# Navigating Privacy in the Age of AI: Evaluating the Adequacy of the GDPR and CCPA to Combat Data Exploitation and Deepfake Technology

**Alexandria Levitt**

*Received August 31, 2024*
*Accepted November 15, 2024*
*Electronic access December 30, 2024*

This study investigates the effectiveness of the GDPR and CCPA in addressing AI privacy challenges, mainly focusing on data exploitation and deepfakes. The rapid growth of AI and its reliance on personal data reveal gaps in legal protections. Through a comparative analysis, this paper examines whether existing laws are sufficient in combating the risks posed by deepfakes, highlighting the limitations in scope, enforcement, and practical application. The research uses a detailed comparative methodology, analyzing the legal frameworks of the GDPR and CCPA alongside recent legislative efforts targeting AI, such as the EU's AI Act and California's AB 602. Case studies of violations under both GDPR and CCPA were analyzed to provide real-world insights into how companies have responded to these laws. Findings reveal that while both the GDPR and CCPA offer baseline protections for personal data, neither framework is equipped to fully address the evolving threat of deepfakes. The GDPR's broader scope offers more potential for regulating AI-driven content, but its lack of specificity harms its practical application. Conversely, the CCPA's business-centric approach limits its effectiveness in regulating deepfake technology, especially when created or shared by individuals outside commercial contexts. This study concludes that clearer legal language and stronger enforcement methods are needed to address AI-specific risks. It suggests adopting strategies used in child protection laws and calls for further research into global approaches to regulating AI and privacy.

## Introduction

### Definitions of AI

According to the European Commission's Communication on AI, "Artificial intelligence (AI) refers to systems that display intelligent behaviour by analysing their environment and taking actions – with some degree of autonomy – to achieve specific goals."[1] By this broad definition, AI is an umbrella term that encompasses various subsets and technologies. When companies use AI, they are likely referring to Machine Learning (ML) algorithms, which are defined as "a subfield of artificial intelligence that gives computers the ability to learn without explicitly being programmed."[2]

Another pair of common AI buzzwords is "neural networks" and "deep learning". Neural networks are a subfield of machine learning and refer to machine learning algorithms meant to process data in a way that mimics neurons in the human brain. "Nodes" act as artificial neurons, processing data and producing outputs that have to exceed a certain threshold in order for the data to be passed on to the next set of nodes or "layer". Deep learning is a subfield of neural networks and refers to a neural network with three or more layers.[3] Deep learning models can learn from raw data with limited human intervention, automatically discovering patterns and representations such as images, text, and audio. This capability allows deep learning models to outperform simpler machine learning models in many applications, especially when dealing with high-dimensional data[4].

The two main types of AI that use machine learning algorithms that I'll be referencing in this paper are predictive AI and generative AI. Predictive AI uses machine learning to identify patterns from vast amounts of data and "predict" (hence the name) behaviors and future outcomes.[5] Generative AI uses machine learning trained on data sets in order to "generate" new content such as images, videos, and audio.[6]

### Current Privacy Threats

These machine learning algorithms mentioned above, both predictive and generative AI, rely on an abundance of data, "the more data, the better the program".[2] The foundation of AI is data and the success of the algorithm relies on the quality of the data it learns from. Data is also needed to continuously train a machine learning algorithm, meaning the algorithm is adapting and improving from the vast amounts of data used.[7]

The issue with AI's reliance on data is that as the use and importance of AI has grown, data has become a new form of currency. In this context, data holds significant value, can be

bought and sold, and the quality or amount of data can be linked to the AI's, and in turn the company's, success. This creates a competition for data and raises new issues over AI and privacy. Privacy concerns over data collection are not new. In the age of the Internet, tracking people's digital activity is easier than ever and that data gives companies valuable information about consumer preferences.[8] However, AI's thirst for data is unprecedented and the expansion of AI systems tests the limits of data collection privacy laws, many of which are obscure and inconsistent.

While not always intended, the methods for collecting this data can be deceptive and the possible uses malicious. Many companies utilize a "notice and choice" approach to data collection where individuals are informed (notice) about how their data will be used and are then given the opportunity to make decisions (choice) about whether or not to allow that data usage. However, the notice and choice approach often fails to provide proper protection to individuals who are frequently unaware of or unable to fully comprehend what they're agreeing to, especially with vague and complicated privacy notices.[9]

Additionally, when it comes to predictive AI particularly, if the data used to train AI is biased, the AI can produce unfair or discriminatory results. For example, Julie Angwin–a senior investigative reporter at ProPublica, a non-profit journalism organization—found that the Correctional Offender Management Profiling for Alternative Sanctions (COMPAS), an algorithm used to predict recidivism (relapse into criminal behavior)[10] in Broward County, Florida incorrectly labeled African-American defendants as "high-risk" at nearly twice the rate it mislabeled white defendants.[11] Furthermore, Amazon has conceded to the high possibility of AI bias after developing a hiring algorithm that unknowingly downgraded resumes with the word "women" as in "women's chess club captain" or "women's college".[12] Such biases perpetuate discrimination and deepen inequalities, eroding trust in institutions, creating economic disadvantages, and causing psychological harm to those unfairly targeted.

Lastly, one of the newest and arguably scariest threats posed by generative AI comes in the form of "deepfakes". The term deepfake (the blending of the words "deep learning" and "fake") refers to "a type of synthetic media that uses deep learning, a subset of machine learning, to generate or modify images, videos, or audio of a real or fictitious person's voice or likeness". The term deepfake was created by a 2017 Reddit user with the handle 'deepfakes' who released videos of female celebrities edited into pornography.[13] Deepfakes can be used for defamation, identity theft, or manipulating elections. Those depicted can suffer mental damage, face threats of violence if the video creates public outrage, be exploited, and have their reputations destroyed.[14]

One significant threat posed by deepfakes is the creation of explicit content, disproportionately targeting women. This form of abuse affects a wide range of individuals, including celebrities, everyday people, and even minors. In October of 2023 reportedly more than 30 girls at Westfield High School in New Jersey were victims of deepfake pornography, one of which was 15-year-old Francesca Mani. Boys at their school had taken photos of these high school girls and digitally manipulated them using AI. Horrified, Francesca spoke out, inspiring a movement for deepfake legislation in New Jersey and demonstrating the true dangers of AI deepfake content.[15]

Another significant threat of deepfakes lies in their potential for political manipulation. For example, during New Hampshire's 2024 presidential primary, some voters reported receiving recorded calls meant to sound like Joe Biden and attempting to persuade them not to vote. While not actually affecting the election, the AI phone call from Joe Biden opens up the possibilities for more damaging political deepfakes.[16] Such deepfakes can be weaponized to misrepresent a politician's actions, damaging reputations, influencing voter behavior, and furthering distrust in the media.

## Overview of the GDPR and CCPA

**The GDPR:** Most US privacy laws prioritize individual control through a "notice and choice" approach which gives users the option to opt-out or stop doing business with a company. In contrast, the EU's General Data Protection Regulation (GDPR) requires explicit consent, meaning users choose to opt in.[14] Passed in 2016 and in effect by 2018, the GDPR is considered one of the most significant pieces of personal data protection legislation in the world.[8]

**The CCPA:** In the US, on the other hand, there is no nationwide privacy legislation comparable to the GDPR. Instead, 12 states in the US have passed their own privacy legislation, the most notable being California's Consumer Privacy Act (CCPA). Going into effect in 2020, the original CCPA allowed people to access, delete, and move their data and allowed them to opt-out of having their data sold every two years. It also required businesses to state what data they collect and to only use that data for their stated purposes. The CCPA was updated in 2022 by the California Privacy Rights Act (CPRA), taking data protection a step further[8]. In this paper when I refer to the CCPA this also includes the adjustments of the CPRA.

## Research Question

This paper compares and contrasts the GDPR and the CCPA in order to answer the question: How do the GDPR and CCPA handle the privacy threats posed by AI-driven data exploitation and deepfake technologies, and what reforms are needed?

## Methods

This paper is a literature review, requiring an analysis of numerous research papers focused on AI privacy, the GDPR, and the CCPA. The papers included were found through key searches using phrases like "GDPR AI privacy," "CCPA data protection," "AI deepfakes legislation," and "privacy law enforcement AI" in databases such as Google Scholar, JSTOR, and HeinOnline. Some of the papers reviewed were case studies on privacy violations, while others provided comparative legal analyses. To learn about the specific details of the GDPR and CCPA I directly reference the legal documents.

The papers selected are from 2014 to 2024, ensuring a comprehensive view of the most relevant and current research. The oldest paper is from 2014, but the majority are from 2018 or later. In total, 49 sources were selected for the review, chosen based on their relevance to AI privacy and how they discussed the legal frameworks of GDPR and CCPA. Snowball tracking was performed to make sure no critical papers were missed, to verify the findings, and to expand the number of sources used.

The main objective of this review was to evaluate the effectiveness of these regulations in addressing AI-driven privacy concerns, especially the rising issues around deepfakes and data exploitation.

## Results

### Comparative Analysis of GDPR and CCPA for data protection

A: Scope and Definitions

**The GDPR:** The GDPR applies to any entity that processes personal data. This includes what the GDPR calls "data controllers" (entities that determine the purpose and means of data processing) and "data processors" (entities that process data on behalf of a controller). The GDPR applies to all entities that operate within the EU, including non-european organizations if the organization is operating in a location where EU laws apply. The GDPR also applies to entities outside the EU if said entities process the personal data of individuals located in the EU, including offering goods or services to individuals in the EU, even if no payment is involved, and monitoring behavior of individuals in the EU, such as tracking their online activities. [17] By this scope the entities that must adhere to the GDPR can include for-profit businesses, non-profit organizations, government agencies, etc. as long as they handle personal data in some way, such as collecting, storing, or using. Under the GDPR "personal data" is defined as "any information relating to an identified or identifiable natural person", including "a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person". In non-legal language this means that personal data is anything that can be used to identify a person. "Processing", on the other hand, refers to "any operation or set of operations which is performed on personal data or on sets of personal data", including–but not limited to–"collection, recording, storage, and alteration". [18]

**The CCPA:** The CCPA on the other hand does not apply to all entities that process data but instead applies solely to "businesses". The CCPA specifically defines a "business" as any legal entity that operates for profit and collects personal information from consumers in California. To qualify, the business must meet one or more of these criteria: (1) Have annual gross revenues exceeding $25 million; (2) Buy, sell, or share personal information of 100,000 or more consumers or households; or (3) Derive 50% or more of its annual revenue from selling or sharing personal information. [19]

Under the CCPA the definition of "personal information" is almost identical to the GDPR's definition of "personal data" in the sense that it refers to any data that can be used to identify a person. Along with listing similar examples to the GDPR like "a real name, alias, postal address, unique personal identifier, online identifier" and others, the CCPA goes on to specify further types of personal information such as biometric information, network activity, geolocation data, employment information, education information, and any inferences made from a person's information to create a profile about their preferences, traits, behavior, and abilities. [19] While this type of personal information would likely be considered "personal data" under the GDPR—since all the types specified by the CCPA can identify a person under the GDPR's definition—the CCPA is more detailed by explicitly listing the types of information protected. Furthermore, the CCPA specifies what is not included under their definition of "personal information", including publicly available information, lawfully obtained truthful data, or de-identified and aggregated data. Publicly available information comes from government records or widely accessible media, however "publicly available" does not mean biometric data collected without the consumer's knowledge. [19]

The CCPA also defines a category called Sensitive Personal Information, which includes: information such as a consumer's social security number, driver's license, financial account details, or precise geolocation; personal details like racial or ethnic origin, immigration status, religious beliefs, union membership, and the contents of private communications; and sensitive data such as genetic information, biometric data used for identification, and personal infor-

mation related to health, sex life, or sexual orientation.[19]

B: Rights Granted

**The GDPR:** As specified by the GDPR, the user or "data subject" has a set of guaranteed rights involving their data. While the GDPR specifies several rights, here I will explicitly explain three main ones. The first is the "right to information", meaning a company (the "controller") must provide data subjects with specific information before processing their data. In brief, this information includes:

- The identity and contact information of the controller and their representative, if applicable.
- The contact information for the data protection officer, if there is one
- The purpose for processing the data and the legal basis for doing so
  *If the controller plans to use the data for a different purpose, they must inform the data subject beforehand
- The recipients of the data
- Details about any transfer of data outside the EU and the protections in place
- How long the data will be stored
- Their rights as a data subject to access, rectify, or erase personal data, object to processing, and request data portability
- The right to withdraw consent at any time
- The right to file a complaint
- Whether providing the data is mandatory and the consequences of not providing it
- Information about any automated decision-making, including profiling, and its implications.[20]

The second right is the "right to rectification" which simply means the right of a data subject to correct inaccurate data and the right to complete incomplete data.[21] For example, a user of a social media site discovers their age is documented incorrectly which is affecting the type of content they see. That user has the right to correct that information by contacting the company.

The third right is the "right to erasure" otherwise known as the "right to be forgotten". A data subject can request a data controller delete their data if the data is no longer needed for the original purpose, if they no longer consent to the processing of their data, or if the data has been unlawfully processed. However, there are exceptions such as if the use of the data is considered freedom of expression, complies with legal obligations, is necessary for public health, is kept for scientific research, or is required for legal claims.[22]

**The CCPA:** Again, the CCPA is almost identical to the GDPR when it comes to the rights granted to what the CCPA calls "consumers". The right to delete, the right to opt-out, and the right to correct are similar to the GDPRs right to erasure, right to withdraw consent, and the right to rectification respectively. It is important to note the CCPA's right to opt-out refers to the right to opt out of the sale or sharing of personal data, while the GDPR's right to withdraw consent refers to not just the sale but the processing of data. The CCPA also grants consumers the right to know, which is similar to the GDPR's right to be informed with one major difference. While the GDPR's right to be informed requires disclosure of information before processing, the CCPA's right to know requires disclosure primarily upon request, meaning consumers must take the initiative to ask for this information[23]. When examining whether or not data subjects/consumers are more informed, the GDPR better informs and protects the data subjects because the GDPR shifts the responsibility from users onto organizations to ensure users are informed. CCPA consumers are likely less informed than GDPR data subjects because not all users, most likely very few, are going to go out of their way to request this information.

The CCPA grants consumers an additional right called the right of no retaliation, which ensures that businesses cannot discriminate against consumers who exercise their rights under the CCPA, including, but not limited to: (1) Denying goods or services, (2) Charging different prices or rates, (3) Offering different levels or quality of goods or services, or (4) Retaliating against employees or contractors for exercising their rights. However, businesses can offer financial incentives (such as discounts or rewards) in exchange for the collection or sale of personal information, as long as these incentives are reasonably related to the value of the consumer's data. Consumers must opt in to these incentives voluntarily, and they must be able to revoke their consent at any time[23] Conversely, the GDPR does not have an equivalent right granted to data subjects, but does specify in Article 7 that consent must be "freely given" and that a company can't make a service dependent on consent to process data that isn't needed for that service.[24] Article 12 also declares that any information provided or communication and actions taken under the articles that grant data subject rights (Articles 13-23  34) shall be provided "free of charge".[25] Although initially it may seem like the CCPA better protects consumers because of it's right of no retaliation, the GDPR does indirectly prevent discrimination and unlike the CCPA has no provision allowing companies to provide incentives for consent. So while the CCPA adds a valuable non-discrimination right,

due to the GDPR requiring proactive transparency versus the CCPA's reliance on consumer action and allowance of consent incentives, the GDPR can be seen as more protective of individuals' privacy while the CCPA can be seen as more business-centric.

C: Case Studies

Since the implementation of privacy regulations like the GDPR and CCPA, companies have had to become more transparent and secure in the way they collect data, or else face the consequences.

**The GDPR:** This can be seen in the 2019 case where a French data protection regulator, the Commission Nationale de l'Informatique et des Libertés (CNIL), fined Google €50 million (almost $57 million) for violating the GDPR.[26] The CNIL claimed the fine was levied for "lack of transparency, inadequate information and lack of valid consent regarding ads personalisation". The regulator said that because Google spread relevant privacy information across several documents, often requiring five or six actions, users couldn't properly understand the extent of Google's processing operations and therefore failed to reach the level of transparency required by the GDPR. The regulator also claimed Google did not gain valid consent since the box agreeing to personalized ad content was "pre-ticked" when users created their account, going against the GDPR's opt in policy.[27] In this case, the $57 million Google was fined fell well below the maximum fine of the GDPR—4% of the company's global revenue, which for Google was more than $4 billion. For Google the size of this fine makes little impact, but the case itself demonstrates a success of the GDPR because it means Google cannot collect personal data and build advertising profiles of people until the privacy laws of the GDPR are properly followed.

In 2021, the CNIL also fined Clearview AI for violating GDPR regulations. Clearview AI is a facial recognition technology company based in the United States. Clearview AI was fined €20 million (almost $24 million) after the CNIL found they had been collecting and processing biometric data, which is considered personal data, without the consent of individuals and therefore in clear violation of the GDPR.[26] When the CNIL was first alerted of the violations, they issued a formal notice to Clearview AI giving them the opportunity to cease the collection of the biometric data and comply with the individuals requests of erasure. After two months Clearview AI did not respond to the notice and the matter was instead referred to a restricted committee who imposed the maximum fine. Clearview AI was then ordered to cease the collection of biometric data and delete the data they had already collected within two months.[28] This case of Clearview AI demonstrates a successful protection of individual privacy by combating the nonconsensual use of personal data for AI training sets, protecting individuals not just from data violations, but also from the possible creations of unwanted inferences and deepfakes.

**The CCPA:** In the United States the CCPA also had a significant impact on business's data collecting and handling practices. In 2021, Zoom paid $85 million dollars for violating the CCPA by sharing users' personal information with Google, Facebook, and LinkedIn and for not properly defending against Zoombombing, a practice where hackers disrupt Zoom meetings. Zoom also agreed to create and enforce new data protection measures and provide data-handling training to its employees.[29]

In 2024, DoorDash agreed to pay $375,000 for the violation of the CCPA through the selling of customers' personal data without proper notice or an option to opt out. The issue arose when DoorDash participated in marketing cooperatives, where businesses shared customer information for advertising purposes. However, the data was improperly shared with companies outside the cooperative and a data broker, who resold the data multiple times. As part of the settlement, DoorDash must now review vendor contracts, monitor data sharing, and submit annual reports to ensure compliance.

Also in 2024, Sephora paid $1.2 million after failing to disclose the sale of customer's personal data, to process opt-out requests made through Global Privacy Control (a common tool that helps users opt-out of the sale of their personal data), and to fix these issues within the required 30-day period. As part of the settlement, Sephora must update its privacy policies, allow consumers to opt out via mechanisms like the Global Privacy Control, ensure its service agreements comply with the CCPA, and provide reports to the Attorney General.

In the mentioned cases, the CCPA has been successful in holding companies accountable forcing businesses to update their privacy policies, enhance transparency, and implement better data-handling practices. This shift has pushed companies to prioritize consumer privacy, indicating the CCPA's positive influence in promoting responsible data collection and use.

## Comparative Analysis of the GDPR and the CCPA for deepfakes

A: Scope and Definitions

Neither the GDPR nor the CCPA explicitly mention deepfakes. In fact, it's questionable if deepfakes even fall under the scope of the GDPR and CCPA. However, the use of personal data to create deepfakes arguably constitutes them

as "personal data" and therefore the GDPR and CCPA can apply.

**The GDPR:** As discussed in Results section 1.A, the GDPR applies to any processing of personal data. The creation of a deepfake requires the processing, or at least collection and alteration (included in the GDPR's definition of processing), of data. Therefore, deepfakes where a person is identifiable can be considered "personal data" and under the jurisdiction of the GDPR.

However, the GDPR contains an exemption that states the GDPR does not apply to the processing of personal data "by a natural person in the course of a purely personal or household activity".[30] But, as Martijn van der Helm argues, there are two cases that indicate that household activities where the data is collected from a public source or published on social media may fall under the GDPR. The first is the František Ryneš case where Mr. Ryneš used CCTV cameras to capture footage of burglars entering his home for personal security. However, the Court of Justice of the EU (CJEU) determined that the household exemption under EU data protection law did not apply because the images were collected from a public domain. This ruling indicates that if personal data used in creating the deepfake comes from public sources, the exemption may not apply. The second is a Dutch court case, where a mother filed a complaint against the children's grandmother for posting pictures of her grandchildren online without consent. The court found insufficient evidence that the grandmother had restricted access to her account. Since it couldn't be determined if the images were shielded from public view or third-party access, the court ruled that the exemption did not apply and ordered the grandmother to remove the photos. The GDPR would be used to combat deepfakes that are intentionally available to the public with third-party access, therefore, based on this ruling it is likely the GDPR does apply to deepfakes.[31]

**The CCPA:** For the same reasons deepfakes would be considered personal data under the GDPR, they'd also be considered personal information under the CCPA. If a business creates or distributes deepfakes using identifiable personal data, the business is required to comply with the CCPA's transparency and consumer rights provisions. This includes informing consumers about the data collected, its intended use, and their rights regarding that data, such as the right to know, delete, and opt-out of the sale of personal information.

Unlike the GDPR, which applies to all entities processing personal data, the CCPA specifically targets for-profit businesses. This means that deepfakes created and distributed by individuals acting outside of a business context would likely not fall under the CCPA's jurisdiction. Therefore, the CCPA could only be possibly applied to deepfakes created or distributed by a business, and not an individual, which leaves the CCPA less effective than the GDPR in combating deepfakes. Even then, the lack of specific definitions, policy, and true cases around deepfakes means that both the GDPR and CCPA are likely not effective at addressing the threats of deepfakes and there is a need for better, more specific regulation.

B: Other Regulations

Since the creation of the GDPR and the CCPA, newer, more specific laws that explicitly address deepfakes have been created in their respective areas.

**The EU:** The GDPR helped pave the way for the EU's AI Act. Rather than data privacy, the AI Act specifically regulates AI technologies and aims to protect health, safety, and democratic values.[32] Unlike the GDPR, the AI Act specifically defines deepfakes as "AI-generated or manipulated image, audio or video content that resembles existing persons, objects, places, entities or events and would falsely appear to a person to be authentic or truthful".[33]

Article 50 discusses policy around deepfakes. Article 50 specifies that companies must clearly inform users when they are interacting with an AI system, except when the use is obvious or authorized for legal reasons, such as crime detection. Additionally, any outputs from AI systems that generate synthetic content, including deepfakes, must be marked as artificially created in a machine-readable format. This ensures that users recognize when content has been manipulated. However, Article 50 will not be enacted until 2026[34] and while deepfakes are acknowledged within the Act, there are no specific enforcement mechanisms or criminal penalties associated solely with their use. The primary purpose is to ensure that such content is labeled appropriately to promote transparency and prevent misuse.

**California:** After the enactment of the CCPA, California passed two laws to address deepfakes: AB 602 and AB 730. AB 602, also known as "Depiction of Individual Using Digital or Electronic Technology: Sexually Explicit Material: Cause of Action" allows a victim to seek legal action against a person who creates and/or intentionally distributes sexually explicit content when they reasonably should have known the depicted individual did not consent. They can recover the defendant's monetary gains, economic and emotional distress damages, or statutory damages ranging from $1,500 to $30,000 (up to $150,000 if the act was malicious). Plaintiffs may also seek punitive damages, attorney's fees, and injunctive relief. The lawsuit must be filed within three years of discovering the unauthorized material. AB 602 applies to all individuals, public or private.[35]

AB 730 on the other hand applies explicitly to candidates running for elected office. AB 730 expired on January 1, 2023 and was an amendment known as 'Deceptive Audio or Visual Media to California's Election Law." It expanded the definition of deepfakes to audio and visual manipulation in order to protect candidates from media where their essence has been intentionally manipulated to falsely appear authentic and impact the public's perception of the candidate.[36]

C: Issues With Enforcement

While these regulations theoretically offer some recourse for victims of malicious deepfakes, enforcement is complicated. These AI-generated manipulations integrate personal data into fabricated content, making it difficult to isolate and remove specific data points, particularly when dealing with unstructured data like voice and facial features. Additionally, the viral nature of deepfakes means they can quickly spread across multiple platforms and jurisdictions, rendering traditional removal efforts often ineffective.[37]

Furthermore, the responsibility for removing harmful content often falls on the victims, who must navigate a tedious process of contacting individual data controllers and persuading reluctant platforms to take action. This process is not only inefficient but also costly and time-consuming. Victims often need to engage lawyers, further compounding the financial and emotional burden.[38]

The GDPR and CCPA's right to erasure or right to delete, while theoretically strong, are difficult to assert in practice. The procedural complexities and the lack of guaranteed success in removing content may discourage many victims from pursuing their rights.[38] These gaps highlight the need for more effective and streamlined mechanisms to address the pervasive issue of deepfakes and their misuse.

## Problems and Solutions

A: Data Protection

**Consent Fatigue:** The GDPR and the CCPA have increased the frequency and complexity of consent requests. Under the GDPR, organizations are required to obtain explicit, informed consent from individuals before processing their personal data. This involves providing clear information about the data being collected, the purposes of processing, and the rights of the individuals.[24] Similarly, the CCPA requires businesses to provide consumers with the option to opt-out of the sale of their personal information, particularly through 'Do Not Sell My Personal Information' links, and mandates privacy notices,[23] thereby increasing privacy-related interactions.

This surge in consent requests has led to a phenomenon known as "consent fatigue," where individuals become overwhelmed by the sheer volume of consent forms and notifications.[39] Studies show that most people do not read privacy notices due to their complexity and length. Even if users attempt to read them, they often find the language vague or ambiguous, leading to a lack of true understanding.[40]

Addressing consent fatigue requires organizations to adopt strategies that make the consent process more user-friendly. The UK's Information Commissioner's Office (ICO) recommends using clear, plain language in consent requests and ensuring that they are prominent and separate from other terms and conditions.[41] Another approach is a differentiated consent system, where explicit consent is only required for high-risk data processing activities, and implied consent is allowed for lower-risk scenarios. Schermer suggests that this model would reduce the number of consent prompts and make them more meaningful when they do appear.[39]

Nonetheless, Solove contends that informed consent in privacy law remains nearly impossible. Simplifying language and implementing differentiated consent may help, but they do not fully address the underlying issues of consent fatigue and limitations of individual understanding.[40]

**Vague Language:** The vague language in privacy regulations like the GDPR and CCPA can create significant challenges for businesses trying to implement effective data protection measures. A common issue is the ambiguity surrounding the principle of "privacy by design". Article 25 of the GDPR requires data controllers to integrate data protection into their processing activities, but many businesses find the lack of specificity regarding what constitutes adequate compliance leaves them uncertain about how to implement these principles effectively. Additionally, the lack of clarity may lead to superficial compliance and allow companies to avoid meaningful privacy protections.[42]

Updates to the GDPR and other regulations could include clearer and more detailed requirements for implementing privacy protections. Specifically, the article should outline precise actions that companies need to take to integrate privacy measures into their technology and business practices from the ground up. This means that the GDPR should specify how privacy by design should be incorporated into the development of products and services, such as embedding data protection features directly into software, conducting regular privacy impact assessments, and ensuring that privacy considerations are part of every stage of product development and operational processes. By providing concrete guidelines and expectations, the updated article would help prevent companies from merely performing

| Aspect | **GDPR (General Data Protection Regulation)** | **CCPA (California Consumer Privacy Act)** |
|---|---|---|
| Scope | Applies to all organizations processing personal data of EU residents, regardless of the company's location. | Targets for-profit businesses that meet specific financial thresholds and handle data of California residents. |
| Personal Data Definition | Defines personal data as any information relating to an identifiable individual (including name, location, online identifiers, etc.). | Similar definition to GDPR, with explicit mention of categories like geolocation, biometric data, and Sensitive Personal Information (SPI) such as health and financial data. |
| Consumer Rights | Provides rights such as access, correction, erasure ("right to be forgotten"), data portability, objection to processing, and mandatory breach notification within 72 hours. | Grants rights to know what data is collected, request deletion of personal data, opt-out of data sales, and be notified of data breaches, but with no specified time frame for breach notifications. |
| Consent | Requires explicit, informed consent from individuals before processing personal data. Opt-in model. | Does not require consent for data collection, but consumers can opt-out of data sales. Opt-out model. |
| Penalties for Non-compliance | Can impose fines up to €20 million or 4% of a company's annual global revenue, whichever is higher. | Fines range from $2,500 per unintentional violation to $7,500 per intentional violation. |
| Global Reach | Applies to any entity processing EU citizens' data, regardless of its location. | Only applies to businesses processing data of California residents. |
| Enforcement Mechanisms | Enforced by national Data Protection Authorities in EU member states. | Enforced by the California Attorney General and consumers via private rights of action. |
| Deepfakes | The GDPR can apply to deepfakes if personal data, like someone's likeness or voice, is used. However, enforcement is challenging, especially when content spreads quickly across borders. It lacks explicit deepfake-specific provisions. | The CCPA does not explicitly address deepfakes, but if a business uses identifiable personal data to create deepfakes, it could fall under CCPA regulation. California's AB 602, passed separately from CCPA, provides more direct protection by allowing victims of deepfake pornography to take legal action. |

**Table 1** Summary Table on GDPR vs CCPA

minimal, symbolic compliance, and instead drive them to make substantial and effective changes that genuinely protect user data. This approach aims to move beyond a basic check-box compliance to a deeper, systemic integration of privacy into corporate practices.[42]

**The Right to Erasure:** The right to erasure is difficult to comply with when the data is being used by an AI system. These systems learn and improve their performance by analyzing and using data over time. Even after the original data is no longer directly accessed, the patterns learned from that data remain in the AI's model. This poses a problem for the right to "be forgotten" because deleting the original data does not remove the influence it had on the model. Additionally, databases use a tree structure to organize data efficiently, with each node representing a piece of information and branches connecting related data. When data is deleted, it's marked as removed but not immediately erased from storage. Instead, the space taken up by deleted data is eventually reused for new information, which means that deleted data might still be present in the system longer than intended, complicating efforts to fully comply with privacy regulations[43].

There are several technologies being explored to address this. The first is differential privacy, a technique that protects individual data by adding "noise" or small, random modifications to the data. "Noise" protects individual privacy by preventing the AI from relying on exact details. By using "noisy" data, the AI learns general patterns

rather than specific information, so if someone's data is deleted, the system's performance remains unaffected because it wasn't dependent on precise individual data to begin with.[44] Another proposed solution is federated learning. In federated learning, instead of collecting raw data, only what the model learned from the data (called model updates) is sent to a central server, keeping individual information private. This way, even if the original data on the device is deleted, the model keeps the patterns it learned from that data. This means the data itself is gone, but the model still benefits from the knowledge it gained during training, which can't be easily removed.[45]

B: Deepfakes

**Detection:** Oddly enough a strong solution for detecting AI generated content is more AI, specifically machine learning models. There are three prominent approaches that use AI to detect deepfakes, each help with detection in a different way:

Neural Architecture Search (NAS) is an automated process that identifies the optimal neural network arrangement for detecting deepfake content. This technique allows AI systems to outperform traditional human-designed models by focusing on subtle inconsistencies in deepfake videos, such as unnatural facial movements or inconsistent lighting. NAS-based models, when trained on datasets, have achieved an accuracy of 99.37%, making them particularly effective for detecting sophisticated deepfakes.[46]

Multimodal fusion is a technique that helps detect deepfakes by combining multiple types of data, like visual cues (e.g., facial expressions, movements) and audio cues (e.g., voice patterns, tone). This approach makes the detection process more reliable because deepfakes often manipulate both video and audio.[46]

Generative Adversarial Networks (GANs) are a type of AI that can both create and detect deepfakes. GAN-based models generate fake examples and teach the AI to recognize the patterns that make a video or image a deepfake.[46]

**Enforcement:** I also argue that established frameworks for child pornography laws could help enforce deepfake regulations across various jurisdictions.

The methods used to combat child sexual abuse material (CSAM), such as PhotoDNA, AI detection tools like Google's Content Safety API, and cross-platform collaboration among social media companies and law enforcement, offer an effective model that could be applied to deepfake detection. Currently, PhotoDNA uses hashing technology to create a unique digital fingerprint for known illegal content, which enables platforms to quickly identify and remove previously flagged material by matching hashes.[47]

For deepfake enforcement, I believe a similar hashing technique could be used to detect and remove known harmful deepfakes, allowing for rapid identification and enforcement across platforms. This hashing-based system ensures that once a harmful deepfake is identified, it can be quickly taken down across the internet.

However, deepfake technology presents a unique challenge because new and sophisticated deepfakes are constantly being created. This is where AI tools like Google's Content Safety API come into play. Google's AI tools, for example, have been used to detect previously unseen CSAM by learning patterns of abuse material, and this approach can be extended to flagging new deepfakes in real-time.[48] Unlike hashing, which only identifies known material, AI can proactively detect new, unseen deepfakes by analyzing the patterns and characteristics commonly found in manipulated videos. This allows AI to flag suspicious content even if it has not yet been flagged.

Cross-platform collaboration could also help with deepfake enforcement, just as in child pornography cases. In child protection, organizations like the International Association of Internet Hotlines (INHOPE) and the Internet Watch Foundation (IWF) work with platforms and law enforcement to track, remove, and trace illegal content across multiple sites.[49] Applying this same model to deepfakes could help with unified, faster detection and removal of harmful content globally.

## Conclusion

The findings of this research clearly indicate that both the GDPR and CCPA provide some level of protection against the privacy threats posed by AI technologies, but significant gaps remain such as unclear language, challenges with the right to erasure, and weak enforcement of deepfake laws. The GDPR's broad definitions of "personal data" and "processing" offer more comprehensive protection than the CCPA, which limits its application to for-profit businesses and places more responsibility on consumers. However, neither regulatory framework directly addresses the growing threat of deepfakes. This issue, while recognized in more recent laws like California's AB 602 and the EU's AI Act, still faces significant challenges in enforcement, particularly regarding the quick dissemination of deepfake content across jurisdictions.

To enhance protection, this paper suggests adopting more specific legislative language that clearly defines and addresses deepfakes, similar to the provisions seen in recent laws such as the EU's AI Act and California's AB 602. By explicitly categorizing deepfake technology and its potential abuses, lawmakers can create more targeted and effective regulations. Furthermore, this study advocates for the application of enforcement strategies

modeled after existing child pornography laws. Techniques such as hashing technology and AI detection tools, which have been successful in identifying and removing illegal content, could be adapted to track and eliminate harmful deepfakes. Cross-platform collaboration and international cooperation, as seen in child protection efforts, could also help manage the spread of deepfakes across different jurisdictions.

While the research objectives of comparing GDPR and CCPA were met, the analysis uncovered critical gaps that were not initially anticipated, particularly regarding the enforcement of deepfake-related privacy violations. This indicates a need for further research into how different legal systems worldwide are approaching this issue and the feasibility of establishing a global standard for deepfake regulation.

The limitations of this study include a primary focus on the GDPR and CCPA, which may not capture the full range of global regulatory responses to AI threats. Additionally, the ever-evolving nature of AI technology means that legislative measures must be continually updated to remain effective. The complexities involved in removing deepfakes once they have been disseminated further complicate enforcement efforts.

In conclusion, while the GDPR and CCPA lay important groundwork for data protection, they are insufficient in addressing the specific and emerging threats posed by AI technologies like deepfakes. To mitigate these risks, it is crucial for policymakers to implement clearer, more detailed legal standards and to adopt enforcement mechanisms proven effective in other areas of digital content regulation. Only through such proactive and comprehensive measures can we hope to protect individual privacy rights in an increasingly AI-driven world.


### Acknowledgments

I would like to thank to the Lumière Program for providing me with the opportunity to engage in this research. I am also grateful to Erin Cooper for her mentorship and support throughout this process.


## References


1 *Communication from the Commission to the European Parliament, the European Council, the Council*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A237%3AFIN.

2 S. Brown, *Machine Learning, Explained*, https://mitsloan.mit.edu/ideas-made-to-matter/machine-learning-explained.

3 I.B.M., *What Is a Neural Network?*, https://www.ibm.com/topics/neural-networks.

4 C. Janiesch, P. Zschech and K. Heinrich, *Machine learning and deep learning*.

5 I.B.M., *What Is Predictive AI?*, https://www.ibm.com/topics/predictive-analytics.

6 *Artificial Intelligence: Overview, Recent Advances, and Considerations for the 118th Congress*, https://crsreports.congress.gov/product/pdf/R/R47644.

7 C. Tschider, *AI'S LEGITIMATE INTEREST: TOWARDS A PUBLIC BENEFIT PRIVACY MODEL*.

8 J. King and C. Meinhardt, *Rethinking Privacy in the AI Era*, https://hai.stanford.edu/sites/default/files/2024-02/White-Paper-Rethinking-Privacy-AI-Era.pdf.

9 C. Tschider, *MEANINGFUL CHOICE: A HISTORY OF CONSENT AND ALTERNATIVES TO THE CONSENT MYTH*.

10 Merriam-Webster, *Recidivism*, https://www.merriam-webster.com/dictionary/recidivism.

11 J. Silberg and J. Manyika, *Notes from the AI Frontier: Tackling Bias in AI*, https://www.mckinsey.com/featured-insights/artificial-intelligence/tackling-bias-in-artificial-intelligence-and-in-humans, and in Humans).

12 E. Albaroudi, T. Mansouri and A. Alameer, *A Comprehensive Review of AI Techniques for Addressing Algorithmic Bias in Job Hiring*.

13 E. Meskys, A. Liaudanskas, J. Kalpokiene and P. Jurcys, *Regulating deep fakes: legal and ethical considerations*.

14 M. Helm, *Harmful Deepfakes and the GDPR*, https://arno.uvt.nl/show.cgi?fid=156861.

15 T. Ryan-Mosley, *Meet the 15-Year-Old Deepfake Victim Pushing Congress into Action*, https://www.technologyreview.com/2023/12/04/1084271/meet-the-15-year-old-deepfake-porn-victim-pushing-congress/.

16 J. Han, *New Hampshire Is Investigating a Robocall That Was Made to Sound like Biden*, https://www.npr.org/2024/01/22/1226129926/nh-primary-biden-ai-robocall.

17 E. Parliament and Council, *Regulation (EU) 2016/679 of the European Parliament and of the Council of*.

18 *GDPR*.

19 *CALIFORNIA CONSUMER PRIVACY ACT OF 2018*.

20 *GDPR*.

21 *GDPR*.

22 *GDPR*.

23 C.C.P.A., *Section 1798.100-1798.125*.

24 *GDPR*.

25 *GDPR*.

26 D. EMAIL and C.O.M.P.L.I.A.N.C.E., *30 Biggest GDPR Fines So Far (2020*, https://www.tessian.com/blog/biggest-gdpr-fines-2020/.

27 C. Fox, *Google Hit with £44m GDPR Fine over Ads*, https://www.bbc.com/news/technology-46944696.

28 E. D. P. Board, *The French SA Fines Clearview AI EUR 20 Million*, https://edpb.europa.eu/news/national-news/2022/french-sa-fines-clearview-ai-eur-20-million_en.

29 J. Stempel, *Zoom Reaches $85 Mln Settlement over User Privacy, 'Zoombombing'*, https://www.reuters.com/technology/zoom-reaches-85-mln-settlement-lawsuit-over-user-privacyzoombombing-2021-08-01/.

30 *GDPR*.

31 M. Helm, *Harmful deepfakes and the GDPR how data protection legislation should be used to address issues revolved around the harmful use of deepfake technology*.

32 *European Parliament*.

33 *AI Act*.

34 *AI Act*.

35 C. S. Legislature, *Assembly Bill No. 602, Depiction of Individual Using Digital or Electronic Technology: Sexually Explicit Material: Cause of Action*.

36 *California State Legislature. Assembly Bill No. 730, Elections: deceptive audio or visual media*.

37 F. Moreno, *Generative AI and deepfakes: a human rights approach to tackling harmful content*.

38 K. Mania, *Legal Protection of Revenge and Deepfake Porn Victims in the European Union: Findings From a Comparative Legal Study*.

39 B. Schermer, B. Custers and S. Hof, *The Crisis of Consent: How Stronger Legal Protection May Lead to Weaker Consent in Data Protection*.

40 D. Solove, *MURKY CONSENT: AN APPROACH TO THE FICTIONS OF CONSENT IN PRIVACY LAW*.

41 *Information Commissioner's Office*, https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/lawful-basis-for-processing/consent/.

42 A. Waldman, *Data Protection by Design? A Critique of Article 25 of the GDPR*.

43 A. Kesa and T. Kerikmäe, *Artificial Intelligence and the GDPR: inevitable nemeses?*

44 C. Dwork and A. Roth, *The Algorithmic Foundations of Differential Privacy*.

45 B. McMahan, E. Moore, D. Ramage and S. Hampson, *Communication-Efficient Learning of Deep Networks from Decentralized Data*.

46 J. Ng, S. Chong and K. Wee, *Enhancing Deepfake Detection for Public Awareness*.

47 Microsoft, *PhotoDNA*, https://www.microsoft.com/en-us/photodna.

48 Google, *Discover Our Child Safety Toolkit*, https://protectingchildren.google/tools-for-partners/.

49 W. Wei, *Online Child Sexual Abuse Content: The Development of a Comprehensive*, https://www.iwf.org.uk/about-us/who-we-are/audits-and-inspections/independent-report-on-international-notice-and-takedown-system/.