers and dealers, finance companies, mortgage bankers, travel agents or any institution that engages in activities that are financial in nature or incidental to such financial activities. In Title V, Subtitle A, SEC. 501 of the Act, it is the policy of the congress that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers’ nonpublic personal information. The act requires organizations to “develop, implement, and maintain a comprehensive information security program that is written in one or more readily accessible parts and contains administrative, technical, and physical safeguards that are appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any customer information at issue.” This act emphasizes the need for communication and explanation between financial institutions and their customers on how they intend to handle their personal information and how essential it is for financial institutions to have a written information security plan in place. The act also ensure adherence to pretexting provisions which provides that organizations that fall under the GLBA take steps to detect and prevent unauthorized access. The GLBA is enforced by the Federal Trade Commission, the Federal Banking Agencies, State Insurance Oversight Agencies and other Federal Regulatory Authorities.

In 2018, the FTC laid some allegations against PayPal concerning its Venmo peer-to-peer payment services. Some of the allegations were that Venmo’s initial privacy notice was not clear and conspicuous, that their privacy policy was not accurate, that Venmo did not require customers to acknowledge receipt of the initial privacy notice; that Venmo misled consumers about their ability to transfer funds to external bank accounts; and that Venmo misrepresented the extent to which consumers could control the privacy of their transactions.[7] FTC subsequently reached a settlement with PayPal prohibiting the company from misrepresentation any material restrictions on the use of its services, the extent of control provided by its privacy settings, and the extent to which it implements or adheres to a certain level of security. Also, PayPal was prohibited from violating the GLBA’s Safeguards and Privacy Rules.[8] Some of the penalties for non-compliance include fines or possible imprisonment which could have business and life implications.

Also, in 2020, the FTC announced a complaint and settlement against Mortgage Solutions FCS in response to negative Yelp reviews that the company publicly posted sensitive personal information, including financial information. The FTC alleges that Mortgage Solutions actions violated the Fair Credit Reporting Act (FCRA), the Gramm Leach Bliley Act (GLBA) and section 5 of the FTC Act. Mortgage Solutions were asked to pay a $120,000 civil penalty for violating the FCRA. According to the complaint on the violation of the GLBA Safeguard Rule, Mortgage Solutions did not have an information security program for the first five years of being in business (2012-2017) and when it finally implemented a plan, the plan made no provision for regularly testing or assessing its own effectiveness. Part of the settlement with FTC was that they must implement a comprehensive data security program.[9]

Another of the relevant sector based law that regulates cybersecurity and privacy is the Health Insurance Portability and Accountability Act (HIPAA). This Act was established as a National Standard for the protection of health information. This law applies to some covered entities which includes: health plans; health care providers; health care clearinghouses. Under these we have health, dental, vision and prescription drug insurers, health maintenance organizations (“HMOs”), medicare, medicaid, providers of health services such as hospital, billing services, repricing companies, community health management information systems.[10]

The HIPAA regulates the use and disclosure of protected health information by the covered entities. “Individually Identifiable Health Information” is information that is a subset of health information including demographic data from an individual, and

1. is created or received by a healthcare provider, health plan, employer, or health care clearinghouse and
2. relates to the past, present, or future physical or mental health or condition of an individual, the provision of health care to an individual, or the past, present, or future payment for the provision of healthcare to an individual, and

(i)that identifies the individual;or

(ii)with respect to which there is a reasonable basis to believe the information can be used to identify the individual.[11]

The law provides for general principles of use and disclosure, as well as the permitted or required use. [12]

Covered entities are expected to meet the following administrative requirement in line with cybersecurity and privacy law under the HIPAA.[13]

1. A covered entity must implement policies and procedures with respect to protected health information that are designed to comply with the standards, implementation specification, or other requirements of this subpart. The policies and procedures must be reasonably designed, taking into account the size and the type of activities that relate to protected health information undertaken by a covered utility, to ensure such compliance.
2. A covered entity must designate a privacy official who is responsible for the development and implementation of the policies and procedures of the entity.
3. A covered entity must have in place appropriate administrative, technical, and physical safeguards to protect the privacy of protected health information.
4. A covered entity must train all members of its workforce on the policies and procedures with respect to protected health information.
5. A covered entity must provide a process for individuals to make complaints concerning the covered entity's policies and procedures.
6. A covered entity must have and apply appropriate sanctions against members of its workforce who fail to comply with the privacy policies and procedures of the covered entity
7. A covered entity may not require individuals to waive their rights under S 160.306 of this subchapter, as a condition of the provision of treatment, payment, enrollment in a health plan, or eligibility for benefits.

In the light of the foregoing, a better exposition of HIPAA's violation would be given using real life cases.

The Anthem data breach is regarded as one of the biggest healthcare data breaches in history after a series of cyber attacks executed by hackers compromised the ePHI (electronic protected health information) of nearly 79 million people in 2015. Anthem settled a consolidated class-action lawsuit for the data breach victims for $115 million in 2018. Additionally, Anthem paid a penalty of $16 million for HIPAA violations paid to the US Department of Health and Human Services (HHS) Office for Civil Rights (OCR). Anthem was also penalized for failing to conduct an enterprise-wide risk analysis, insufficient system monitoring procedures, lack of identification and response to cyber security incidents, and failing to implement the minimum requirements for access controls to protect against cyber attackers from as early as February 2014. Anthem was also forced to pay for substantial corrective actions to clear up any other potential violations of HIPAA Privacy and Security Rules.[14]

Also, South Broward Hospital District, a Florida health system that does business as Memorial Healthcare System, has agreed to settle an alleged violation of the HIPAA Right of Access with the U.S. Department of Health and Human Services’ Office for Civil Rights (OCR).

The HIPAA Privacy Rule gives individuals rights over their health records, including the right to obtain a copy of those records and to only be charged a reasonable cost-based fee. When a HIPAA-regulated entity receives a request, the records must be provided within 30 days, or in limited circumstances, a 30-day extension is possible. OCR received a complaint from a patient on June 23, 2021, who alleged he had submitted a request to Memorial Healthcare System on April 26, 2021, for a copy of specific health records but those records had not been provided.

OCR investigated and found that while the patient had mailed a written request for the records on April 26, 2021, it was not the first time the records had been requested. The patient had requested a copy of an EEG tracing via the Memorial Healthcare System patient portal on December 30, 2020, and then sent a second request for those records via the patient portal on April 25, 2021. The patient also sent a follow-up request for the EEG tracing on May 23, 2021. Memorial Health System provided the patient with a copy of the requested records, but only after OCR had initiated its investigation. The patient received the requested records on September 29, 2021, 9 months after the initial request was made. OCR discovered that Memorial Healthcare System had provided the EEG tracing to the patient on one previous occasion; however, failed to respond to the December 30, 2020, request and the subsequent requests. OCR proposed a civil monetary penalty of $100,000 to resolve an alleged HIPAA Right of Access violation. Memorial Health System contested the findings and requested a hearing before an Administrative Law Judge, and while the matter was docketed before the Civil Remedies Division of the Departmental Appeals Board, OCR and Memorial Healthcare System engaged in settlement negotiations and agreed to settle the alleged violation. Under the terms of the settlement, Memorial Health System has agreed to pay a $60,000 financial penalty to resolve the pending litigation.[15]

Moving forward, another sector based cybersecurity law in the United States is the Defense Federal Acquisition Regulation (DFARS). Clause 252.204-7012 addresses cybersecurity which ensures Safeguarding Covered Defense Information and Cyber Incident Reporting which outlines requirements for contractors handling sensitive defense information, including procedures to detect and report cyber incidents affecting covered defense information. Covered defense information refers to intricate information related to national security that contractors handling defense contracts must protect. These contractors are obligated to promptly report any cyber incidents that impact covered defense information to the government. In the event that they want to subcontract, they must include similar cybersecurity requirements in their subcontracts to ensure a consistent level of protection across the supply chain. Failure to comply may result in debarment.

On August 22, 2024, the U.S. Department of Justice (DOJ) filed a complaint as intervenor in a False Claims Act (FCA) lawsuit filed against Georgia Tech Research Corporation and the Board of Regents of the University System of Georgia (Georgia Tech). The case was originally filed against Georgia Tech under seal in July 2022 by two whistle-blowers, its former associate director of cybersecurity and a former principal information security engineer.The DOJ complaint alleges that Georgia Tech violated cybersecurity standards found in Defense Federal Acquisition Regulation Supplement (DFARS) section 204.7302, and the contract clauses found in DFARS section 252.204-7008, 252.204-7012, 252.204-7019, 252.204-7020 and Federal Acquisition Regulation (FAR) section 52.204-21. This case against Georgia Tech is in its early stages, and it is not clear whether the Government will be able to substantiate its allegations. Nevertheless, this case shows that the Government takes cybersecurity compliance seriously, and that contractors must do the same. [16]

**2.3 State Based Laws**

As it relates to states based privacy and cybersecurity law, one of the strongest laws that can be discussed is the California Consumer Privacy Act (CCPA). The CCPA was further expanded by the California Privacy Rights Act (CPRA). These laws are concerned with how businesses and organizations that operate in California or that handle data of consumers (data subjects) from California handle the data and protect personal information, ensuring measures in line with the law are put in place. In adhering to this law, the data controller or processor has to make account for the past, present and future of data subjects’ rights as there is a retrospective protection period of 12 months. Also, the Act provides a requirement for conducting an enterprise privacy risk assessment which involves an analysis of the organization's recent policies regarding data privacy, consumer protection, and security access controls. This embodies the physical, technical and administrative structure of the organization. This culminates in some of the things required for audit compliance.

On August 24, 2022, California Attorney General (AG) Rob Bonta announced that the office of the Attorney General (OAG) has entered into its first settlement under the California Consumer Protection Act (CCPA). The settlement, reached with Sephora USA, Inc. (a global beauty retailer that sells makeup, skincare, fragrance and more), requires Sephora to pay $1.2 million and comply with several injunctive terms. This is on the allegation that Sephora failed to:

1. disclose to consumers that it was selling their personal information;
2. process user requests to opt out of sale requests via user-enabled global privacy controls;
3. provide a clear and conspicuous “Do Not Sell My Personal Information” link enabling consumers to opt-out of the sale of their personal information; and
4. provide two or more designated methods for submitting requests to opt-out.

In addition to the $1.2million fine imposed on Sephora, the settlement obligated Sephora to:

1. clarify its online disclosures and privacy policy to include an affirmative representation that it sells data;
2. provide mechanisms for consumers to opt out of the sale of personal information;
3. conform its service provider agreements to CCPA's requirements; and
4. provide reports to the OAG relating to its sale of personal information, the status of its service provider relationships, and its efforts to honour Global Privacy Control.

In Canada, one of the important laws that regulate the management, collection, use and disclosure of personal information is the “Personal Information Protection and Electronic Document Act” (PIPEDA). This law is a Federal privacy legislation which applies to private sector organizations across Canada. Federally regulated organizations that conduct business in Canada are also subject to the PIPEDA. The PIPEDA expects organizations to protect the personal information of the customers by taking appropriate security measures. In Schedule 1 of the Act, ten principles also referred to as the fair information principles were explained. They are: accountability; identifying purposes; consent; limiting use; disclosure and retention; accuracy; safeguards; openness; individual access; and challenging compliance.

In June 2014, the complainant sent a letter to a telecommunications company (“the telco”) requesting access to her personal information using an online access to information tool. As part of her request, she asked for any information about disclosures of her personal information, or information about her account or devices, to other parties, including law enforcement and other state agencies.The complainant alleges that the response of a telecommunications company (the “telco”) to her access request is incomplete. Specifically, she alleges that the telco refused to advise her of whether her personal information, or information about her account or devices, had been disclosed to other parties, including law enforcement and other state agencies. Through the Office of the Privacy Commissioner of Canada, it was found that the telco’s response did not meet its obligation under Principle 4.9 of the Act. As recommended by the commission, the telco provided the complainant with a response about the disclosure of her personal information to all other parties. [17]

**3. How to Ensure Cybersecurity and Privacy Compliance.**

 To ensure cybersecurity and privacy compliance, organizations should ensure an in-depth evaluation of regulations and laws that serve as guides to make this possible.

1 The National Institute of Standards and Technology Cybersecurity (NIST CSF) provides guidance for improving important security and cybersecurity risk management. The NIST CSF core structure includes: functions, categories, subcategories, and informative references. While they do not intend to be procedural steps, they act as an operational culture and provide concrete plans for cybersecurity risk. It serves as a checklist of things to ensure to set up a functional structure. Such steps as identifying risk, protecting against risk, detecting anomalies, incident response, incident recovery are some of the angles covered by NIST CSF. It is an excellent beginning for any private sector organization especially in the United States to implement.

2. Employee Training: Employees are very important in the labour aspect of the factors of production. They can contribute to the success or failure of any company. It is important that in organizations that handle individual data, regular trainings should be conducted on cybersecurity awareness, dangers of data theft, misuse and breach, recognition of intending cyber attack, password maintenance, access control and proper data handling procedures amongst other things.

3. Thorough Risk Assessment Plan: In order to know where to tighten up your security, a good risk assessment plan is advised. It helps to find vulnerability and weak points in systems and ensure that security tools are engaged.

4. Identify relevant regulations: Understand which data privacy laws and cybersecurity standards apply to your industry and region, such as GDPR, HIPAA, GLBA, CCPA, etc.

5. Data Privacy Policies: Organizations should state clear data privacy policies outlining how personal information is collected, used, stored, and protected.

6. Employing Cybersecurity Measures: Adequate physical, technical and administrative protection should be put in place. Encryption, pseudonymization, access control management, incident response plan, regular audits, network testing, reviews and other measures to ensure that data is protected from attack.

**4. Conclusion**

This article only scratches the surface of regulatory compliance and all it contains as it relates to ensuring proper and functioning cybersecurity and privacy frameworks in different companies, organizations, sectors and jurisdictions. To ensure compliance the industry and jurisdiction has to be considered to know what applies. Different agencies and commissions continue to enforce compliance as it is within their legal power and capacity to do so. Companies should ensure that they set in place adequate cybersecurity plans, employ and train their employees on the importance of data protection, conduct regular checks on their systems to find any weakness or vulnerability that could be taken advantage of if not properly fixed, conduct audits and abide by the law. Data will continue to be valuable and protection of it will be the difference between scaling in any industry or falling behind and getting penalized.

**References**

1 Sharon Shea and Alexander S. Gillis. What is cybersecurity?[Internet]. London: TechTarget; 2024 [updated 2024 February; cited 2025 March 6th]. Available from: <https://www.techtarget.com/searchsecurity/definition/cybersecurity>

2 Federal Trade Commission. Eli Lilly Settles FTC Charges Concerning Security Breach [Internet]. FTC's Press Releases; 2002 [updated 2002 January 18; cited 2025 March 6th]. Available from:

<https://www.ftc.gov/news-events/news/press-releases/2002/01/eli-lilly-settles-ftc-charges-concerning-security-breach>

3 Federal Trade Commission. MoviePass, Inc., In the Matter of [Internet]. FTC's Cases and Proceedings; 2021 [last updated 2021 October 5; cited 2025 March 6th]. Available from: <https://www.ftc.gov/legal-library/browse/cases-proceedings/192-3000-moviepass-inc-matter>

4 Edward R. McNicholas, Frances E. Faircloth and Ropes & Gray. Cybersecurity Laws and Regulations USA 2025 [Internet]. ICLG; 2024 November 6th [cited 2025 March 7th]. Available from: <https://iclg-com.cdn.ampproject.org/v/s/iclg.com/practice-areas/cybersecurity-laws-and-regulations/usa/amp?amp_gsa=1&amp_js_v=a9&usqp=mq331AQIUAKwASCAAgM%3D#amp_tf=From%20%251%24s&aoh=17411689072650&referrer=https%3A%2F%2Fwww.google.com&ampshare=https%3A%2F%2Ficlg.com%2Fpractice-areas%2Fcybersecurity-laws-and-regulations%2Fusa>

5 Irini K. Miyashiro. Case Study: Equifax Data Breach[Internet]. Kansas City: Seven Pillars Institute; 2021 [updated 2021 April 30; cited 2025 March 5th]. Available from: <https://sevenpillarsinstitute.org/case-study-equifax-data-breach/>

6 Gramm-Leach-Bliley Act Pub. L. No. 106-102, 113 Stat. 1338, codified in relevant part primarily at 15 U.S.C. SS 6801-6809, SS 6821-6827

7 Edward Holman and Kelly Singleton. FTC Announces Settlement with PayPal for Alleged FTC Act and GLBA Violations by Venmo[Internet]. US: Wilson Sonsini; 2018 [updated 2018 March 26; cited 2025 March 8th]. Available from: <https://www.wsgrdataadvisor.com/2018/03/ftc-venmo-paypal-settlement/>

8 In the Matter of PAYPAL, INC., a corporation. FILE NO. 162-3102 before the Federal Trade Commission.

9 Kathleen Benway and Alston & Bird. FTC Announces Settlement with Mortgage Broker for Publishing Personal Information about Consumers[Internet]. JDSUPRA; 2020 [updated 2020 January 15; cited 2025 March 8]. Available from: <https://www.jdsupra.com/legalnews/ftc-announces-settlement-with-mortgage-98917/>

10 United States Department of Health and Human Services. OCR Privacy Brief: Summary of HIPAA Privacy Rule[Internet]. U.S. HHS; 2002 [updated 2002 August 14; cited 2025 March 10].

11 45 CFR S 160.103

12 45 CFR S 164.502

13 45 CFR S 164.530

14 Kyle Chin. Top 20 Worst HIPAA Violation Cases in History[Internet]. UpGuard; 2025 [updated 2025 January 2nd; cited 2025 March 10th]. Available from: <https://www.upguard.com/blog/worst-hipaa-violation-cases>

15 Steve Alder. Memorial Healthcare System Settles Alleged HIPAA Right of Access Violation [Internet]. The HIPAA Journal; 2025 [updated 2025 January 15; cited 2025 March 10th]. Available from: <https://www.hipaajournal.com/memorial-healthcare-system-hipaa-settlement/>

16 Meghan D. Doherty, Matt Carter, Aaron S. Ralph and Toghrul Shukurlu. U.S. Government Intervenes in Georgia Tech Cybersecurity False Claims Case[Internet]. Pillsbury; 2024 [updated 2024 September 6; cited 2025 March 10th]. Available from: <https://www.pillsburylaw.com/en/news-and-insights/us-government-georgia-tech-cybersecurity-false-claims-case.html>

17 Office of the Privacy Commissioner of Canada. Investigation into a telecommunications company’s response to an individual’s request for access to information about disclosures of her personal information to other parties [Internet]. OPC; 2016 [updated 2016 July 14; cited 2025 March 10th]. Available from: <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2016/pipeda-2016-008/>