Journal of Cybersecurity Education, Research and Practice

Volume 2023 | Number 2 Article 3

2023

Privacy Harm and Non-Compliance from a Legal Perspective

Suvineetha Herath
Dakota State University, sherath@sandburg.edu

Haywood Gelman
Dakota State University, haywood.gelman@trojans.dsu.edu

Lisa McKee
Dakota State University, lisa.mckee@trojans.dsu.edu

Privacy Harm and Non-Compliance from a Legal Perspective

Abstract

In today's data-sharing paradigm, personal data has become a valuable resource that intensifies the risk of unauthorized access and data breach. Increased data mining techniques used to analyze big data have posed significant risks to data security and privacy. Consequently, data breaches are a significant threat to individual privacy. Privacy is a multifaceted concept covering many areas, including the right to access, erasure, and rectify personal data. This paper explores the legal aspects of privacy harm and how they transform into legal action. Privacy harm is the negative impact to an individual as a result of the unauthorized release, gathering, distillation, or expropriation of personal information. Privacy Enhancing Technologies (PETs) emerged as a solution to address data privacy issues and minimize the risk of privacy harm. It is essential to implement privacy enhancement mechanisms to protect Personally Identifiable Information (PII) from unlawful use or access. FIPPs (Fair Information Practice Principles), based on the 1973 Code of Fair Information Practice (CFIP), and the Organization for Economic Cooperation and Development (OECD), are a collection of widely accepted, influential US codes that agencies use when evaluating information systems, processes, programs, and activities affecting individual privacy. Regulatory compliance places a responsibility on organizations to follow best practices to ensure the protection of individual data privacy rights. This paper will focus on FIPPs, relevance to US state privacy laws, their influence on OECD, and reference to the EU General Data Processing Regulation. (GDPR).

Keywords —Privacy harm, Privacy Enhancing Technologies(PETs),Fair Information Practice Principles (FIPPs)

Keywords

privacy harm, Privacy Enhancing Technologies (PETs), Fair Information Practices (FIPS)

Cover Page Footnote

Privacy Harm and Non-Compliance from a Legal Perspective

1st Suvineetha Herath
Beacom College of Computer and Cyber Sciences
Dakota State University
Madison, USA
0009-0002-1262-7823

2nd Haywood Gelman
Beacom College of Computer and Cyber Sciences
Dakota State University
Madison, USA
0009-0009-7208-1624

3rd Lisa McKee
Beacom College of Computer and Cyber Sciences
Dakota State University
Madison, USA
0009-0008-1320-3815

***Abstract*— In today's data-sharing paradigm, personal data has become a valuable resource that intensifies the risk of unauthorized access and data breach. Increased data mining techniques used to analyze big data have posed significant risks to data security and privacy. Consequently, data breaches are a significant threat to individual privacy. Privacy is a multifaceted concept covering many areas, including the right to access, erasure, and rectify personal data. This paper explores the legal aspects of privacy harm and how they transform into legal action. Privacy harm is the negative impact on an individual as a result of the unauthorized release, gathering, distillation, or expropriation of personal information. Privacy Enhancing Technologies (PETs) emerged as a solution to address data privacy issues and minimize the risk of privacy harm. It is essential to implement privacy enhancement mechanisms to protect Personally Identifiable Information (PII) from unlawful use or access. FIPPs (Fair Information Practice Principles), based on the 1973 Code of Fair Information Practice (CFIP), and the Organization for Economic Cooperation and Development (OECD), are a compendium of broadly accepted US codes applied to the assessment of technology programs, applications, and solutions impacting data privacy. Regulatory compliance places a responsibility on organizations to follow best practices to ensure the protection of individual data privacy rights. This paper will focus on FIPPs, relevance to US state privacy laws, their influence on OECD, and reference to the EU General Data Processing Regulation (GDPR).**

Keywords— Privacy harm, Privacy Enhancing Technologies (PETs), Fair Information Practice Principles (FIPPs)

I. INTRODUCTION

The increased adoption of information and communication tools in our daily lives has created opportunities for privacy breaches more than ever before. We leave our digital footprints in cyberspace in many ways without considering the possible risks. The number of Internet crime complaints received by the Internet Crime Complaint Center (IC3) between 2017 and 2021 was 2.76 million [1]. Internet and cybercrime complaints were reported by victimized individuals and organizations as a reported $18.7B US loss [1]. According to the Proxenus Breach Barometer of 2023, 50,406,838 patient health records were compromised in 2022 [2]. Personally Identifiable Information (PII) is defined as "any attributes of a person, such as their hair color, the sound of their voice, height, name, qualifications, past actions, reputation, and medical records" [3]. A wide range of personal data can be used to uniquely identify an individual, including, but not limited to, name, social security number, date, and place of birth [4]. The provided definitions indicate that any characteristic of individuals that reasonably distinguishes one person from all others is considered PII. PII has emerged as a valuable commodity for cybercriminals [5].

In response to concerns over data privacy, various administrative, technical, and legal approaches have been developed over the years. Administrative solutions include policies, procedures, standards, and guidelines to protect personal information. Technological measures provide the methods needed to enforce these policies. "This protection is implemented by multiple measures that include policies, education, training and awareness, and technology" [6]. Security and Privacy compliance ensures that organizations meet legal, regulatory, and industry requirements such as the (GDPR) [7], the Privacy Act of 1974 [8], the California Privacy Rights Act (CPRA) [9], the Colorado Privacy Act (CPA) [10], the Virginia Consumer Data Protection Act (VCDPA) [11] and the Utah Consumer Privacy Act (UCPA) [12] for protecting sensitive data and maintaining data privacy. Due diligence is an integral part of security and privacy compliance. Fair Information Practice Principles (FIPPs) guide organizations to follow required best practices to meet privacy compliance. The context of FIPPs has evolved based on developments in data processing technologies. In 1980, the Organization for Economic Cooperation and Development (OECD) established a framework for protecting privacy and cross-border data based on FIPPs [13]. When data breaches bypass existing security measures, the next step is for the affected parties to seek judicial redress. While legal frameworks have been formed to protect privacy rights, failing to evaluate the gravity of harm in a data breach can adversely affect victims and society. The Standing Doctrine in privacy litigation requires demonstrating that the plaintiff has suffered concrete harm from the defendant's actions [14], [15]. Establishing actual harm has been an enormous challenge for parties seeking justice in privacy litigations [16]. Enforcement of the doctrine depends on the context of the harm. Recognized legal frameworks require adaptability to address the unique challenges of cybersecurity, and new laws and regulations are needed to ensure adequate protection in the digital era [17]. Despite the growing global and national effort to protect individual privacy, quantifying the harm caused by

privacy infringement remains a challenge. As privacy breaches rapidly arise, defining the privacy context in every situation is complex. Numerous studies [15], [16], [17], [18], [19] defined the context of privacy violations in the face of evolving data privacy breaches. However, there is still a gap in research that provides a broad overview of privacy harm, how courts interpret the privacy context, and how to comply with regulatory obligations by mapping FIPPs and OECD to data processing practices. As privacy breaches occur in many ways, a multidisciplinary approach is needed to expand the well-known legal boundaries and overcome these challenges. This paper addresses the concern by combining legal and technological concepts relevant to privacy harm and answering the following research questions:

1) How has the context of privacy harm changed over time?
2) How can existing legal frameworks effectively address emerging data breaches?
3) What are the most efficient ways to use technology to enhance privacy?

This paper aims to inform the public and policymakers about the nature of privacy harm and promote best practices for reducing privacy risks. It also seeks to assist policymakers in understanding regulatory compliance, legal precedents, and implementing Fair Information Practice Principles (FIPPs) to encourage the adoption of effective privacy risk mitigation strategies. The paper employed a meta-analysis approach to review pertinent studies on privacy rights, data breaches, court rulings, privacy laws, FIPPs, and OECD implementation. A review of sources was conducted using literature from the ACM Digital Library, IEEE Xplore, EBSCO, LexisNexis, and other resources. Several significant areas were covered in this study, including the regulatory landscape related to data privacy and the implementation of FIPPs/OECD to promote best practices in data processing. The remaining structure of the paper is as follows: Section II examines the evolution of privacy harm from a historical perspective. Section III analyzes the legal implications and examines the effectiveness of the existing legal framework in addressing privacy harm. Section IV of the article discusses enhancing privacy through FIPPs. Section V specifically addresses the mapping of FIPPs to privacy program objectives, and the final remarks are provided in Section VI.

II. Examining the Evolution of Privacy Harm

A. Historical Perspective of Privacy

The concept of privacy has broadened dramatically over time from its origins. The right to privacy has been shaped by a multidisciplinary approach, such as legal, philosophical, social, economic, and technical, as a solution to address the increasing rate of privacy violations caused by technological advancements. The evolution of privacy in the US can be traced back to the First, Third, Fourth, Fifth, and Ninth Amendments to the US Constitution to protect freedom of expression and individual rights against unreasonable searches and seizures by the Government [20]. Although the United States Constitution does not explicitly focus on protecting personal information, safeguarding individuals from unsolicited invasions was integrated into its jurisprudence by penumbras [21]. The groundwork for recognizing US privacy rights was advanced by "The Right to Privacy," a seminal article by Samuel D. Warren II and Louis Brandeis in 1890 [22]. The authors defined privacy rights as the "right to be let alone," referencing Judge Thomas Cooley in 1888 [23]. An early example of privacy harm litigation is the 1902 case Roberson v. Rochester Folding Box Co., 171 NY 538 (NY 1902) [24]. In this case, Franklin Mills Co. Printed 25,000 flyers with photographs and information about the plaintiff without their permission to be included in advertisements. The applicant alleged that the distribution and display of the brochures with her image in public places adversely affected her reputation, physical, and mental state [24]. The Supreme Court rejected the plaintiff's claim because the precedent had not been established, and the concept of the "right to be let alone" [22] was not a recognized doctrine in jurisprudence at the time. New York State legislators identified gaps in legislation and passed a landmark law in 1903 prohibiting the use of personal images for advertising without the consent of the individual [25]. The 1903 law made New York the first state to recognize privacy rights. The 1905 case of Pavesich v. New England Life Ins. Co., 122 Ga. 190, 50 SE 68 (1905) [26], was a similar case where the Supreme Court of Georgia ruled that publishing an image of someone for advertising without consent breached their right to privacy [26]. As early court opinions ruled, physical or tangible harm is a determining factor in litigation regarding protecting personal information. In another landmark case in 1965, Griswold v. Connecticut, 381 US 479, 85 S. Ct. 1678 [27] the US Supreme Court held that the right to privacy was recognized by penumbras under the Bill of Rights and the US Constitution [21].

B. Technological Advances and Privacy in the 1960s

Privacy torts offer legal recourse for privacy rights violations. Torts are defined by Cornell Law School as "an act or omission that gives rise to injury or harm to another and amounts to a civil wrong for which courts impose liability" [28]. Prosser presented a unique perspective on tort law in 1960 by identifying four distinct types of privacy torts, including" intrusion upon physical solitude, public disclosure of private facts, false light in the public eye, and appropriation of name or likeness for commercial purposes" [29]. Alan Westin's Privacy and Freedom article in 1967 used a multidisciplinary approach to define the notation of privacy harm [18]. Westin investigated the dimensions of privacy violations under three main categories, including "physical, informational, and decisional privacy." The author argued individuals should have the autonomy to be free from unwanted physical invasions, control the amount of personal information shared, know how it is shared and who has access to it. Westin defines privacy as the autonomy of individuals to make decisions, engage in activities and control personal information without being subject to unwanted observation, scrutiny, or influence [18]. The new technical perspective in the context of privacy harm had a significant impact on future privacy litigation. In Katz v. United States, 389 US 347 (1969), the United States Supreme Court ruled that the Government's eavesdropping activities violated privacy [30]. It also violated the context of search and seizure under the Fourth Amendment and established individuals rights to the reasonable expectation of privacy expectation of privacy [30]. The Kartz decision was in contrast to Olmstead v. United

States, 277 US 438 (1928) [31]. By comparison, Olmstead determined that a wiretapped phone conversation of the defendant was not a Fourth Amendment violation because no physical invasion of property was made to install wire trapping equipment. Changes in technology, and the ubiquity of telephones in private residences, led to the change of the Court opinion in Olmstead, 1928. The increased adoption of computers and concerns over personal data ingested by organizations, the focus on PII surfaced in the early 1970s. A 1977 report by the Privacy Protection Study Commission titled "Personal Privacy in an Information Society" discussed the impact of record keeping on individual privacy on individual privacy [32]. In 1971, Browne [33] emphasized protecting personal data from accidental or unauthorized disclosure

C. . Impact of Privacy Harm on PII

Through the 1990s and 2000s, privacy research became increasingly focused on "fair and legitimate processing of personal information" [34]. Privacy harm occurs if automatically processed data generates distorted information about an individual [35]. In Spokeo, Inc. v. Robins - 136 S. Ct. 1540 (2016), the United States Supreme Court addressed whether a plaintiff had standing to sue the defendant's personal information broker under the Fair Credit Reporting Act (FCRA) the defendant disseminated inaccurate information about the plaintiff [36]. The case addressed a situation where the Court examined a privacy breach that resulted in an auto-generated process.

D. Privacy Harm in the Digital Age

According to Calo [19], privacy harm can be divided into two related categories: "subjective and objective." The subjective category of privacy violation refers to a person's perception of being observed without consent, which can lead to unwanted observation subjective privacy harm is "the feeling of being observed without consent, such as in government surveillance or wiretapping, use, and dissemination of PII (which) can cause negative mental states like anxiety, embarrassment, and fear. [19].This is also referred to as the "perception of unwanted observation[19]. Calo continues, "Objective privacy harm is the unanticipated or coerced use of information concerning a person against that person"[19]. Simply stated, objective privacy harm is using PII without consent from the individual, which leads to personal damages. The case of Carpenter v. United States - 138 S. Ct. 2206 (2018) [37] is one of the recent precedent-setting cases influenced by new research on privacy harm. The Supreme Court overturned the Court of Appeals for the Sixth Circuit, adjudicating that individuals have a reasonable expectation of privacy in the digital age [37]. Justices also ruled that the Government must obtain a warrant to access historical cell site location information on a suspect accused in the commission of a robbery [37]. Solove [38] argued that the accepted legal perspective of privacy harm was inadequate to protect individuals from complex privacy invasions and introduced a new taxonomy to assess privacy harm. The new taxonomy includes 16 categories of privacy harm. These categories encompass a wide range of aspects, such as physical harm, economic harm, reputational harm, psychological harm, emotional harm, disturbance, autonomy harm, discrimination harm, and harm to relationships [38]. This description provides a holistic perspective to deliberate what constitutes privacy harm. The research established the contributions of legal scholars to the alignment of harm elements, which addressed the complex nature of factors behind privacy harm. According to Solove, [38], harm acts as a gatekeeper in privacy litigation, but many cases are not remedied based on the element of harm [38]. Courts must take a broad view of privacy damages beyond tangible or financial harm when determining privacy litigation. Furthermore, the research identifies that the modern perspective of privacy harm is closely linked to personal identification and privacy rights [38], [39]. The concept of privacy has evolved to protect personal information from unauthorized disclosure, as shown in Figure 1.

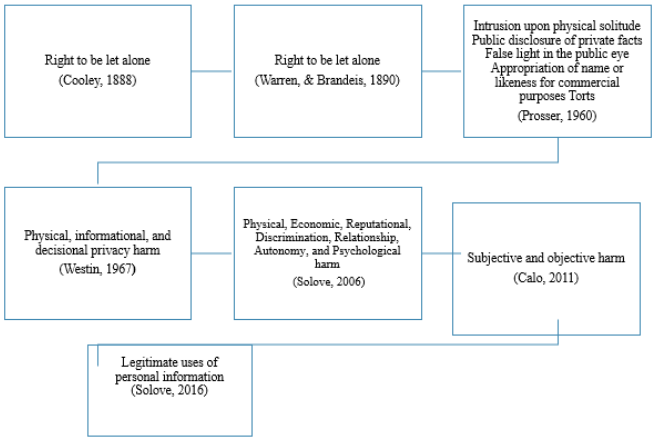

Fig. 1. Evolution of Privacy Harm

III. LEGAL CONSEQUENCES OF PRIVACY INFRINGEMENT

The legal consequences of privacy harm have extended beyond the violation of the "right to be let alone" [22] to the protection of personal information from unauthorized access and disclosure. As stated previously, tort law is a branch of civil law that deals with damages or prejudices caused by one party to another. It places legal obligations and responsibilities on individuals and organizations to act in a way that does not cause harm to others. Contract law enforces legal commitments and obligations on individuals and organizations to fulfill contractual agreements. In 2018 Cambridge Analytica, a UK based political consulting firm, improperly used information of Facebook users to build voter profiles with the goal of influencing voters during the 2016 United States presidential election and the British' Brexit' vote to leave the European Union [40], [41]. In March 2017, The Guardian and The New York Times newspapers reported that "Cambridge Analytica harvested 50 million Facebook user profiles" [40], [41]. A Facebook press release corrected the claim and stated the number of American user profiles harvested by the company increased to" over 87 million" [42]. The scandal exposed the dark side of social networks, plus it raised implications and threats regarding the security, privacy, and integrity of PII. The aftermath of the breach sparked worldwide concern over privacy violations, with the adoption of data regulation policies soon to follow [43]. The EU General Data Protection Regulation (GDPR) began enforcement in May 2018, followed by countries

outside of EU control to update weak policies and implement privacy regulations [44]. Facebook was fined £500,000 in 2019 by the United Kingdom Information Commissioner's Office (ICO) under the U.K. Data Protection Act of 2018 and settled the fine [45]. In 2019, Federal Trade Commission (FTC) levied a $5B US fine on Facebook for deceptive privacy control practices and required additional oversight. This included the hiring of a Privacy Officer, implementation of a comprehensive Information Security Plan, and Privacy Impact Assessments for new and existing applications [45]. As a result, global and national standards have established strict requirements for organizations handling PII. As stated previously, regulatory compliance place a responsibility on organizations to follow best practices to ensure the protection of individual data privacy rights. Meta (formerly Facebook) agreed to pay $725 million to settle a class-action lawsuit in December 2022 related to the Cambridge Analytica case [46**].**

According to GDPR, noncompliance exposes responsible parties to an increased risk of litigation, financial loss, and reputational damage [7]. The CPRA, which is modeled after GDPR, protects the consumer as a natural person who is a California resident [8]. Similar to CPRA, the VCDPA protects the consumer as a natural person who is a Virginia resident, while CPA refers to residents of Colorado [47]. Table 1 shows a high-level comparison of GDPR and US privacy laws.

TABLE I. Comparison of GDPR and US State Data Privacy Laws

Criteria	GDPR	CPRA	VCDPA	CPA
Data Subject	Natural person in the EU	Natural Person CA resident	Natural person VA resident	Natural Person CO resident
Types	Personal data	Personal data	Personal data	Personal data
Coverage	All businesses that gather personal data from EU citizens, regardless of size, Extraterritorial application	Businesses outside of California if they collect or sell the PII of CA residents	Businesses in Virginia or market their goods and services to VA residents	Businesses that process the personal data of Colorado residents or target them with goods or services
FIPPs	Lawfulness, fairness, and transparency Purpose Limitation Data Minimization Accuracy Storage Limitation and Integrity	Accountability Monitoring Transparency	Transparency Purpose Limitation Data Minimization Data quality Data Quality Security Accountability	Transparency Purpose Limitation Data Minimization Data Quality Security Accountability

Note: Data for the table adapted from State level comparison charts of data privacy laws [47]

Data privacy and compliance laws have placed a regulatory burden on data privacy teams to ensure that information collection, processing, and disclosure is managed according to privacy regulations and consumer protection laws [47]. The objectives of data protection legislation are grounded in the principles of fair information practices and FIPPs to ensure that parties that process personal data are responsible for privacy. While there are legislative remedies, the ambiguous interpretation of the invasion of privacy when deciding how a particular statute applies to a violation poses challenges to the right to privacy. In the case of TransUnion LLC v. Ramirez - 141 S. Ct. 2190 (2021), the Court ruled that to have Constitutional standing to sue in Federal court, a plaintiff must have a "tangible" loss or "injury" [48]. In Spokeo, Inc. v Robins, the Supreme Court opined that the company did not comply with the requirements of the Fair Credit Reporting Act (FCRA) [36]. Carlo [19] noted that courts might sometimes misdiagnose harm, offering simple remedies that only address the surface level aspects of the problem rather than tackling the underlying issues. Wachter and Mittelstadt established a close link between personal identification and data protection in the modern data protection construct [49]. The underlying objectives of data protection legislation are historically grounded in FIPPs, and later, OECD principles to ensure that parties that process personal data are responsible for protecting privacy. Regardless of the jurisdiction or legal framework, adherence to FIPPs is essential to safeguard an individual's PII and privacy rights.

IV. ENHANCING PRIVACY THROUGH FAIR INFORMATION PRACTICE PRINCIPLES (FIPPs)

The common model for information security, including confidentiality, integrity, and availability (CIA triad), is the primary framework used to guide the development and implementation of information security practices. It is not sufficient to meet legal, regulatory, and contractual obligations for privacy. Threats to the confidentiality, integrity, and availability of information have evolved into a vast collection of events, including but not limited to accidental or intentional damage, destruction, theft, unintended modification, unauthorized access, or another misuse from human or nonhuman threats. [6]. Confidentiality ensures that only authorized individuals or entities obtain access to information. However, if authorized individuals access or misuse PII inappropriately, it will breach the confidentiality of personal information, which can lead to a loss of privacy. As a result, data integrity can also be compromised. FIPPs provide a framework to guide organizations in implementing best practices to safeguard the privacy of information. The FIPPs were developed in the United States in the 1970s in response to privacy concerns over collection and dissemination of personal information by automated systems used by government agencies and companies [50]. According to Solove [51], the recommendation for Fair Information Practice Principles originated from the 1973 Code of Fair Information Practice (CFIP). CFIP was described in a landmark research report by the US Department of Health and Human Services (HHS) titled Education and Welfare Records: Computer, the Right of the Citizen Report [52]. The fundamental principles of fair information practice that organizations should adhere to are:

- There should be no secret system to store personal information [52]. This statement maps to US state privacy laws "right to access" [53].
- Individuals should be able to access information about them and know how it is used [52]. This statement maps to several US state privacy rights [53].

- Individuals should have the right to correct or amend any identifiable information about them in a record[52]. This statement maps to several US state privacy rights [53].
- Individuals should have the right to correct or amend any identifiable information about them in a record[52]. This statement maps to several US state privacy rights [53].
- Organizations must guarantee the reliability of personal data for its intended use and take reasonable precautions to prevent data misuse [52]. This statement maps to several US state privacy rights [53].

In 1974, the US Congress established the protection of individual privacy in the United States. Based on the Commission, the Privacy Act of 1974, 5 USC § 552 [8], incorporated the FIPPs into Federal law governing agencies on data collection, maintenance, use, and dissemination of personal information. [54]. FIPPs have five principles: data processing, notice, choice, access, security, and enforcement [54]. OECD guidelines contain core privacy principles adopted in national and international privacy legislation. OECD Principles include collection limitations, data quality, purpose specification, use limitations, security safeguards, openness, individual participation, and accountability [13]. In 2000, the FTC updated the FIPPs to address changes in technology and economics and make them more user-friendly. The revised versions of FIPPs were adopted in 2013 to meet the evolution of security and privacy risks [55]. The European Union adopted GDPR legislation in 2018 [7], which shares similarities to OECD guidelines [13] and is influenced by FIPPs. “The EU's General Data Protection˙ Regulation (GDPR) is the latest and most important in the FIPPs that became influential internationally" [56].

V. MAPPING FIPPS INTO A PRIVACY PROGRAM

Privacy solutions require integrating universal privacy principles into the data processing lifecycle. [57]. A well-written plan defines due diligence actions for collection, processing, and handling of personal data. Privacy risks can arise at any stage of PII processing, “from data collection through disposal" [58]. System owners may consider these stages outside the typical authorization boundary in some circumstances [58]. Organizations must minimize privacy risks, identify vulnerabilities, enable data owner stewardship and controller management, and protect against possible compromise by implementing security and privacy protection mechanisms into the data management life cycle [34]. Privacy by Design (PbD) is a holistic approach that integrates technical and organizational measures to integrate and apply privacy and data protection principles into systems that have specific capabilities [59]. This has resulted in the development of privacy enhancing technologies (PET). FIPPs have acted as universally recognized privacy values and a widely adopted framework for effectively translating privacy objectives into legal requirements. [57].

According to Dilmegani [60], PETs consist of various hardware and software solutions that help extract data without compromising security and privacy. There are many benefits of PET adoption which include:

- Secure data sharing.
- Improved privacy.
- Reduced risk of data breaches.
- Reduced litigation costs.
- Demonstrated compliance with governance and regulation

Various PETs are depending on the privacy use case. Use cases include anonymous remailing services, IPsec VPN, and encryption algorithms. Each share a common goal of maximizing data utility and preserving the privacy of PII.

Dilmegani [60] states the following are among the most noteworthy tool classes.

1) Cryptographic algorithms [60]
2) Secure multi-party computation (SMPC) [60]
3) Differential privacy [60]
4) Zero-knowledge proofs (ZKP) [60]
5) Obfuscation [60]
6) Pseudonymization [60]
7) Data minimization [60]
8) Synthetic data generation [7]
9) Federated learning [60]

FIPPs mapping into the data processing life cycle is achieved through Privacy by Design (PbD) principles [56]. Privacy by Design (PbD) is a set of principles used in Privacy engineering. Privacy Engineering is an emerging subdomain of software engineering that incorporates data privacy, data control methodology, and data control techniques in the system development lifecycle [56], [57]. According to Cavoukian, Privacy by Design has evolved from early efforts to embed FIPPs directly into the design and operation of information and communications technologies [57]. “Privacy by design refers to the philosophy and approach of directly incorporating privacy into the design and operational specifications of technology and systems informational” [61]. Privacy by Design originated in various emerging privacy practices and trends, including adoption and integration of Privacy-Enhancing Technologies (PETs) [61]. PETs play a crucial role in translating privacy principles into contextual privacy protection goals that are derived from legal frameworks and standards [62]. By embedding privacy principles in the CIA triad, organizations can establish a holistic and pragmatic approach to protecting the security and privacy of information.

There are security concerns unrelated to privacy, such as safeguarding trade secrets, while privacy concerns may not always be directly tied to information security [58]. In addition, the NIST Privacy Framework identifies other essential aspects of privacy protection, such as accountability, maintaining data quality and integrity, and enabling individual participation [58]. FIPPs five principles and OECD's eight principles represent varying levels of privacy protection for organizations when designing privacy programs.

To prevent unauthorized collection and processing of PII, and to enforce lawfulness, fairness, and transparency, storage limitation principle is aligned with confidentiality in the CIA

model. To preserve integrity, only the minimal amount of data required for the specified purpose should be collected, processed, and retained. For availability, data should be easily accessible and not needlessly duplicated or stored.

Figure 2 illustrates the integration of Fair Information Practice Principles (FIPPs) with the Confidentiality, Integrity, and Availability (CIA) model. The table maps the corresponding principles of FIPPs and OECD frameworks with relevant, appropriate aspects of privacy and data protection. By integrating these FIPPs principles into the CIA model (Confidentiality, Integrity, Availability), organizations can enhance privacy protections.

TABLE. 2 Comparison of Privacy Principles

Type	Principles	Description
FIPPs	Notice	Inform about data collection.
	Choice	Control data use
	Access	Provide data access
	Security	Protect data from unauthorized access.
OECD	Enforcement	Ensure compliance and accountability.
	Collection Limitation	Limit data collection
	Data Quality	Maintain data quality
	Purpose Specification	Define processing purposes
	Use Limitation	Restrict data use
	Security Safeguards	Implement security measures
	Openness	Promote transparency
	Individual Participation	Enable individual rights
	Accountability	Accountability for data handling

Note: Data for the table adapted from IAPP Legislation Tracker [53]and F. H. Cate [54].

As FIPPs strongly focus on the accountability and integration of the concepts in the processing of CIA triad data, it makes all parties involved more accountable for following best practices to comply with privacy laws and regulations. Protecting critical information characteristics, including confidentiality, integrity, and availability, from unauthorized access is essential to enhancing data privacy. According to Gregory [62], privacy control objectives are similar to common objectives in general but are specifically defined and implemented within the context of privacy and information security.

Privacy control objectives focus on protecting personal information while ensuring compliance with privacy regulations and standards. Establishing enforcement and accountability mechanisms mitigates non-compliance with privacy regulations, including obtaining and managing consent. Integrating FIPPs (with CIA security goals) provides a comprehensive approach to enhancing data security and privacy throughout the privacy rights data processing lifecycle. By aligning FIPPs with security goals, organizations can protect personal data from unauthorized access, maintain reliability and accuracy, and make information to authorized individuals as required. By ensuring proper consent practices, the availability of personal data is protected. While imposing significant fines on negligent corporations that cause privacy harm to individuals may serve as a deterrent, research indicates that fines alone are ineffective for preventing privacy harm.

Fines may act as a form of punishment, but they do not provide sufficient restitution for affected parties or bring closure for the improper usage and release of personal data [54]. Robust regulatory policies and technology adoption are crucial to ensure fairness and adequate protection of data to minimize privacy harm. This is especially important in light of data privacy concerns in the technology sector highlighted in this paper, where laws often struggle to address the breadth of intrusion on private information.

Figure 2 illustrates the integration of Fair Information Practice Principles (FIPPs) with the Confidentiality, Integrity, and Availability (CIA) model. As Figure 2 describes, integrating PbD, PE, and PET privacy functions while the CIA triad protects critical information characteristics, including confidentiality, integrity, and availability, from unauthorized access.

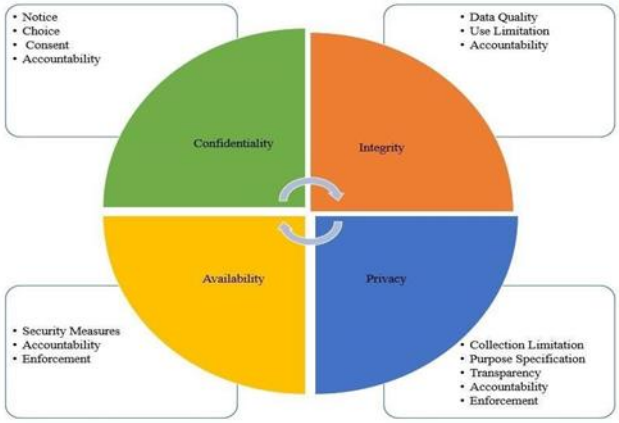

Fig. 2. Integrating FIPPS into CIA Model

Note: Data content adapted from M. E. Whitman and H. J. Mattord [6] and F. H. Cate [54].

Despite their promise and growing demand, there are significant downsides to PETs. A common critique of PETs is their implementation and use complexity, which may result in unauthorized users that can undermine individual privacy and security. Another common complaint is the cost of deployment and the requirement for vast computational capacity. Given the complexity and resource limitations, PETs can also challenge law and policymakers to audit or govern their use [63].Ultimately to maximize the protection of data privacy, the advantages of PETs far outweigh their disadvantages.

VI. CONCLUSION

The evolution of technology, the "right to be let alone" [17] has expanded into a broader topic that involves the intersection

of human rights, law, cybersecurity, data privacy, and geopolitics. Global efforts to promote data privacy control has resulted in the adoption of new guidelines, regulations, and models based on FIPPs. Important laws aiming to protect information security and privacy were enacted due to the increase in privacy violations, Compared to GDPR, the United States does not have a broad, sweeping law governing data privacy. Court decisions are focused more on tangible harm rather than actual harm and are inadequate to address the evolution and complex needs of data privacy. As such, robust laws must be enacted to adequately adapt to the changing landscape. The definition of privacy harm and control approaches evolved rapidly to mitigate privacy risk and meet compliance requirements. Therefore, awareness of the privacy harm regulatory environment is essential for organizations to avoid potential legal risks of noncompliance and reputation damage. This paper examined the legal aspects of privacy harm and how it evolved through the advancement of technology. Explained why FIPPs should be the foundation of privacy protection strategies, and can be utilized to integrate PbD and PETs with business processes to protect private information collection, processing, and disclosure [54]. As a solution to protect and secure personal information from emerging privacy threats and meet compliance requirements, PETs have rapidly evolved. A vital PET component is authentication, which enhances privacy by differentiating legitimate users from unauthorized users in a protected environment. A strong password policy, multifactor authentication, along with critical controls, improves information privacy and security to meet compliance requirements. Stewardship is an essential role for data owners and controllers, a role which requires integration of accountability with data protection strategies. The research has effectively addressed the changing context in privacy harm over time, how the existing legal framework adjudicates emerging privacy breaches, and the most efficient ways to use technology to improve privacy.

VII. STUDY LIMITATIONS

This study only exhaustively analyzed some legal frameworks and their implications. The jurisdiction and legal frameworks of data privacy may vary significantly across regions, including countries and states. The complexity of data privacy laws and their morphing nature were acknowledged. The study's scope and depth were subject to these limitations.

VIII. FUTURE WORK

The authors' next research project includes the connections between workplace privacy laws, insider threat programs, and privacy harm that can result from disseminating private information by insider threats within organizations. Additional research opportunities include implications of data privacy on virtual healthcare, implications of deep fakes, machine learning, artificial intelligence, and ChatGPT on personal privacy.

REFERENCES

[1] Federal Bureau of Investigation, "2021 Internet Crime Report," 2021. [Online]Available:https://www.ic3.gov/Media/PDF/AnnualReport/2021_IC3Report.pdf. Accessed on: Jan. 1, 2023.

[2] "Breach Barometer Report: Patient Privacy," [Online]. Available: https://www.protenus.com/breach-barometer-report. Accessed on: Mar. 29, 2023.

[3] D. W. Chadwick, "Federated identity management," in Foundations of Security Analysis and Design V: FOSAD 2007/2008/2009 Tutorial Lectures, vol. 5705, pp. 96-120, 2008.

[4] E. McCallister, Guide to Protecting the Confidentiality of Personally Identifiable Information, vol. 800, no. 122, Diane Publishing, 2010.

[5] S. Wairimu and L. Fritsch, "Modelling Privacy Harms of Compromised Personal Medical Data-Beyond Data Breach," in Proceedings of the 17th International Conference on Availability, Reliability, and Security, pp. 19, 2022.

[6] M. E. Whitman and H. J. Mattord, "Principles of Information Security," 5th ed., Boston, MA, USA: Cengage Learning, 2016.

[7] European Parliament and of the Council, "General data protection regulation," [Online]. Available: https://gdpr-info.eu/

[8] US Department of Justice, "Privacy Act of 1974," [Online]. Available: https://www.justice.gov/opcl/privacy-act-1974

[9] California Legislative Information. "Title 1.81.5 California Consumer Privacy Act of 2018 [1798.100-1798.199.100]," Jan. 01, 2023. [Online]. Available:https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5. Accessed on: May 08, 2023.

[10] Colorado General Assembly. "Protect Personal Data Privacy | Colorado General Assembly," Colorado General Assembly. [Online]. Available: https://leg.colorado.gov/bills/sb21-190. Accessed on: March 18, 2023.

[11] Virginia General Assembly, "Chapter 53. Consumer Data Protection Act," Code of Virginia. SB 227 Consumer Privacy Act, "SB0227," Mar. 24, 2022. [Online]. Available:https://tinyurl.com/pfsrjnj3. Accessed on: Apr. 04, 2023.

[12] SB0227 "Consumer Privacy Act, State of Utah." [Online]. Available: https://le.utah.gov/~2022/bills/static/SB0227.html

[13] CCDCOE, "The OECD Issues Revised Privacy Guidelines," [Online]. Available: https://ccdcoe.org/incyder-articles/the-oecd-issues-revised-privacy-guidelines/. Accessed on: May 14, 2023.

[14] Library of Congress, "ArtIII.S2.C1.6.1 Overview of Standing," Congress.gov. [Online]. Available: https://tinyurl.com/42nck379. Accessed on: March 14, 2023.

[15] E. Sherman, "No injury plaintiffs and standing," Geo. Wash. L. Rev., vol. 82, p. 834, 2013.

[16] J. Kosseff, "Defining cybersecurity law," Iowa L. Rev., vol. 103, p. 985, 2017.

[17] D. J. Solove, "A brief history of information privacy law," Proskauer on Privacy, 2016

[18] F. Westin, "Privacy and freedom," Washington and Lee Law Review, vol. 25, no. 1, p. 166, 1968.

[19] R. Calo, "The boundaries of privacy harm," Ind. LJ, vol. 86, p. 1131, 2011.

[20] National Constitution Center. (2023.) The amendments. [Online]. Available: https://constitutioncenter.org/the-constitution/amendments

[21] D. Minto, "Perversion by penumbras: Wolfenden, Griswold, and the Transatlantic Trajectory of Sexual Privacy," The American Historical Review, vol. 123, no. 4, pp. 1093–1121, Oct. 2018.

[22] L. Brandeis and S. Warren, "The right to privacy," Harvard law review, vol. 4, no. 5, pp. 193–220, 1890.

[23] Britannica, "Thomas Cooley," Accessed on March 29, 2023. [Online]. Available: https://www.britannica.com/biography/ThomasCooley. Accessed on: March 12, 2023.

[24] "Roberson v. Rochester Folding Box Co.," p. 538, 1902

[25] R. Kessler, "A common law for the statutory era: The right of publicity and New York's right of privacy statute," Fordham Urban Law Journal, vol. 15, no. 4, pp. 951-997, 1987.

[26] LexisNexis Community, "Pavesich v. New England Life Ins. Co. - Case Brief for Law School-LexisNexis." [Online]. Available: https://tinyurl.com/36zdhypb. Accessed: Feb. 28, 2023.

[27] Griswold v. Connecticut, 381 US 479, 85 S.Ct. 1678, 14 L.Ed.2d 51 (1965).

[28] Cornell Law School. Tort definition. LII / Legal Information Institute. [Online]. Available: https://www.law.cornell.edu/wex/tort

[29] W. L. Prosser, "Privacy," California Law Review, vol. 48, pp. 383–389, 1960

[30] LexisNexis, "Katz v. United States — Case Brief for Law School," Community, n.d., [Accessed: March 28, 2022]. [Online]. Available: https://www.lexisnexis.com/community/casebrief/p/ casebrief-katz-v-united-states

[31] R. F. Hamm, "Olmstead v. united states: The constitutional challenges of prohibition enforcement," Federal Trials and Great Debates in United States History, pp. 1–75, 2010.

[32] United States Privacy Protection Study Commission, Personal Privacy in an Information Society: The Report of the Privacy Protection Study Commission. The Commission, 1977, vol. 2.

[33] P. S. Browne, "Data privacy and integrity: an overview," in Proceedings of the 1971 ACM SIGFIDET (now SIGMOD) Workshop on Data Description, Access and Control, 1971, pp. 237–240

[34] M. F. Dennedy, J. Fox, and T. R. Finneran, The privacy engineer's manifesto: getting from policy to code to QA to value. Springer Nature, 2014.

[35] H. Nissenbaum, "Privacy as contextual integrity," Wash. L. Rev., vol. 79, p. 119, 2004.

[36] Spokeo, Inc. v. Robins, 136 S. Ct. 1540 (2016). Available: https://www.lexisnexis.com/community/casebrief/p/casebrief-spokeo-inc-v-robins

[37] Carpenter v. United States, Supreme Court of the United States, 2018. Available: https://www.supremecourt.gov/opinions/17pdf/16-402h315.pdf.

[38] D. J. Solove, "A taxonomy of privacy," Univ. Pennsyl. Law Rev., vol. 154, no. 3, pp. 477–564, 2006.

[39] Q. Covert, M. Francis, D. Steinhagen, and K. Streff, "Towards a triad for data privacy," Journal of Information Privacy and Security, vol. 17, no. 3, pp. 4379–4384, 2021.

[40] E. Graham-Harrison and C. Cadwalladr, "Cambridge analytica execs boast of role in getting donald trump elected," The Guardian, vol. 20, 2018.

[41] M. Rossenberg, N. Confessore, and C. Cadwalladr, "How trump consultants exploited the facebook data of million," The New York Times, 2018.

[42] Schroepfer, M., "An Update on Our Plans to Restrict Data Access on Facebook," Facebook Newsroom. [Online]. Available: https://about.fb.com/news/2018/04/restricting-data-

[43] K. A. Houser and W. G. Voss, "Gdpr: The end of google and facebook or a new paradigm in data privacy," Rich. JL & Tech., vol. 25, p. 1, 2018.

[44] U General Data Protection Regulation, "Questions and Answers," Human Rights Watch, June 2018. [Online]. Available: https://www.hrw.org/news/2018/06/06/eu-general

[45] Reuters, "Meta's Facebook agrees to settle data privacy lawsuit," Reuters, Aug 2022. [Online]. Available: https://www.reuters.com/legal/metas-facebook-agrees-settle-data-privacy-lawsuit-2022-08-26/

[46] N. Raymond, "Facebook parent Meta to settle Cambridge Analytica scandal case for $725 million," Reuters, Dec. 24, 2022. [Online]. Available: https://www.reuters.com/legal/facebook-parent-meta-pay-725-mln-settle-lawsuit-relating-cambridge-analytica-2022-12-23/

[47] "Comparison Charts: US State vs. EU Data Privacy Laws," Bloomberg Law, May 03, 2023. [Online]. Available: https://pro.bloomberglaw.com/brief/privacy-laws-us-vs-eu-gdpr/. Accessed: May 03, 2023.

[48] Supreme Court of the United States, "TransUnion LLC v. Ramirez," Syllabus, 2021. [Online]. Available: https://www.supremecourt.gov/ opinions/20pdf/20-297 4g25.pdf

[49] S. Wachter and B. Mittelstadt, "A right to reasonable inferences: rethinking data protection law in the age of big data and ai," Colum. Bus. L. Rev., p. 494, 2019.

[50] HEW report, "PDPEcho." [Online]. Available: https://pdpecho.com/tag/hew-report/. Accessed: March 29, 2023.

[51] .D. J. Solove, "A brief history of information privacy law," Proskauer on privacy, PLI, 2016.

[52] R. Gellman, "Fair Information Practices: A Basic History - Version 2.22 (April 6, 2022)," Available at http://dx.doi.org/10.2139/ssrn.2415020.

[53] IAPP Legislation Tracker, "US State Privacy Legislation Tracker," [Online]. Available: https://iapp.org/media/pdf/resource center/State Comp Privacy Law Chart.pdf, 2023, accessed: March 22, 2023.

[54] F. H. Cate, "The failure of fair information practice principles," Consumer protection in the age of the information economy, 2006

[55] Harper, "Privacy and fair information practices: The struggle to protect threatened values," 2021.

[56] Aljeraisy, M. Barati, O. Rana, and C. Perera, "Privacy laws and privacy by design schemes for the internet of things: A developer's perspective," ACM Computing Surveys (Csur), vol. 54, no. 5, pp. 1–38, 2021.

[57] A. Cavoukian, S. Shapiro, and R. J. Cronk, "Privacy engineering: Proactively embedding privacy, by design," Office of the Information and Privacy Commissioner, 2014. [Online]. Available: https://www.ipc.on.ca/wp-content/uploads/Resources/pbd-priv-engineering.pdf

[58] K. R. Boeckl and N. B. Lefkovitz, "NIST privacy framework: A tool for improving privacy through enterprise risk management, version 1.0," 2020

[59] J. Notario et al., "Pripare: Integrating privacy best practices into a privacy engineering methodology," in 2015 IEEE Security and Privacy Workshops, San Jose, 2015.

[60] C. Dilmegani, "Top 10 privacy enhancing technologies (pets) use cases," 2022. [Online]. Available: https://research.aimultiple.com/privacy-enhancing-technologies//

[61] A. Cavoukian, "Privacy by Design: Origins, Meaning, and Prospects for Assuring Privacy and Trust in the Information Era," in G. Yee (Ed.), Privacy Protection Measures and Technologies in Business Organizations: Aspects and Standards, pp. 170-208, IGI Global, 2012. [Online]. Available: DOI: 10.4018/978-1-61350-501-4.ch007

[62] A. Alshammari and A. Simpson, "Privacy architectural strategies: An approach for achieving various levels of privacy protection," in Proceedings of the ACM Conference on Proceedings of the ACM Conference, 2022, pp. 143-154, DOI: 10.1145/3267323.3268957.

[63] P. H. Gregory, CIPM Certified Information Privacy Manager All-in-One Exam Guide, ser. All-in-One. New York: McGraw-Hill Education, 2021

[64] J. Enieris, "Why PETs (Privacy-Enhancing Technologies) May Not Always Be Our Friends," September 2020. [Online]. Available: https://www.adalovelaceinstitute.org/blog/privacy-enhancing-technologies-not-always-our-friends.