FMDB *Transactions on Sustainable Public and Law*

Reimagining Tort Law as a Shield for Privacy: Assessing Digital-Age Resilience in Common Law Jurisdictions

Biranchi Narayan P. Panda[1,*]

[1]Xavier Law School, XIM University, Puri, Odisha, India.
biranchi@xim.edu.in[1]

Abstract: The technological innovations have profoundly transformed the scope and nature of privacy intrusions, raising pressing questions about the adequacy of tort-based protections in common law jurisdictions. This paper examines the conceptual foundations of privacy, the evolution of tort doctrines across the United States, United Kingdom, Canada, Australia, and India, and their effectiveness in addressing modern challenges such as surveillance, artificial intelligence profiling, and cross-border data leaks. Through a comparative analysis of statutory frameworks, such as the GDPR, and insights from human rights instruments, such as the ICCPR, the study evaluates whether tort law remains sufficient as a safeguard for individual privacy. Further, the paper contextualizes India's constitutional recognition of privacy in Puttaswamy v. Union of India alongside emerging statutory measures, and it underscores the broader need for reform across common law systems. Ultimately, the study concludes that tort law must be complemented by proactive legislation, judicial innovation, and alignment with international standards to protect privacy in the digital era adequately.

Keywords: Privacy Intrusions; Tort and Common Law; Digital Age; Data Protection; Law Systems; Human Rights; Technological Innovations; Artificial Intelligence (AI); Law Jurisdictions.

Received on: 03/06/2025, **Revised on:** 10/08/2025, **Accepted on:** 08/10/2025, **Published on:** 03/03/2026

Journal Homepage: https://www.fmdbpub.com/user/journals/details/FTSPL

DOI: https://doi.org/10.69888/FTSPL.2026.000581

Cite as: B. N. P. Panda, "Reimagining Tort Law as a Shield for Privacy: Assessing Digital-Age Resilience in Common Law Jurisdictions," *FMDB Transactions on Sustainable Public and Law*, vol. 1, no. 1, pp. 47–59, 2026.

1. Introduction

Privacy has long been regarded as a cornerstone of individual autonomy and dignity, yet its scope and significance have expanded dramatically in the digital age [29]. In classical liberal thought, privacy was framed as a right to be "let alone," famously articulated by Kastlová [26]. Over time, privacy developed into a multi-dimensional right encompassing informational self-determination, decisional autonomy, and protection against unwarranted state or private intrusion [30]. In today's interconnected world, privacy functions as a prerequisite for exercising other fundamental rights, including freedom of expression, association, and participation in democratic life [1]. The digital revolution has intensified debates over the adequacy of existing legal frameworks, particularly tort law, in providing meaningful remedies for modern privacy harms [31]. The rise of digital technologies, ranging from social media platforms and e-commerce to biometric surveillance and artificial intelligence, has created unprecedented challenges for privacy protection [32]. Personal data is constantly collected, processed, and monetized by corporations and governments, often without meaningful consent from individuals [33]. Cybersecurity breaches, data leaks, and algorithmic profiling demonstrate the scale of risks faced in the digital ecosystem [2]. Reports by

[*]Corresponding author.

international organizations indicate that billions of personal records are compromised annually, reflecting both the commercial value of data and the inadequacy of legal safeguards [34]. The borderless nature of the internet further complicates enforcement, as personal data can be transferred across jurisdictions in seconds, bypassing traditional regulatory and legal boundaries [35].

In common law jurisdictions, tort law has historically provided remedies for individual harms not explicitly covered by statute. Privacy, while not universally recognized as a stand-alone tort, has gradually been incorporated into tort law frameworks through judicial innovation [3]. In the United States, the Restatement (Second) of Torts adopted Prosser's fourfold classification of privacy torts: "intrusion upon seclusion, appropriation of name or likeness, public disclosure of private facts, and false light". Similarly, courts in the United Kingdom have developed the tort of misuse of private information, building upon equitable doctrines of breach of confidence. Canada, Australia, and India have each taken varied approaches, ranging from partial judicial recognition to reliance on constitutional or statutory rights [4]. These developments underscore tort law's adaptability, but also raise questions about its adequacy for addressing the novel harms emerging in the digital age [5]. The digital context presents challenges that traditional tort frameworks may not adequately address. Unlike physical intrusions, digital privacy violations often occur invisibly, at scale, and across borders. The harms are diffuse, affecting large populations simultaneously, and may be difficult to quantify in monetary terms. For instance, individuals subjected to algorithmic profiling may suffer discrimination or reputational damage without clear evidence of financial loss [6]. Tort law's traditional emphasis on individualized harm and compensatory damages raises doubts about its suitability for systemic digital privacy violations. Evaluating the adequacy of tort-based privacy protections in common law countries, therefore, requires examining whether existing doctrines can be stretched to address these challenges, or whether statutory and regulatory supplements are indispensable.

This paper critically evaluates the adequacy of tort-based privacy protections in common law jurisdictions, accounting for the unique challenges posed by digital technologies [7]. It asks multiple questions, such as: How have common law countries recognized and developed tort-based privacy protections? To what extent are these protections adequate to address digital-age intrusions such as mass surveillance, data breaches, and artificial intelligence profiling? What comparative insights can be drawn from statutory and civil law frameworks, including the GDPR? And what reforms or hybrid approaches may enhance the effectiveness of tort law in protecting privacy in the digital age? By addressing these questions, the study situates tort law within broader debates on global privacy governance and technological regulations. The paper proceeds in eight substantive sections. Section II develops a conceptual framework for privacy protection, distinguishing among privacy, data protection, and confidentiality, and tracing the evolution of tort-based remedies. Section III surveys the development of privacy torts across common law jurisdictions, focusing on the United States, United Kingdom, Canada, Australia, and India. Section IV evaluates the adequacy of these frameworks in addressing digital-age harms. Section V provides comparative perspectives, drawing lessons from statutory and civil law regimes. Section VI analyzes the challenges of applying tort law to digital privacy disputes, including cross-border complexities and freedom-of-expression concerns. Section VII outlines policy and reform options, while Section VIII situates India within the broader common law discourse. Section IX concludes with findings, implications, and recommendations for future research.

2. Conceptual Framework of Privacy Protection

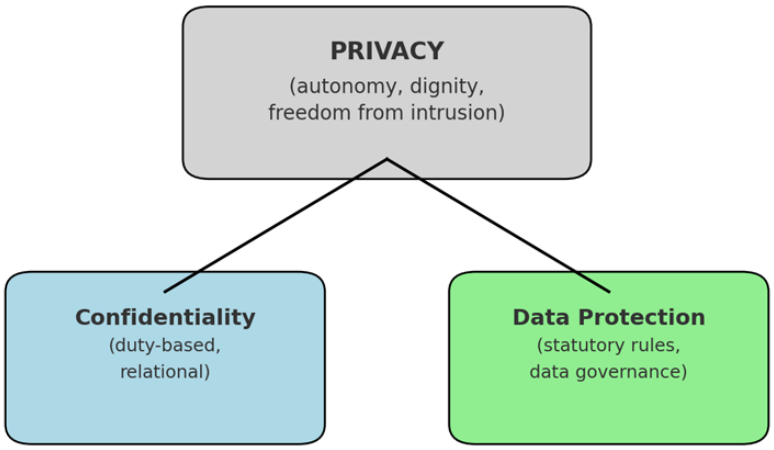
2.1. Defining Privacy in Legal and Philosophical Terms

Privacy is an elusive concept, notoriously difficult to define with precision. Philosophically, it has been described as the "condition of being free from unwanted intrusion or observation, allowing individuals to control access to themselves and their personal information". In legal discourse, definitions vary across jurisdictions and disciplines. In common law traditions, privacy has often been framed in negative terms as the right "to be let alone". More contemporary scholars, however, view privacy as a positive right to informational self-determination and decisional autonomy, suggesting that privacy is best understood as a "pluralistic set of related problems" rather than a single coherent right, encompassing surveillance, data processing, aggregation, and dissemination [8]. This conceptual diversity complicates the formulation of effective legal protections, particularly in the digital context where harms do not map neatly onto traditional legal categories.

2.2. Distinction between Privacy, Data Protection, and Confidentiality

Although often used interchangeably, privacy, data protection, and confidentiality represent distinct but overlapping concepts. Privacy refers to "an individual's ability to control access to their personal sphere, including body, space, communications, and information". Data protection, by contrast, focuses on regulatory mechanisms governing the collection, storage, and processing of personal data, typically through statutes and administrative frameworks such as the GDPR. Whereas confidentiality arises primarily in relational contexts, it imposes duties on parties, such as doctors, lawyers, or employers, not to disclose information entrusted to them. The distinctions matter for tort law [9]. While confidentiality has long been recognized in equity and contractual obligations, privacy torts have emerged only recently in common law countries, often borrowing from confidentiality doctrines. Data protection, meanwhile, is generally a statutory innovation that fills gaps where tort law is

inadequate [10]. Understanding these distinctions is crucial to assessing whether tort-based approaches can provide sufficient remedies in the digital age (Figure 1).



(Author's illustration, adapted from Chaffey [16]; Solove and Citron [17]; and Solove [18])

Figure 1: Conceptual Distinctions in Privacy Protection

2.3. Evolution of Tort-Based Privacy Protections

The development of tort-based privacy protections in common law jurisdictions reflects judicial efforts to adapt traditional doctrines to new forms of harm [11]. In the United States, the landmark work of Isaak and Hanna [28] systematized privacy into four distinct torts: "intrusion upon seclusion, appropriation of name or likeness, public disclosure of private facts, and false light". While influential, Prosser's framework has been criticized for fragmentation and conceptual inconsistency. In the United Kingdom, courts initially relied on breach of confidence to protect private information [12]. Still, the Campbell v. MGN Ltd. decision formally recognized misuse of private information as a distinct cause of action, influenced by the European Convention on Human Rights (ECHR). Canada has gradually recognized an intrusion upon seclusion through cases such as the Court of Appeal for Ontario [3], though the scope of other privacy torts remains unsettled. Australia has shown hesitance, with some courts acknowledging the possibility of a privacy tort while leaving much of the field to statutory frameworks [13]. India, meanwhile, recognized privacy as a constitutional right in the South Asian Translaw Database [4], but tort-based remedies remain underdeveloped. This uneven evolution underscores both the adaptability and limitations of tort law. Courts have responded incrementally to social and technological change, but gaps persist in addressing systemic, large-scale intrusions characteristic of digital technologies.

2.4. Frameworks for Assessing Adequacy of Legal Protections in the Digital Age

Evaluating the adequacy of tort-based privacy protections requires a multidimensional framework. Three criteria are particularly salient:

- **Substantive Scope of Protection:** Does the law cover modern privacy harms, such as online surveillance, biometric data misuse, and algorithmic profiling? Many tort doctrines remain tethered to individualized harms, leaving systemic digital intrusions inadequately addressed.
- **Procedural Accessibility:** Can individuals realistically bring tort claims in digital privacy cases? High litigation costs, difficulty proving damages, and cross-border enforcement challenges often limit access to remedies.
- **Effectiveness of Remedies:** Do torts provide deterrent and compensatory outcomes sufficient to address large-scale digital harms? Traditional damages may fail to capture non-economic injuries such as loss of control over data, reputational harm, or chilling effects on autonomy.

Comparative insights also matter [14]. The European Union's GDPR, though statutory rather than tort-based, illustrates how robust rights, administrative enforcement, and significant penalties can provide systemic protection. By contrast, tort-based frameworks often operate reactively, addressing harms after they occur rather than preventing them. A holistic assessment thus requires analyzing not only the doctrinal adequacy of tort law but also its institutional effectiveness and capacity to evolve

alongside technological innovation [15]. This framework will guide subsequent sections of the paper in evaluating common law jurisdictions.

3. Tort Law and Privacy in Common Law Jurisdictions

3.1. United States: Restatement (Second) of Torts and Prosser's Four Privacy Torts

The United States is often considered the birthplace of modern privacy torts, owing largely to the work of William Prosser. In his influential 1960 article, Prosser systematized privacy into four distinct torts: Intrusion upon seclusion, appropriation of name or likeness, public disclosure of private facts, and false light [16]. These categories were subsequently adopted by the House of Lords [27], which has guided courts across multiple states. These are: "Intrusion upon seclusion, protects individuals against intentional intrusions into their private affairs, such as unauthorized surveillance or wiretapping". Appropriation addresses commercial use of a person's name or likeness without consent, forming the basis for modern "right of publicity" claims. Public disclosure of private facts prevents the dissemination of highly offensive personal information not of legitimate public concern [17]. False light protects against misleading portrayals that damage reputation, overlapping with defamation but broader in scope. Despite this framework, U.S. privacy torts have been criticized for fragmentation and uneven application. State-level variations create inconsistency, and First Amendment concerns often limit recovery where speech interests are implicated. Moreover, proving damages in digital privacy cases remains challenging, as harms are often intangible and collective rather than individual. While U.S. courts continue to develop these torts incrementally, statutory interventions such as the California Consumer Privacy Act (CCPA) highlight the insufficiency of tort law alone in regulating digital privacy.

3.2. United Kingdom: Misuse of Private Information and Breach of Confidence

The United Kingdom has approached privacy protection through the equitable doctrine of breach of confidence, which evolved into a broader tort of misuse of private information [18]. The turning point came in 32, when the House of Lords recognized that "Article 8 of the European Convention on Human Rights (ECHR) requires effective protection of personal privacy". In Campbell, the court held that publishing details of Naomi Campbell's drug treatment infringed her privacy, establishing a test that weighs the claimant's reasonable expectation of privacy against the publisher's freedom of expression under Article 10 ECHR. This balancing exercise has since guided UK courts in cases involving celebrities, journalists, and ordinary citizens. While the tort provides a flexible remedy for unauthorized disclosure of personal information, its reliance on proportionality balancing raises uncertainty [19]. Critics argue that English law lacks a unified privacy tort comparable to the U.S. fourfold model, leaving gaps in protection for emerging harms such as online data scraping and algorithmic profiling. Nonetheless, the UK experience demonstrates how courts can expand equitable principles into modern tort remedies, influenced heavily by human rights jurisprudence [20].

3.3. Canada: Intrusion Upon Seclusion and Provincial Privacy Torts

Canada's approach combines statutory and common law elements. Several provinces, including British Columbia, Manitoba, and Saskatchewan, enacted statutory privacy torts as early as the 1970s, granting individuals the right to sue for "wilful violation of privacy". However, broader recognition at common law came in the Ontario Court of Appeal [3], where the court formally recognized the tort of intrusion upon seclusion [21]. In Jones, the court held that unauthorized access to personal banking records constituted an actionable intrusion, even in the absence of economic loss. Importantly, it awarded modest damages ($10,000) to signal the seriousness of the violation. This decision marked a significant development, affirming that common law can adapt to digital privacy harms without statutory intervention. Other Canadian cases have cautiously extended privacy torts to misuse of personal data and unauthorized dissemination of intimate images [22]. However, courts remain hesitant to recognize broader torts such as public disclosure of private facts, preferring incremental development. Critics note that the modest damages awarded in such cases may fail to deter large-scale digital intrusions. Still, Canada demonstrates how privacy torts can evolve pragmatically alongside statutory data protection frameworks, such as the federal Personal Information Protection and Electronic Documents Act (PIPEDA).

3.4. Australia: Emergent Recognition of Privacy Torts

Australian courts have historically resisted recognizing a standalone tort of invasion of privacy. In LawTeacher [8], the High Court left open the possibility of such a tort but declined to establish it directly. Since then, lower courts have occasionally entertained privacy claims, but recognition remains patchy and uncertain. Scholars argue that Australia's reliance on statutory frameworks, such as the Privacy Act 1988, has stunted the development of privacy torts by the courts. While the Act regulates the handling of personal information by government and private entities, it does not provide robust remedies for individuals in cases of personal intrusion or misuse. As a result, tort-based privacy protection remains embryonic. Recent law reform commissions have recommended creating a statutory cause of action for serious invasions of privacy, but progress has been

slow [23]. Australia illustrates how judicial hesitancy, combined with reliance on statutes, can leave gaps in tort-based privacy protection in the digital age.

3.5. India: Judicial Recognition of Privacy Rights and Tort Remedies

India presents a hybrid model where constitutional recognition of privacy intersects with underdeveloped tort remedies. In the South Asian Translaw Database [4], the Supreme Court held that privacy is a fundamental right under the Indian Constitution. This landmark decision provided a robust normative foundation for privacy but did not directly create tort remedies. At the tort level, Indian jurisprudence remains limited [24]. While some courts have recognized claims for defamation, harassment, or unauthorized publication of personal information, there is no clearly defined privacy tort comparable to those in the U.S. or Canada. The recent enactment of the Digital Personal Data Protection Act suggests a statutory shift, potentially diminishing the role of tort law in this field [25]. Critics argue that without clear tort remedies, individuals face difficulties in pursuing redress for digital privacy harms such as non-consensual data sharing, cyberstalking, or surveillance. India's case underscores the need for harmonizing constitutional, statutory, and tort-based approaches to ensure meaningful privacy protection (Table 1).

Table 1: Comparative tort-based privacy protection in common law jurisdictions

Jurisdiction	Key Doctrines/Torts Recognized	Landmark Cases	Strengths	Weaknesses
United States	Four privacy torts (intrusion, appropriation, public disclosure, false light)	Dietemann v. Time; Cox Broadcasting v. Cohn	Well-developed doctrinal framework; right of publicity	Fragmented across states; difficulty proving damages; First Amendment limits
United Kingdom	Misuse of private information; breach of confidence	Campbell v. MGN Ltd.	Strong linkage to human rights law (ECHR)	Balancing test creates uncertainty; lacks a unified tort model
Canada	Intrusion upon seclusion; provincial privacy statutes	Chaffey [16]	Incremental judicial innovation; statutory support	Limited damages; uneven recognition of broader privacy torts
Australia	No formal privacy tort; statutory privacy law dominates	LawTeacher [8]	Strong statutory framework	Judicial reluctance; weak individual remedies
India	Privacy as a constitutional right; underdeveloped tort remedies	South Asian Translaw Database [4]	Robust constitutional foundation	Lack of tort clarity; reliance on emerging statutes

3.6. Adequacy of Tort-Based Protections in the Digital Age: Surveillance, Data Leaks, and AI Profiling

Drastically, the digital age has transformed the nature of privacy infringements. Unlike traditional harms such as unauthorized entry into a home, modern violations often occur invisibly, at scale, and through highly technical means. Tort law's effectiveness in addressing such harms varies considerably. Mass surveillance illustrates the challenge. In the United States, programs such as the National Security Agency's PRISM surveillance (revealed in 2013) raised concerns about bulk data collection and its compatibility with Fourth Amendment protections. Yet tort claims against government surveillance are typically barred by doctrines of state immunity or national security exceptions. Similarly, in the UK, litigation before the Investigatory Powers Tribunal and the European Court of Human Rights has underscored the difficulty of framing surveillance as a tortious intrusion rather than a regulatory or constitutional issue. Similarly, Data breaches also demonstrate inadequacy. Courts in Canada and the U.S. have sometimes recognized a claim for intrusion upon seclusion or negligence in the context of unauthorized data disclosures. However, proving compensable harm remains difficult when stolen data has not yet been misused, leaving many victims uncompensated. Further, Artificial intelligence (AI) profiling poses novel risks, such as algorithmic discrimination, predictive policing, or reputational harms from automated scoring systems. These harms often lack a clear analogy in Prosser's four torts or in the UK misuse of private information. Proving causation and damages against opaque algorithmic systems is exceedingly difficult, raising questions about whether tort law is structurally equipped to address such harms.

3.7. Gaps in Existing Tort Frameworks for Digital Harms

Several structural gaps limit the adequacy of tort law in addressing digital harms:

- **Individualization of Claims:** Tort law is designed to remedy individualized harms. Digital privacy violations, however, often affect millions simultaneously, such as in large-scale data breaches. Class actions are possible, but procedural barriers and jurisdictional complexities limit their effectiveness.
- **Intangible Harms:** Many digital intrusions cause emotional distress, reputational loss, or chilling effects, which tort law often undervalues. Traditional emphasis on economic damages leaves victims undercompensated.
- **Cross-Border Enforcement:** Digital platforms operate globally. A privacy intrusion in California may affect users in India, but local courts may lack jurisdiction or enforcement mechanisms to hold foreign defendants accountable.
- **Delay in Doctrinal Evolution:** Courts move incrementally, often lagging behind rapid technological innovations. By the time tort doctrines adapt, new privacy threats emerge, creating a perpetual gap between law and technology.

Thus, while torts can provide remedies in specific, narrow contexts, they often fail to address systemic harms of the digital environment.

4. Challenges of Proving Damages in Privacy Torts

Damage is central to evaluating adequacy. In many cases, plaintiffs struggle to demonstrate tangible losses from privacy intrusions. For instance, U.S. courts frequently dismiss data breach claims for lack of "standing," requiring proof of actual identity theft or financial loss. This threshold excludes harms that include loss of control over personal data, increased risk of misuse, or dignitary injuries. Canadian courts have partially addressed this gap through the Court of Appeal for Ontario [3], which recognized that intrusion itself could ground liability without proof of economic loss. However, damages awarded in such cases are typically modest, insufficient to deter large-scale corporate intrusions. Similarly, in the UK, damages for misuse of private information have increased in celebrity cases but remain limited for ordinary individuals. In the digital age, harms are collective and probabilistic. Therefore, a stolen dataset may harm none, some, or all its millions of subjects, depending on subsequent misuse. Tort law's individualized damages model is poorly suited to this reality, necessitating supplemental regulatory or statutory approaches.

4.1. Cross-Border Nature of Digital Privacy Violations

The borderless nature of digital networks further challenges tort law. Data routinely flows across multiple jurisdictions, often stored in "cloud" servers spanning different countries. This complicates both jurisdiction and choice of law. For example, litigation following the Cambridge Analytica scandal involved users from multiple countries, but remedies varied widely depending on whether the claimants were in the U.S., the UK, or India. Courts often dismiss claims against foreign defendants due to jurisdictional hurdles, leaving victims without recourse [36]. Moreover, enforcement of tort judgments across borders is uncertain. Even where jurisdiction is established, practical difficulties arise in enforcing awards against multinational corporations headquartered abroad. By contrast, statutory regimes such as the GDPR impose extraterritorial obligations, underscoring how tort law alone may be insufficient in transnational digital disputes.

4.2. Case Studies of Digital Privacy Litigation in Common Law Jurisdictions

- **Equifax Data Breach (United States):** A massive data breach exposed the personal information of 147 million Americans. While lawsuits were filed under the torts of intrusion upon seclusion and negligence, settlement largely relied on statutory consumer protection claims. Tort remedies were secondary and limited.
- **Google Street View Litigation (United States and Canada):** Lawsuits alleged unauthorized collection of Wi-Fi data by Google vehicles. U.S. plaintiffs struggled under federal statutory frameworks, while Canadian courts entertained tort claims under the intrusion upon seclusion doctrine, though outcomes were modest.
- **Campbell vs. MGN Ltd. (United Kingdom):** While not a digital case, it illustrates the expansion of privacy torts into personal information contexts, laying the foundation later applied in online cases involving social media disclosures.
- **Cambridge Analytical Scandal:** Millions of Facebook users had their data harvested for political profiling. Litigation in multiple jurisdictions showed the limits of tort law, as claims often failed without statutory support. UK claimants pursued misuse of private information, but remedies were narrow; U.S. litigation largely relied on consumer statutes rather than privacy torts.

These cases demonstrate that tort law can contribute to redress, but it rarely forms the backbone of digital privacy enforcement. Instead, statutory and regulatory claims dominate litigation strategies (Table 2).

Table 2: Global data breaches reported (2013–2022)

Reported Data Breaches (Millions of Records Exposed)	
2013	500
2014	800
2015	1,100
2016	2,700
2017	2,700
2018	3,400
2019	4,200
2020	4,700
2021	5,100
2022	5,300

(*Data source: Hawkes [10]*)

This upward trend highlights the scale of harms tort law struggles to address, reinforcing arguments for systemic, statutory, or hybrid solutions.

5. Comparative Perspectives

5.1. Tort-Based Protections vs. Statutory/Regulatory Frameworks

Tort law, as analyzed in prior sections, provides an important but limited mechanism for redressing privacy violations. In contrast, statutory and regulatory frameworks explicitly impose obligations on data processors and controllers, offer clearer enforcement mechanisms, and often provide remedies independent of tort principles [37]. The GDPR exemplifies this, as it imposes proactive duties on organizations: "data minimization, purpose limitation, security safeguards, and the right to erasure". Unlike tort claims, which require proof of harm and causation, the GDPR grants individuals' rights regardless of demonstrable damage, shifting the burden toward compliance rather than post hoc litigation. In the United States, where no comprehensive federal privacy law exists, reliance on tort law and sector-specific statutes (e.g., HIPAA, COPPA, and the CCPA in California) leaves gaps [38]. For example, data brokers may exploit personal information in ways not neatly addressed by Prosser's torts. This illustrates the regulatory deficit of tort-centered systems, particularly in addressing large-scale or anticipatory privacy risks [39]. While Canada represents a middle ground, common law torts, such as Jones v. Tsige, supplement statutory frameworks, such as the Personal Information Protection and Electronic Documents Act (PIPEDA). Here, tort fills residual gaps but is not the primary enforcement tool [40]. Thus, while tort provides flexible, judge-made remedies, statutory frameworks offer systemic, preventive protection, suggesting that reliance on tort alone leaves significant inadequacies in the digital era.

5.2. Hybrid Models: Integrating Tort and Statutory Protections

Many jurisdictions have implicitly adopted hybrid models in which tort law coexists with statutory regimes. The interaction between the two can be complementary:

- **Deterrence + Compensation:** Statutes impose compliance duties and fines, while tort offers individualized remedies. For instance, under the GDPR, regulatory authorities may fine corporations, while victims can simultaneously pursue damages in national tort law.
- **Doctrinal Evolution:** Tort litigation can highlight systemic weaknesses, prompting statutory reform. U.S. class actions on data breaches, though often dismissed, have pressured legislatures to expand breach notification laws.
- **Residual Safeguards:** Where statutes are silent, tort provides a fallback. In Canada, intrusion upon seclusion protects against non-commercial invasions of privacy not covered by PIPEDA.

However, hybrid models face tensions such as overlapping claims, double recovery risks, and increased litigation costs. In practice, courts often defer to statutory schemes where they exist, limiting tort's independent role [41]. The hybrid approach may therefore be best understood as a safety net rather than a coequal pillar.

5.3. Comparative Civil Law Approaches to Privacy Protection

Civil law jurisdictions, particularly in continental Europe, conceptualize privacy less as a tort and more as a fundamental right. This has important implications for enforcement:

- **France:** Privacy is protected under Article 9 of the Code Civil, which grants individuals broad remedies for violations, including injunctions and damages, without the need to fit within Prosser's categories.
- **Germany:** The Allgemeines Persönlichkeitsrecht (general personality right), derived from the German Basic Law, provides a constitutional foundation for privacy claims. Courts have developed a rich jurisprudence protecting informational self-determination, which has shaped both statutory law and EU data protection frameworks.
- **European Union:** The Charter of Fundamental Rights enshrines data protection (Article 8) as distinct from privacy (Article 7), reinforcing a rights-based approach. This contrasts sharply with the common law's piecemeal, tort-based protections.

These civil law models illustrate the structural advantage of embedding privacy in fundamental rights; they permit broader, more flexible judicial reasoning than tort categories allow, and they integrate seamlessly with statutory regimes like the GDPR.

5.4. Influence of Human Rights Instruments on Tort Doctrine

Human rights instruments increasingly shape tort law in common law jurisdictions. In the UK, the Human Rights Act 1998 incorporated the European Convention on Human Rights (ECHR) into domestic law. Article 8 (right to respect for private and family life) has driven the expansion of tort-like protections through the doctrine of misuse of private information. Courts have recognized that traditional breach of confidence was insufficient, and Article 8 inspired doctrinal evolution. Similarly, in Canada, the Charter of Rights and Freedoms influences courts' willingness to recognize new torts in response to evolving privacy needs. The U.S. courts, although not bound by an equivalent supranational rights regime, have seen constitutional privacy doctrines inform tort adjudication in areas such as surveillance and reproductive rights. These examples show that human rights law acts as a catalyst for tort evolution, encouraging courts to stretch existing categories or recognize new causes of action where privacy interests demand it. However, reliance on rights-based interpretation risks inconsistency and concerns about judicial activism [42].

5.5. Case Studies of Comparative Approaches

- **Google Spain SL vs. AEPD (EU Court of Justice):** The case established the "right to be forgotten," grounded in EU data protection and fundamental rights. No equivalent tort exists in U.S. or UK law, underscoring the difference between rights-based and tort-based approaches.
- **Campbell vs. MGN Ltd (United Kingdom):** A landmark misuse of private information case, where the UK courts explicitly integrated Article 8 ECHR into tort-like protections. This demonstrates hybridization between tort and human rights law.
- **Jones vs. Tsige (Canada):** The Ontario Court of Appeal recognized intrusion upon seclusion as a standalone tort, illustrating the common law's capacity for doctrinal innovation, influenced indirectly by international privacy discourse.
- **Google LLC vs. Equustek Solutions Inc. (Canada):** The Supreme Court of Canada issued a global injunction requiring Google to delist search results, demonstrating how domestic courts grapple with the cross-border dimension of digital privacy.

Together, these cases illustrate that while tort plays a role, the most robust privacy protections emerge in jurisdictions where statutory frameworks and human rights instruments supplement tort law.

5.6. Comparative Evaluation: Lessons Learned

From a comparative perspective, several lessons emerge:

- **Common Law Torts Remain Reactive:** They provide remedies after harm occurs, but struggle with systemic, large-scale risks.
- **Civil Law Systems are Structurally More Protective:** By embedding privacy in fundamental rights, they enable proactive and expansive judicial reasoning.
- **Statutory Frameworks are Indispensable:** GDPR and similar laws demonstrate that proactive regulation, backed by strong enforcement, is essential to supplement tort remedies.
- **Hybrid Models are Pragmatic:** Jurisdictions like Canada show that torts remain useful for filling statutory gaps, but cannot substitute for robust regulation.
- **Human Rights Law Bridges the Gap:** It allows courts to reinterpret torts in light of evolving privacy norms, aligning domestic doctrine with global standards.

Thus, the comparative evidence strongly suggests that tort law alone is insufficient, but its integration into broader statutory and rights-based frameworks enhances overall privacy protection.

6. Challenges in Applying Tort Law to Digital Privacy

6.1. Rapid Technological Change Outpacing Legal Evolution

Tort law is inherently reactive, designed to redress harms after they occur rather than prevent them. This characteristic creates tension in the recent age, where technological innovations such as artificial intelligence (AI), machine learning, and mass data analytics evolve faster than courts or legislatures can respond [43]. Privacy harms such as algorithmic profiling, biometric tracking, and predictive policing often occur invisibly, leaving victims unaware of intrusions until consequences emerge. Traditional tort categories, intrusion upon seclusion or disclosure of private facts, were never designed to capture such complex, diffuse harms. This mismatch generates uncertainty about whether courts can extend existing doctrines or whether statutory innovation is essential [44].

6.2. Balancing Freedom of Expression with Privacy Rights

Another major challenge arises from conflicts between privacy and freedom of expression, particularly in media and digital platforms. In jurisdictions like the U.K., courts have struggled to balance the tort of misuse of private information with Article 10 of the European Convention on Human Rights, protecting free expression [45]. Landmark cases such as Reis et al. [34] illustrate the judiciary's attempts to balance celebrity privacy with press freedom. In the U.S., the First Amendment exerts even greater influence, often limiting the scope of privacy torts when they conflict with public-interest reporting. The tension intensifies in the digital environment, where bloggers, influencers, and platforms blur the boundaries between private and public spheres. Tort law alone may lack the nuanced balancing mechanisms needed to address these competing rights.

6.3. Jurisdictional Hurdles in Cross-Border Digital Disputes

Digital privacy harms rarely respect territorial boundaries. A data breach in California may impact users in India, while surveillance conducted in one jurisdiction may involve servers located in another [46]. Tort law, rooted in territorial jurisdiction, struggles with these cross-border dimensions. Conflict-of-law rules often leave victims uncertain about where to sue, what law applies, and whether judgments will be enforced. For example, U.S. courts have often dismissed privacy suits against foreign corporations on jurisdictional grounds, leaving victims without redress. The cross-border nature of digital privacy violations underscores the limits of tort-based frameworks and highlights the need for harmonized international rules.

6.4. Inequalities in Access to Justice for Individuals vs. Corporations

Tort law presupposes that individuals can vindicate their rights through litigation. In practice, litigation is expensive, lengthy, and uncertain, especially in complex digital privacy cases that involve expert evidence and technical discovery [47]. By contrast, corporations often have greater resources to defend against such claims or to negotiate settlements. This imbalance risks making tort remedies inaccessible to ordinary individuals whose data rights are violated. Class actions can mitigate this imbalance, as seen in Canada and Australia, but they are not universally available [48]. The uneven distribution of resources thus limits tort law’s effectiveness in protecting digital privacy.

6.5. Risk of Chilling Effects on Media and Innovation

Finally, expanding tort remedies to cover digital privacy risks would chill legitimate activities, such as investigative journalism, whistleblowing, and technological innovation. If privacy torts are interpreted too broadly, they may deter journalists from reporting on matters of public interest or dissuade companies from developing new technologies for fear of liability. This concern is evident in U.S. debates over privacy litigation, where courts caution against overextending tort liability that could undermine free markets or democratic discourse. The challenge is thus twofold: ensuring robust protection against genuine privacy violations while safeguarding spaces for free expression and innovation.

7. Policy and Reform Options

7.1. Need for Statutory Supplements to Tort Law in Common Law Countries

While tort law provides a flexible, judge-made mechanism for privacy protection, its reactive nature and case-by-case orientation make it poorly suited to address systemic digital harms. Statutory supplements are therefore essential to establish clear rules, uniform protections, and proactive safeguards. The GDPR demonstrates how comprehensive legislation can secure

rights of access, rectification, and erasure that tort law alone cannot. In common law countries, statutes such as the UK's Data Protection Act 2018 and Canada's Personal Information Protection and Electronic Documents Act (PIPEDA) supplement tort protections by creating baseline obligations for data controllers. These statutory frameworks fill the gaps left by tort law, especially regarding data governance, breach notification, and preventive oversight.

7.2. Expanding Definitions of Actionable Harms in Tort Law

One reform option is to expand tort law's recognition of actionable harms. Currently, courts often require proof of tangible damages, such as financial loss, before awarding remedies for privacy violations. However, digital intrusions often result in dignitary harm, loss of control over personal data, reputational injury, or emotional distress that are harder to quantify but equally significant. Judicial recognition of these harms, as seen in Canada's Court of Appeal for Ontario's intrusion upon seclusion tort [3], signals a shift towards broader conceptions of injury. Extending such principles across common law jurisdictions would enhance tort law's capacity to address digital-age privacy harms.

7.3. Encouraging Judicial Innovation and Interpretation

Judges in common law systems play a vital role in shaping privacy protections through creative interpretation. In Australia, courts have cautiously recognized the possibility of a tort of privacy, while in India, judicial activism has elevated privacy to a constitutional right. Encouraging courts to adapt tort principles to new contexts—such as algorithmic profiling or biometric surveillance could bridge gaps while legislatures catch up. Judicial innovation allows tort law to evolve incrementally, ensuring responsiveness without wholesale legal reform. However, excessive reliance on judicial activism risks inconsistency and unpredictability across jurisdictions.

7.4. Integrating Tort Law with Data Protection Legislation

Another reform option is greater integration between tort law and statutory data protection regimes. Tort claims can complement regulatory enforcement by providing victims with individualized remedies while regulators address systemic noncompliance. For example, the GDPR allows data subjects to seek damages compensation in addition to regulatory fines, creating a dual enforcement mechanism. In common law countries, similar integration could ensure that tort law and statutes operate in tandem rather than in isolation. This dual approach would strengthen accountability for data controllers and expand individuals' access to remedies.

7.5. Proposals for Harmonized International Frameworks

Given the global nature of digital privacy violations, piecemeal national approaches are insufficient. A harmonized international framework could help overcome jurisdictional barriers by establishing common principles for privacy protection. Instruments such as the OECD Privacy Guidelines and the Council of Europe's Convention 108+ provide promising starting points. Building on these, common law countries could advocate for a multilateral treaty that balances privacy rights, freedom of expression, and innovation. Harmonization would also reduce compliance burdens for multinational corporations and ensure a baseline level of protection for individuals worldwide. However, political and cultural differences between jurisdictions remain a significant obstacle to such initiatives.

8. India's Position in Context

8.1. Constitutional Recognition of Privacy

India's recognition of privacy as a constitutional right is a landmark development in the global common law landscape. In the South Asian Translaw Database [4], a nine-judge bench of the Supreme Court unanimously declared "privacy to be a fundamental right under Article 21 of the Constitution, which guarantees the right to life and personal liberty". The judgment elevated privacy beyond statutory or tort protections, framing it as intrinsic to human dignity and autonomy. Importantly, the Court emphasized informational privacy in the digital age, acknowledging the risks posed by state surveillance, data mining, and private-sector data collection. This constitutional grounding creates a normative foundation for privacy protection but leaves questions about the adequacy of existing tort remedies.

8.2. Limited Development of Privacy Torts in Indian Jurisprudence

Unlike Canada, the United States, or the UK, Indian tort law has not developed a robust body of privacy torts. While cases such as Chaffey [16] recognized liability for harassment arising from data misuse, India lacks distinct torts such as intrusion upon seclusion or public disclosure of private facts. Privacy disputes are often litigated under defamation, negligence, or breach of

confidence rather than as standalone torts. Courts have sometimes granted damages for non-consensual disclosure of personal information, but precedents remain inconsistent. This underdevelopment creates uncertainty for claimants seeking redress for modern privacy harms such as data breaches, AI-driven profiling, or mass surveillance.

8.3. Overlap with Statutory Developments

The enactment of the Digital Personal Data Protection Act, 2023 (DPDPA), marks a significant statutory step toward regulating digital privacy. The law introduces consent requirements, obligations for data fiduciaries, and penalties for non-compliance. However, the DPDPA has been critiqued for granting the government wide exemptions, potentially undermining individual protections against state surveillance. Importantly, the Act does not provide a comprehensive private right of action for individuals, leaving tort claims as a potential supplementary avenue. This statutory-tort overlap highlights the need for a more coherent framework that integrates judicially recognized harms with legislative protections.

8.4. Comparative Adequacy of India's Tort-Based Privacy Protection in the Digital Age

In a comparative perspective, India's reliance on constitutional principles and emerging statutes contrasts with jurisdictions such as Canada, where privacy torts are well-defined by the judiciary. While Puttaswamy provides a strong normative foundation, its translation into actionable remedies remains limited. Victims of digital privacy violations in India often lack clear avenues for civil damages. For example, remedies for identity theft or data breaches largely depend on sectoral regulations or consumer protection statutes rather than tort principles. Compared to the EU's GDPR, which offers both regulatory oversight and individual redress, India's framework appears fragmented and underdeveloped. This raises concerns about adequacy, especially in an era of increasing cross-border data flows and AI-driven decision-making.

8.5. Path Forward for India in Common Law Discourse

For India to strengthen its privacy protection framework, several paths are available. First, courts could more explicitly recognize privacy torts, drawing inspiration from Canadian jurisprudence or Prosser's four privacy torts in the U.S. Second, legislative reforms could integrate tort remedies with statutory provisions, ensuring individuals have access to damages alongside regulatory enforcement. Third, India could adopt a hybrid model where constitutional principles, tort law, and statutory data protection operate in tandem, offering layered protection against both private and state intrusions. Finally, India's leadership role in the Global South positions it to influence international privacy discourse, particularly in shaping equitable frameworks that balance technological innovation, surveillance, and individual rights.

9. Conclusion

Privacy is increasingly recognized as a fundamental right in the digital era, yet tort law in common law countries remains a limited and uneven mechanism for protection. This paper has shown that while tort-based doctrines such as Prosser's four privacy torts in the United States, misuse of private information in the UK, and intrusion upon seclusion in Canada offer important remedies, they often struggle to address modern harms like large-scale surveillance, algorithmic profiling, and cross-border data transfers. Difficulties in proving damages, high litigation costs, and the fragmented nature of judicial innovation weaken tort law's capacity to provide adequate and consistent safeguards in the digital age. The broader implication for common law jurisdictions is that tort law alone cannot ensure effective privacy protection. While judicial creativity, as seen in Canadian courts' recognition of intrusion upon seclusion, demonstrates adaptability, reliance on case-by-case evolution produces uncertainty. It leaves gaps compared to statutory regimes such as the GDPR, which provides more comprehensive rights and an enforcement mechanism. Hybrid models that combine tort remedies with statutory data protection frameworks appear to offer the most promise, particularly when aligned with constitutional guarantees and human rights principles. This layered approach not only strengthens individual remedies but also enhances systemic accountability. Looking ahead, global privacy protection debates highlight the importance of integrating common law traditions with international standards such as the ICCPR and UN privacy guidelines. Future reforms should focus on harmonizing tort law with statutory frameworks, encouraging courts to recognize new digital harms, and ensuring the availability of cross-border enforcement mechanisms. Ultimately, tort law remains a valuable but incomplete tool; its adequacy for the digital age depends on whether common law countries supplement it with proactive legislation, judicial innovation, and alignment with international human rights standards.

Acknowledgment: The author acknowledges XIM University, Bhubaneswar, for providing the infrastructure to conduct this research work.

Data Availability Statement: The data supporting this study are available from the corresponding author upon reasonable request, subject to privacy and ethical restrictions.

Funding Statement: This research received no financial support or external funding.

Conflicts of Interest Statement: The author declares no conflicts of interest related to this study.

Ethics and Consent Statement: This study was conducted by ethical standards and approved by the relevant institutional review board.

References

1. Justia, "Cox Broadcasting Corp. v. Cohn, 420 U.S. 469," *U.S. Supreme Court*, 1975. [Accessed by 12/05/2024].
2. Justia**,** "A. A. Dietemann, Appellee, v. Time, Inc., a New York Corporation, Appellant, 449 F.2d 245," 9th Cir. *U.S. Supreme Court*, 1971. [Accessed by 24/05/2024].
3. Court of Appeal for Ontario, "Jones v. Tsige, 108 O.R. (3d) 241, 2012 ONCA 32," *Court of Appeal for Ontario*, 2012. [Accessed by 22/05/2024].
4. South Asian Translaw Database, "Justice K.S. Puttaswamy vs. Union of India," *South Asian Translaw Database*, 2017. [Accessed by 14/05/2024].
5. Acts of Parliament, "The Digital Personal Data Protection Act, 2023, 9, No. 22," Acts of Parliament, 2023. [Accessed by 02/05/2024].
6. A. Jain and P. Waghre, "Internet Freedom Foundation Statement on the Digital Personal Data Protection Bill, 2023," *Internet Freedom Foundation*, 2023. [Accessed by 12/05/2024].
7. A. Murray, "Information Technology Law: The Law and Society," 5th ed. *Oxford University Press*, Oxford, England, United Kingdom, 2023.
8. LawTeacher, "Australian Broadcasting Corporation v. Lenah Game Meats," *LawTeacher*, 2001. [Accessed by 22/05/2024].
9. Australian Law Reform Commission (ALRC), "Serious Invasions of Privacy in the Digital Era," *Australian Law Reform Commission (ALRC)*, 2014. [Accessed by 25/05/2024].
10. B. Hawkes, "Annual Activity Report of the Data Protection Commissioner (2021)," *OECD*, 2022. [Accessed by 28/05/2024].
11. B. Rössler, "The Value of Privacy," *Polity Press*, Cambridge, United Kingdom, 2005.
12. C. J. Bennett and C. D. Raab, "The Governance of Privacy: Policy Instruments in Global Perspective," 1st ed. *Routledge*, London, England, United Kingdom, 2020.
13. C. Kuner, "Transborder Data Flows and Data Privacy Law," *Oxford Univ. Press*, Oxford, England, United Kingdom, 2013.
14. Justia, "Cantrell v. Forest City Publ'g Co., 419 U.S. 245," *U.S. Supreme Court*, 1974. [Accessed by 16/05/2024].
15. D. Butler, "A Tort of Invasion of Privacy in Australia?" *Melbourne University Law Review*, vol. 29, no. 9, pp. 339–389, 2005.
16. D. C. Chaffey, "The Right to Privacy in Canada," *Political Science Quarterly*, vol. 108, no. 1, pp. 117–132, 1993.
17. D. J. Solove and D. K. Citron, "Privacy Harms," *Boston University Law Review*, vol. 102, no. 2, pp. 793–864, 2021.
18. D. J. Solove, "A Taxonomy of Privacy," *University of Pennsylvania Law Review*, vol. 154, no. 3, pp. 477–564, 2006.
19. D. J. Solove, "Understanding Privacy," *Harvard Univ. Press*, Cambridge, Massachusetts, United States of America, 2010.
20. E. Barendt, "Freedom of Speech," *Oxford Univ. Press*, Oxford, England, United Kingdom, 2007.
21. E. Paton-Simpson, "Privacy and the reasonable paranoid: The protection of privacy in public places," *University of Toronto Law Journal*, vol. 50, no. 3, pp. 305–346, 2000.
22. European Data Protection Board (EDPB), "Guidelines 07/2020 on the Concepts of Controller and Processor in the GDPR," *European Data Protection Board (EDPB)*, 2021. [Accessed by 12/05/2024].
23. European Union, "General Data Protection Regulation (Regulation (EU) 2016/679)," 2016. [Accessed by 12/05/2024].
24. G. Bhatia, "Offend, Shock, or Disturb: Free Speech under the Indian Constitution," *Oxford University Press*, Oxford, England, United Kingdom, 2016.
25. G. Phillipson, "Transforming Breach of Confidence? Towards a Common Law Right of Privacy under the Human Rights Act," *The Modern Law Review*, vol. 66, no. 5, pp. 726–758, 2003.
26. H. Kastlová, "Report on Extraterritorial Enforcement of GDPR," *European Data Protection Board*, 2024. [Accessed by 18/05/2024].
27. House of Lords, "Judgments – Campbell (Appellant) v. MGN Limited (Respondents)," *House of Lords*, 2004. [Accessed by 12/05/2024].
28. J. Isaak and M. J. Hanna, "User Data Privacy: Facebook, Cambridge Analytica, and Political Profiling," *Computer*, vol. 51, no. 8, pp. 56–59, 2018.

29. J. S. Chandpuri and V. Kumar, "Emerging Trends in Law of Torts: An Overview," *International Journal of Law Management & Humanities*, vol. 5, no. 2, pp. 1178–1195, 2022.
30. K. Haggerty and R. Ericson, "The New Politics of Surveillance and Visibility," *University of Toronto Press*, Ontario, Canada, 2006.
31. L. H. Scholz, "Privacy Remedies," *Indiana Law Journal*, vol. 94, no. 2, pp. 653–688, 2019.
32. M. Hiloidhary and B. Deka, "Privacy and Data Protection in the Digital Era: Prospect & Challenges," *IJLLR Journal*, vol. 4, no. 2, pp. 1–14, 2022.
33. N. M. Richards and D. J. Solove, "Privacy's Other Path: Recovering the Law of Confidentiality," *Georgetown Law Journal*, vol. 96, no. 1, pp. 123–182, 2007.
34. O. Reis, N. E. Eneh, B. Ehimuan, A. Anyanwu, T. Olorunsogo, and T. O. Abrahams, "Privacy Law Challenges in the Digital Age: A Global Review of Legislation and Enforcement," *International Journal of Applied Research in Social Sciences*, vol. 6, no. 1, pp. 73–88, 2024.
35. O. Tambou, "Privacy and Data Protection Law in France," *Kluwer Law International*, Alphen aan den Rijn, Netherlands, 2024.
36. P. M. Schwartz and E. J. Janger, "Notification of Data Security Breaches," *Michigan Law Review*, vol. 105, no. 5, pp. 913–984, 2007.
37. P. M. Schwartz and K. N. Peifer, "Transatlantic Data Privacy Law," *Georgetown Law Journal*, vol. 106, no. 1, pp. 115–178, 2017.
38. P. Voigt and A. V. D. Bussche, "The EU General Data Protection Regulation (GDPR): A Practical Guide," *Springer*, Cham, Switzerland, 2017.
39. R. Gavison, "Privacy and the Limits of Law," *Yale Law Journal*, vol. 89, no. 3, pp. 421–471, 1980.
40. R. Wacks, "Privacy and Media Freedom," *Oxford Univ. Press*, Oxford, England, United Kingdom, 2013.
41. S. Livingstone, "The Complex Task of Improving Media Literacy," *LSE Business Review*, 2018. [Accessed by 12/05/2024].
42. S. T. Margulis, "Three theories of privacy: An overview," in Privacy Online, 1st ed. *Springer*, Berlin, Germany, 2011.
43. S. Zuboff, "The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power," *PublicAffairs*, New York, United States of America, 2019.
44. United Nations Human Rights Committee, "General comment No. 34 Article 19: Freedoms of opinion and expression," *United Nations Human Rights Committee*, 2010. [Accessed by 22/05/2024].
45. V. Bhandari and R. Sane, "Protecting citizens from the state post Puttaswamy: Analysing the privacy implications of the Justice Srikrishna Committee Report and the Data Protection Bill, 2018," *Socio-Legal Review*, vol. 14, no. 2, pp. 143-169, 2018.
46. V. Johnson, "Cybersecurity, Identity Theft, and the Limits of Tort Liability," *South Carolina Law Review*, vol. 57, no. 1, pp. 255-311, 2005.
47. W. Hartzog and N. M. Richards, "Privacy's Constitutional Moment and the Limits of Data Protection," *Boston College Law Review*, vol. 61, no. 5, pp. 1-17, 2020.
48. W. L. Prosser, "Privacy," *California Law Review*, vol. 48, no. 3, pp. 383–423, 1960.