ChatGPT

Privacy Laws for Social Media Users and Content Creators: GDPR vs CCPA

Introduction

Social media has transformed how we share personal information, leading to new legal protections for privacy. Two landmark privacy laws – Europe's **General Data Protection Regulation (GDPR)** and California's **Consumer Privacy Act (CCPA)** – have significant impact on social media users and content creators. The GDPR (in effect since 2018) is a comprehensive EU law that treats personal data protection as a fundamental right, and it set strict rules on how organizations worldwide must handle Europeans' data. The CCPA (effective 2020, and expanded by the CPRA in 2023) is the first major U.S. state law giving consumers control over personal information, often nicknamed "California's GDPR" [1]. This report explains the key rights and obligations under each law as they relate to social media, highlights major enforcement actions and cases, compares GDPR and CCPA, and discusses practical implications for content creators, influencers, and everyday social media users.

GDPR: Key Rights and Obligations for Social Media

User Data Rights under GDPR: The GDPR grants individuals (data subjects) a bundle of powerful rights over their personal data. Social media users in the EU have the **right to access** their data (to obtain a copy of personal information a platform holds about them) [2]. They also have the **right to rectification** – to correct inaccurate or incomplete data – and the **right to erasure**, meaning they can request deletion of their personal data in certain circumstances (this "right to be forgotten" can require a platform to remove posts or profiles) [3]. Additionally, users can **restrict processing** of their data or **object** to certain uses (for example, objecting to data being used for targeted advertising) [4] [5]. The GDPR also created the **right to data portability**, which lets individuals receive their data in a common format to reuse it or transfer it to another service [6]. There are even rights related to **automated decision-making**, so if a social network uses algorithms to make significant decisions (like content moderation or account suspensions), users have the right not to be subject solely to automated decisions and to seek human review. In practical terms, these rights mean a social media user in the EU can request Facebook, Instagram, YouTube or any platform to **provide a full report of the user's personal data, correct or delete content/data upon request, and respect preferences such as opting out of profiling** [7]. Platforms must respond to most requests within one month, making these rights a real tool for users to control their online data footprint.

Obligations on Platforms and Creators under GDPR: To comply with GDPR, social media companies and anyone collecting personal data must follow strict rules. **Lawful basis & consent:** There must be a legal justification for processing personal data [8]. In social media marketing or content creation, the most common lawful bases are user consent or the controller's "legitimate interest." For example, an influencer collecting email addresses for a newsletter must get explicit, opt-in consent from subscribers under GDPR rules [9] [10]. Consent cannot be buried in fine print or assumed; it must be clear and can be withdrawn at any time [11]. Platforms and creators also can rely on legitimate interests for data use (like basic analytics), but they must ensure they aren't overriding individuals' rights [12].

Transparency and privacy principles: GDPR mandates transparency about data practices. Social media platforms must provide users with clear privacy notices explaining what data is collected and how it's used [13] [14]. They must adhere to core data protection principles such as **data minimization** (collect only data that is necessary for a stated purpose) and **purpose limitation** (use data only for the specific, legitimate purposes disclosed) [15]. They should also keep data accurate and up-to-date, store it only as long as needed, and secure it appropriately [16]. GDPR's principle of **accountability** means companies must not only follow the rules but be able to demonstrate their compliance (e.g. maintaining records, policies, and evidence of consent) [17].

Security and breach duties: Platforms must safeguard personal information with appropriate security measures. If a data breach occurs affecting users' personal data, GDPR requires that the company notify the national data protection authority (and in some cases the affected users) within 72 hours [18]. This has forced social networks to improve their cybersecurity and breach response plans.

Applicability to content creators: It's not just Big Tech that has to comply – **even individual content creators or small businesses can be "data controllers" under GDPR if they collect or decide how personal data is processed**. For example, if a YouTuber or blogger runs a personal website that tracks visitors or sells merch to EU fans, GDPR likely applies to them. They would need to post a GDPR-compliant privacy policy and possibly a cookie consent banner on their site [19]. An influencer launching an app must inform users how their data is handled and get necessary consents, or they could face legal challenges under GDPR [19]. In short, content creators should treat personal info of their followers (emails, names, shipping info, etc.) with the same care a larger company would – by collecting only what is needed, securing it, and honoring any requests to access or delete that data. Failure to do so can result in GDPR penalties even for smaller operators, though enforcement tends to focus on larger-scale violations.

GDPR Enforcement Actions and Case Law

Since coming into force, the GDPR has been actively enforced by European data protection authorities, including against major social media platforms. **Regulators have not shied away from issuing huge fines for privacy violations**, sending a message that misuse of user data has serious consequences. For example, in 2022 Ireland's Data Protection Commission (the lead EU regulator for many tech firms) fined Instagram €405 million for mishandling children's personal data on the platform [20]. The investigation found Instagram allowed teenage users (ages 13–17) to set up business accounts that published their email addresses and phone numbers publicly, violating children's privacy rights [21]. (Instagram has since changed its settings and is appealing the fine [22].) Another enforcement in 2021 penalized WhatsApp €225 million for failing to provide transparent information about how it shared users' data with Facebook, breaching GDPR's transparency requirements [23].

More recently, **Meta (Facebook's parent company)** was hit with the largest GDPR fine to date – **€1.2 billion** – for illegal data transfers of Facebook users' personal information to the United States [24]. In that case, Facebook was found to have continued transferring European users' data to U.S. servers despite an EU court ruling that such transfers could expose Europeans' data to U.S. surveillance without adequate privacy protections. The fine (issued by Ireland's DPA in 2023) underscores that GDPR's reach is global and that even data flows between continents must comply with European privacy standards [25]. Andrea Jelinek, the Chair of the European Data Protection Board, noted that Meta's infringement was "systematic" and the **record penalty is a strong signal that serious infringements have far-reaching consequences** [26].

Beyond fines, **GDPR has been enforced through landmark court cases** that shape how social media companies operate. A pivotal case was the series of challenges by Austrian privacy activist Max Schrems against Facebook. In 2020, the **"Schrems II" case** led the European Court of Justice to invalidate the EU–US Privacy Shield agreement (a data-sharing framework), on the grounds that U.S. law did not sufficiently protect EU citizens' data from government surveillance [27]. This case, stemming from a user's complaint about Facebook Ireland sending his data to Facebook's U.S. servers, forced companies to scramble for alternate legal mechanisms to transfer data and spurred negotiations for new international agreements. Another influential decision involved the "right to be forgotten" – even before GDPR, an EU court in *Google Spain v. AEPD* (2014) recognized individuals' right to have search results about them delisted in some cases. GDPR codified this right to erasure, and social platforms/search engines must comply by removing personal content upon valid request (unless an exception applies for public interest, free expression, etc.) [28].

Enforcement trends: EU authorities have focused on issues like children's privacy (as seen with Instagram and TikTok fines), transparency failings, unlawful ad targeting, and data breaches on social media. They cooperate via the EDPB to handle cross-border cases, ensuring companies can't evade scrutiny. The penalties can be very steep – GDPR allows fines up to **€20 million or 4% of a company's worldwide annual revenue for the most serious violations** (whichever is higher) [29]. For big tech firms, 4% of global revenue can mean billions, which is meant to deter non-compliance. Even aside from fines, companies risk reputational damage and mandated changes to their business practices. The bottom line for social media users and creators is that GDPR enforcement has pressured platforms to give users more control and transparency. Features like Facebook's privacy dashboard or Instagram's data download tool (allowing you to get a copy of all your photos, posts, and messages) are direct results of GDPR compliance efforts [30] [31].

CCPA: Key Rights and Obligations for Social Media

Consumer Data Rights under CCPA: The California Consumer Privacy Act gives California residents important rights over their personal information, which affect how social media and online businesses operate. Under the original CCPA, consumers have the **right to know** what personal information a business has collected about them and **how it is used or shared** [32]. In a social media context, this means a California user can request a report of the categories of personal info a social network or even an influencer's online store has gathered on them (e.g. profile data, purchase history, device identifiers, etc.) and who it's shared with. Consumers also have the **right to delete** personal information that a business collected from them (with some exceptions) [32]. For example, a user could ask a platform or an online content creator's shop to delete the personal data they provided (although businesses may retain data needed for security, legal compliance, or internal uses allowed by the law). Another key right is the **right to opt out of the sale of personal information** to third parties [33]. "Sale" is defined broadly in CCPA – it can include any sharing of personal data for valuable consideration, which covers a lot of online advertising and tracking scenarios. For instance, if a social media site sells or exchanges user data with ad networks, California users must be given a way to opt out of that sale. In practice, websites and apps have added **"Do Not Sell My Personal Information"** links or toggles to honor this right. Finally, the CCPA grants the **right to non-discrimination**: a business cannot deny services, charge different prices, or provide a lower quality of service just because a consumer exercised their privacy rights [34] [35]. This prevents, say, a social platform from banning or throttling a user who opted out of data sales (though the law does allow loyalty program incentives as long as they are properly disclosed).

Expanded rights under CPRA: In 2020, California passed the **California Privacy Rights Act (CPRA)**, which amended the CCPA effective January 1, 2023 [36]. The CPRA added two new rights for consumers: the **right**

to correct inaccurate personal information, and the **right to limit the use or disclosure of "sensitive" personal information** [37]. Sensitive personal information (like precise geolocation, race/ethnicity, health data, etc.) now gets special protection – businesses must minimize its use and honor consumers' requests to limit its use for secondary purposes. With the right to correction, a California social media user could ask a business to fix wrong data (for example, if an e-commerce influencer's site has a misspelled name or incorrect profile info on file). These additions make California law a bit more GDPR-like. As of 2023, California residents enjoy a set of rights **akin to GDPR rights**: know/access, delete, opt-out (plus opt-in consent for minors' data sales), correct, limit sensitive data use, and non-discrimination [37]. Social media companies had to update their workflows to accommodate these – for example, by adding options for users to edit or correct stored info, and by treating browser signals like the **Global Privacy Control** as opt-out requests (the CCPA regulations clarify that a user can send a "do not sell" signal via a browser or plugin which companies must honor) [38].

Obligations on Businesses under CCPA: The CCPA primarily regulates **"businesses"**, defined as for-profit entities that determine the purposes and means of processing consumers' personal info, do business in California, and meet certain thresholds [39]. Those thresholds (after CPRA's updates) include: having annual gross revenues over about $25 million; or annually buying/selling/sharing personal info of 100,000 or more consumers or households; or deriving 50%+ of annual revenue from selling or sharing personal info [40] [41]. This means the law directly targets medium and large companies (like major social media platforms, ad tech firms, large influencers who monetize data, etc.), while exempting small businesses that don't meet the criteria. However, even smaller content creators should be aware that if their online activities grow (e.g. a popular app or site with hundreds of thousands of users), they could become subject to CCPA compliance.

Businesses covered by CCPA must **provide transparency and notices to consumers** about their data practices. They are required to have a clear, publicly available **privacy policy** disclosing the categories of personal information collected, the purposes for which it's used, the categories of sources and third parties it's shared with, and details of consumers' CCPA rights and how to exercise them [42]. At or before the point of data collection, businesses should give a **notice at collection** – for example, a pop-up or statement on a website explaining what info is being gathered from a user and why [43]. If the business "sells" personal data, it must provide a **"Do Not Sell My Personal Information"** link on its website or app, which allows users to opt out of data sales [44]. (Since 2023, this has expanded to "Do Not Sell or Share" to cover sharing for targeted advertising). Social media services that serve Californians have had to implement these mechanisms; many show a CCPA opt-out link in their footers or settings for California users.

Honoring consumer requests: Just as important as providing notice is the obligation to **honor consumer rights requests.** Businesses need to have methods for consumers to submit requests to know, delete, or correct information (typically toll-free numbers and/or web forms) and then verify the requestor's identity and respond within 45 days (with a possible extension to 90 days) [45]. For deletion requests, businesses must delete the person's data from their systems (and notify service providers to do the same) unless an exemption applies. For opt-out of sale requests, they must stop selling that individual's data and refrain from asking the person to re-opt-in for at least 12 months. An important practical point is that CCPA's regulations now **require businesses to honor the Global Privacy Control (GPC)** – a browser or device signal that communicates a user's universal opt-out. If a user installs, say, a browser extension that sends a GPC signal, and they visit a website, that site must treat it as a valid "Do Not Sell" request for that user [46]. This is particularly relevant for content creators who monetize via third-party ads: they need to ensure any GPC signals are respected by their site's scripts or their ad partners, or they could unknowingly violate the CCPA.

Data minimization and security: The CPRA amendments introduced explicit **data minimization and purpose limitation requirements** similar to GDPR [47]. Now, businesses should only collect, use, and retain personal data that is reasonably necessary and proportionate to the purposes consumers expect or have consented to [48]. In other words, even under CCPA, companies shouldn't stockpile user data "just because" – it needs to serve a disclosed purpose. Businesses also have an obligation to implement "reasonable security procedures and practices" to protect personal information [49]. If they fail to safeguard data and a breach occurs, they may face liability (more on that in enforcement). Although CCPA does not mandate practices like GDPR's Data Protection Officers or impact assessments, it pushes companies toward good data hygiene and security, which is especially relevant for social platforms that collect sensitive personal content.

In summary, the CCPA/CPRA regime requires social media companies, advertising firms, and any qualifying business to **be transparent, give users control over data sales, respond to privacy requests, and secure personal data**. For content creators and influencers: if you run a monetized blog, an e-commerce store, or any venture involving California residents' personal info at a significant scale, you need to follow these obligations. Even if you're below thresholds, adopting some of these privacy-friendly practices (clear privacy notices, opt-outs, good security) can be beneficial for audience trust.

CCPA Enforcement Actions and Case Law

Enforcement of the CCPA in its early years has been led by the California Attorney General (and now also the California Privacy Protection Agency). The law provides for civil penalties and, in limited cases, private lawsuits for violations. **Major enforcement actions to date have signaled that California is serious about protecting consumers' data rights.**

A landmark action came in 2022, when California's Attorney General announced a settlement with **Sephora, Inc.** – this was one of the first public CCPA enforcement cases and a wake-up call to industry [50]. Sephora, a cosmetics retailer, was accused of failing to disclose to consumers that it was "selling" their personal information and failing to honor opt-out requests sent via Global Privacy Control signals [51] [52]. According to the AG's findings, Sephora allowed third-party ad and analytics trackers on its website which collected data on consumers' browsing, shopping cart, device details, and precise locations [53] [54]. These third parties used the data to create consumer profiles (for targeted advertising), and under CCPA this arrangement counted as a **"sale" of personal information** [55]. However, **Sephora did not inform consumers of this sale nor provide a "Do Not Sell" option, and it ignored the global opt-out signals** that some users sent from their browsers [52] [38]. The AG's office gave Sephora notice of these violations but the company did not cure them within the 30-day grace period (which at the time CCPA allowed) [56]. The result was a settlement in which **Sephora paid $1.2 million in penalties** and agreed to implement a robust compliance program [57] [58]. Specifically, Sephora had to update its privacy policy to clearly state that it sells personal data, provide a way for consumers to opt out of sale (including via GPC signals), fix its contracts with third-party trackers to meet CCPA's requirements, and report to the AG on its progress [58]. The case was widely publicized and **underscored consumers' rights under CCPA to control commercial surveillance of their data** [59]. Following this, the AG conducted a sweep sending notices to various businesses (in industries like retail, fitness, data brokers, etc.) that had missing or unclear opt-out mechanisms, loyalty program data practices that weren't properly disclosed, or confusing privacy policies [60] [61]. Many companies heeded the warnings and adjusted their practices to avoid fines.

Starting in 2023, the new California Privacy Protection Agency (CPPA) took over primary responsibility for CCPA enforcement. The CPPA can conduct audits and bring administrative enforcement actions, while the AG can still go to court for civil penalties [62]. Notably, the **30-day "cure period" for violations expired in 2023** (as allowed by the CPRA) [63] [64]. Now regulators can immediately enforce the law without giving a breaching company an automatic opportunity to fix issues first. We can expect more stringent enforcement going forward, potentially in areas like how social media apps handle sensitive information or targeted advertising disclosures.

On the **case law** side, CCPA is still relatively new, but there have been some lawsuits invoking its provisions. The CCPA includes a limited **private right of action** that lets consumers sue for statutory damages if certain types of data breaches occur (specifically, if a business failed to implement reasonable security and a consumer's unencrypted personal information was stolen) [65] [66]. Early examples include a class-action lawsuit against retailer **Hanna Andersson** after a 2019 data breach exposed 200,000 customers' credit card and contact information. In 2020, that case settled for **$400,000** plus promises of improved security [67]. Each affected customer could claim a small cash payment, and it was one of the first settlements citing CCPA's statutory damages for a data breach [68]. While the payout per person was modest (a few dollars each or up to $750 if they had actual losses), the case signaled that companies could face liability from consumers themselves if they don't protect personal data. Another high-profile lawsuit involved social media app **TikTok**, which faced CCPA-based claims (along with federal privacy claims) for allegedly mishandling children's data; TikTok settled that in 2021 for $92 million (though that settlement covered broader privacy issues, not solely CCPA).

It's worth noting that **most CCPA enforcement so far has been through regulatory action rather than court judgments**. The Sephora case didn't go to trial – it was a negotiated settlement. Many companies choose to cure violations or settle because it's often cheaper and more predictable than litigation. However, we're likely to see more case law developing as plaintiffs test the boundaries of CCPA (for instance, whether certain targeted advertising arrangements count as a "sale" – an issue likely to be litigated). For now, the enforcement message is clear: businesses that ignore CCPA can face significant fines (up to **$2,500 per violation or $7,500 per intentional or children's data violation** [69]), and those that suffer breaches may pay out to affected users. Social media platforms operating in California have adjusted by, for example, adding **comprehensive privacy dashboards and tools for California residents**, mirroring some GDPR-style controls. And importantly for influencers and creators, if you partner with brands or monetization platforms, you may be asked to contractually comply with CCPA (since the law also imposes duties on "service providers" and partners of big businesses to handle data per CCPA rules [70]).

GDPR vs CCPA: Scope, Definitions, Compliance, and Penalties

GDPR and CCPA share a common goal of giving individuals more control over personal data, but they differ in scope and approach. Here is a comparison from the perspective of social media users and creators:

- **Scope and Applicability:** GDPR is an **EU-wide law** that protects any person **in the EU**, regardless of nationality, and it applies to **any organization (of any size, anywhere in the world)** that processes those individuals' personal data [71] [72]. There are no revenue or size thresholds – a solo app developer or a global tech giant alike must comply if handling EU residents' data. GDPR also covers non-profits, government agencies, etc., not just businesses. CCPA, by contrast, is a **state law** protecting **California residents** (defined as people residing in CA, excluding tourists or temporary visitors) [73]. CCPA only applies to **for-profit businesses** doing business in CA that meet certain

thresholds (>$25 million revenue, or data on 100k+ individuals/households, or 50% revenue from data sales) [40]. Thus, CCPA is narrower: for example, a small hobby forum or an individual influencer not meeting those criteria wouldn't be directly obligated by CCPA, whereas under GDPR even a small website must comply if it has EU users. Also, GDPR's reach is global (extraterritorial effect) – a U.S. content creator could be obligated by GDPR if they knowingly attract EU followers or track EU users, while a European company with California customers isn't automatically under CCPA unless it meets the business criteria. In summary, **GDPR covers more entities and countries; CCPA covers a specific population and exempts many small businesses.**

- **Definitions of Personal Data:** Both laws define personal data very broadly. **GDPR's definition of "personal data"** includes "any information relating to an identified or identifiable natural person," which covers obvious identifiers (name, email, ID numbers) and also things like IP addresses, device IDs, location data, or online behavioral data if they can be linked to a person. **CCPA's term "personal information"** is similarly broad and in some ways even more explicit – it includes information that "identifies, relates to, describes, or could reasonably be linked with" a consumer or **household**, directly or indirectly [74] [75]. CCPA uniquely mentions households and devices, which means data need not be tied to a named individual as long as it is linked to a particular device or dwelling [76]. For example, under CCPA a smart TV's data about a household could be protected, even if the individuals aren't named. GDPR typically focuses on individuals, but its reach covers digital identifiers that can indirectly identify a person. Both laws exclude truly anonymous data. CCPA also lists specific categories (identifiers, biometric, internet activity, geolocation, etc.) to clarify what is covered. One notable difference is **sensitive data**: GDPR treats certain sensitive data (race, health, sexual orientation, etc.) as "special category" requiring extra protection. CCPA (as amended by CPRA) defines "sensitive personal information" and gives consumers a right to limit its use [77], which is conceptually similar. Overall, social media content – posts, profile info, contacts – would generally be personal data under GDPR and personal information under CCPA if it's about an identifiable person. Both laws also exclude public information (like content made public by the user) from some provisions, and CCPA excludes certain data already regulated by other laws (e.g. medical info under HIPAA).

- **Consent vs. Opt-Out (Legal Bases):** A fundamental difference is how each law approaches **permission to process data**. **GDPR requires a lawful basis for all personal data processing [8].** There are six bases (consent, contract, legal obligation, vital interest, public task, or legitimate interests) [8], and if no legal basis applies, the processing is unlawful [78]. In practice, this means EU social media platforms and content creators often must obtain **explicit consent** from users for activities like targeted advertising, certain cookies, or collecting sensitive data [10]. For example, after GDPR, many websites introduced cookie consent banners because dropping tracking cookies relies on user consent unless strictly necessary. Users must *opt in* (particularly for non-essential data uses), and they can withdraw consent at any time [14]. By contrast, **CCPA does not generally require prior consent to collect personal data**. Businesses can collect and use data by default (apart from children's data, where opt-in consent is required for selling info of minors under 16). The CCPA model is **"notice and opt-out"** – businesses tell consumers what they collect and give them the right to say no to sales. Consumers are **automatically "in" until they opt out** of sale or sharing. This is why, for instance, you don't see general data processing consent boxes on U.S. sites as you do in the EU, but you might see a "Do Not Sell My Info" link to handle California opt-outs. In short, **GDPR is stricter upfront (requiring a justification like consent)** for most data uses, whereas **CCPA places the burden on consumers to opt out** of certain data flows. For social media users, this means EU users

often encounter consent prompts (e.g. “Allow this app to collect data?”), while Californians might have to hunt for an opt-out if they don’t want their data sold. However, with the GPC and user-friendly opt-out signals, California is moving toward making opt-outs easier and more universal [46]. Another implication is that GDPR mandates features like **privacy by design/default** – services should be designed to minimize data use and have privacy-friendly defaults – whereas CCPA doesn’t have an explicit equivalent requirement.

- **Consumer/User Rights:** Both laws give individuals rights, but **GDPR’s list of individual rights is longer and more granular**. GDPR grants rights to access data, rectify it, erase it, restrict processing, data portability, and to object, as well as rights around automated profiling [79] [28]. The **CCPA’s core rights** (until CPRA added more) were the right to know, delete, and opt-out of sales, and to not be discriminated against [32]. Now CPRA has added the right to correct and to limit sensitive data use [37], bringing CCPA closer to GDPR’s level. Still, GDPR has no direct analog of the “opt out of sale” because GDPR would typically require opt-in consent to share data with third-party advertisers in the first place. In practice, a social media user in Europe can demand much more – e.g. they could object to a platform’s **legitimate interest** processing (like certain data analytics) and the company might have to cease that processing for that user. A Californian can’t object to all processing – only to sale/sharing. Also, GDPR’s rights apply universally to any personal data held (unless an exemption applies), whereas CCPA’s deletion right, for example, has more exceptions (a business can refuse to delete data it needs for legitimate reasons like security, completing a transaction, free speech, etc.). **Enforcement of rights** also differs: GDPR rights are enforced by regulators (with individuals lodging complaints to authorities if not honored), and individuals can also directly sue for damages under GDPR in some cases. Under CCPA, the AG/CPPA can enforce failures to honor access or delete requests, but there’s no private lawsuit for most rights (only for breaches). For users and creators, this means GDPR rights might be more consistently fulfilled (due to big fines risk), whereas with CCPA, one largely depends on regulator oversight or the business’s goodwill.

- **Compliance Requirements and Business Responsibilities:** GDPR is far more prescriptive about internal compliance. It often requires activities like conducting Data Protection Impact Assessments for high-risk processing, appointing a Data Protection Officer (DPO) for certain organizations, and maintaining detailed data processing records [80] [81]. It also requires notification of breaches within 72 hours and potentially to users [18]. CCPA has no DPO requirement, no specific audit/assessment mandate (though the CPPA is considering regulations for cybersecurity audits in the future), and a longer timeline for responding to breaches (notification “in the most expedient time possible” under California’s breach law, which predates CCPA). However, CCPA does require training employees who handle consumer inquiries about CCPA, and it requires businesses to flow down data protection terms to their service providers (e.g. when a content creator uses an email marketing service, they should have a contract saying the service provider won’t sell the personal info and will assist in deleting data, etc.) [82]. Both GDPR and CCPA necessitate that businesses update their **contracts** with third parties: GDPR has controller-processor contract clauses; CCPA requires specific clauses with “service providers” to ensure they don’t misuse data. In essence, GDPR compliance is a heavier ongoing exercise (privacy governance, documentation, data mapping, etc.), whereas CCPA compliance has been more about consumer-facing disclosures and handling requests, with slightly less administrative burden. From a creator’s perspective, if you comply with GDPR, you’re likely covering most of CCPA, but not vice versa.

- **Penalties and Remedies: GDPR's penalties are famously high** – up to €10 million or 2% of global turnover for certain violations, and up to €20 million or 4% of global turnover for the most serious (like basic principles or data subject rights breaches) [29]. This scaling to global revenue means tech giants face huge fines (as seen with hundreds of millions against Meta, Google, etc.), while a small entity could theoretically face fines in the thousands or millions depending on circumstances. GDPR fines are imposed by data protection authorities in Europe, and there is cooperation so that one lead authority can issue fines affecting multiple countries. By contrast, **CCPA's statutory fines are capped per violation**. The law sets civil penalties up to **$2,500 per violation** (for unintentional violations) or **$7,500 per violation** if the violation is intentional or involves children's data [83]. "Per violation" can be interpreted as per consumer, per incident – so the cost can multiply if many individuals are affected. For instance, if a social media company failed to honor opt-outs for 1,000 users, that could be 1,000 violations. Still, even in a large case, CCPA fines are likely to be lower than GDPR fines for a similar incident because of these caps (e.g., 100,000 violations even at $7,500 each would be $750 million, whereas GDPR 4% of revenue for a Facebook-scale company can exceed a billion). Another difference: CCPA (post-CPRA) allows the CPPA to impose administrative fines, and the AG or CPPA can also seek civil penalties through court. The **CPRA removed the 30-day cure period** that initially gave businesses a chance to fix issues before fines – GDPR never had a grace period; authorities can directly penalize if they find non-compliance [64]. On the individual side, GDPR allows individuals to claim compensation for material or non-material damage caused by violations (e.g., if a data leak caused harm). CCPA's only individual remedy is for certain data breaches, with statutory damages of $100–$750 per consumer per incident (or actual damages) [65]. So, European users theoretically have more avenues to seek redress (complaints to DPAs or lawsuits), whereas Californians largely rely on the regulator unless it's a breach case.

In summary, **GDPR is more expansive and strict, while CCPA is more targeted and somewhat less demanding**. GDPR pushes for *data protection by default* – getting consent, minimizing data, protecting all personal data – whereas CCPA focuses on *transparency and choice* – tell consumers and let them opt out of certain uses. For a content creator or company dealing with both EU and California audiences, it's usually necessary to meet the higher GDPR standard (which will by extension satisfy most CCPA duties, aside from providing a do-not-sell link). Both laws carry significant penalties and reputational risks for non-compliance, and both are influencing new laws around the world. (Already, other U.S. states like Virginia, Colorado, etc., have passed similar laws, often blending concepts of GDPR and CCPA.)

Practical Implications for Social Media Users and Content Creators

For Social Media Users: GDPR and CCPA empower users to take control of their personal data in ways not possible a decade ago. As a social media user in an GDPR jurisdiction (Europe), you should know that you can **request a copy of all your data** from major platforms (and they must provide it in a commonly used format, often through automated download tools) [84] [85]. You have the right to ask a platform to delete your account and all associated personal data – and except in certain cases (like public interest or legal obligations), they have to comply [28]. If something about you is wrong (say, a birthdate or an email), you can ask them to correct it [79]. You can also object to how your data is being used – for example, you can opt out of personalized ads on many services, and under GDPR the company must respect that decision for your account. In California, as a user, you should be aware of the **"Do Not Sell" rights** – if you don't want your social media or web browsing data shared with third-party advertisers, use the opt-out links or browser signals like **Global Privacy Control** to tell companies to stop selling/sharing your info [46]. You can also request businesses to show you the specific pieces of personal information they have on you [86]. This

can be eye-opening – for instance, you might discover a social network has collected precise location tracks or a list of inferred interests about you. Using these rights can help you manage your digital footprint: you could periodically delete old data, or ensure that data brokers connected to social media (like those tracking via cookies) are forced to purge your data if you request deletion through them or via a service.

Users should also know that these laws mean **companies are watching their own behavior more closely**. Social media platforms have had to implement more privacy controls for users post-GDPR [87]. You may have noticed clearer privacy settings, or prompts asking for permission for certain features. For example, Facebook now has a Privacy Center where you can see and manage data collected about you (which arose from GDPR requirements). Instagram introduced the ability to download your data easily, aligning with the data portability right [30]. Twitter (now X) added more opt-outs for personalized ads and shows users what data is being collected [88]. These changes make it easier for you as a user to self-serve your privacy preferences – **take advantage of them**. Regularly review your privacy settings on each platform; under GDPR and CCPA, the companies have to honor those settings (e.g., if you opt out of ad personalization, they must actually stop using your data for that). And if you ever feel a platform is violating your rights – say, refusing a legitimate deletion request – GDPR allows you to complain to your country's Data Protection Authority, and CCPA allows you to report issues to the CPPA or AG. There have been cases where user complaints led to investigations and fines, so your voice matters in enforcement.

For Content Creators and Influencers: If you're a content creator (like a YouTuber, blogger, podcaster, or influencer) who handles personal data, you need to be aware of these laws both to protect your audience's privacy and to avoid legal risks as your brand grows. **On the compliance side:** consider what personal data you collect from fans or followers. This could be obvious data like email addresses (for newsletters or giveaways), shipping info (if you sell merchandise), or less obvious data like tracking visitors on your website via Google Analytics. Under laws like GDPR, you may be deemed a **data controller** for that information, which means you're expected to do things like **post a privacy notice**, **get consent for non-essential cookies**, and **honor deletion or access requests**. For example, if you have a blog with EU visitors, you should have a cookie consent banner if you use ad trackers, and a privacy policy explaining your data practices [19]. It's not just big companies – even a solo content creator is legally on the hook in the EU if they're processing EU personal data in the course of business. Complying might sound daunting, but there are many free resources and templates (even the government websites and services like LegalFix mentioned) to help create basic privacy policies and respond to user rights. Additionally, if you collaborate with brands or platforms, **read your contracts**: brands may require that you comply with privacy laws (to not cause them liability). For instance, if you run an email list through a service, the terms likely require you to only upload contacts who consented (a GDPR expectation). If you ever do a promotion that collects viewers' personal info, ensure you're transparent and maybe limit it by region if you can't comply with all laws (some creators geo-restrict contests to avoid legal complexity).

Data security is another practical aspect: even as an individual, store any personal data (like fan addresses for giveaways) securely (use passwords, two-factor authentication, etc.). GDPR and CCPA both expect reasonable security, and the last thing you want is a breach that could hurt your followers and land you in a legal mess. If you don't actually need some personal data, don't collect it – this reduces your risk. For example, if you run a community forum, think twice about which data fields are truly needed from users.

On the opportunity side: These laws can help creators build trust with their audience by respecting privacy. Make it clear that you value your followers' data: for instance, state that you won't sell or misuse their information (if you're CCPA-covered, you'd explicitly offer a do-not-sell link, but even if not, you can

voluntarily follow that principle). If you're GDPR-covered, consider offering an easy way for users to request data or delete their info – even if few use it, the gesture counts. Also be mindful of the content you post about others: GDPR includes privacy rights that might affect posting personal data of private individuals without their consent. As a creator, if you moderate a group or handle user-generated content, you might need policies to quickly handle someone's request to remove personal info they accidentally shared.

Risk awareness: While regulators are not likely to target an individual influencer as quickly as a Facebook or Google, non-compliance can still have consequences. European authorities have occasionally investigated small companies and imposed fines (though often smaller amounts) for things like unsolicited emails or lack of a privacy notice [89]. California's CPPA can also enforce against any sized business if a pattern of complaints arises. Furthermore, your reputation is at stake: an influencer caught in a scandal of leaking followers' emails or misusing personal info could face public backlash and lose partnerships. So privacy compliance is part of professionalizing your online presence.

Practical tips for creators:
- **Be transparent:** Clearly communicate how you collect and use data. For example, if you start a mailing list, explain what emails will be used for and honor unsubscribe requests (GDPR/CCPA require this).
- **Use available tools:** Many platforms (e.g., Instagram, Twitter, YouTube) provide settings to help comply with local laws. If you run ads or use analytics, use the privacy settings (like Google Analytics' IP anonymization for GDPR, or YouTube's audience selection tools for kid content compliance). California's law spurred the **Global Privacy Control** – you as a user or creator can even use it in your own browsing to signal your preferences [46], and be aware that your audience might be using it too.
- **Stay updated:** Privacy laws evolve. GDPR is stable now, but California's law is enforced by a new agency that issues regulations (for example, expected rules on automated decision-making transparency). Other states (like Virginia, Colorado) have new laws that might affect nationwide activities. Keep an eye on legal updates – following tech law blogs or even Twitter accounts of privacy advocates can give heads-up. As a paralegal student or legal professional, your understanding here can even be a value-add if you're advising a business or working in compliance.

For social media platforms and large content operations: They will continue to adapt features to comply. As a user, this means more control at your fingertips. As a creator using those platforms, it may mean new rules – e.g., Facebook might restrict how you can target ads or require you to certify compliance with its data policies (they do this to adhere to laws). Influencer marketing campaigns now often include clauses about not exposing personal data of participants without permission, etc.

In conclusion, from a user and creator perspective: **GDPR and CCPA give you rights and impose responsibilities that ultimately foster a more privacy-conscious social media environment.** Users can demand transparency and fairness in how their data is handled, and creators/businesses who respect these laws not only avoid penalties but also build trust and credibility. These regulations are shaping the future of social media by establishing that personal data is not a free-for-all commodity – it comes with strings attached, whether in the EU or California. By learning about and leveraging your rights (if you're a user) or diligently meeting your obligations (if you're a creator/business), you become an active participant in protecting privacy online.

Conclusion

Privacy laws like the GDPR and CCPA were developed in response to public concern over personal data exploitation in the age of social networks and big data. For social media users, these laws are empowering: **you have the right to know what happens with your data, to control it, and to hold companies accountable**. For content creators and influencers, the laws may pose new compliance challenges, but they also offer a framework to **build trust with your audience by respecting their data rights**. The GDPR's European regime and California's CCPA share the common thread of putting people in charge of their own information, albeit with different mechanisms. We've seen regulators enforce these rules in high-profile cases – from massive fines on tech giants under GDPR to the California AG making an example of companies that ignored CCPA's requirements. Going forward, we can expect privacy enforcement only to increase. As aspiring paralegals and legal professionals, understanding these regulations is crucial: not only to help organizations navigate compliance, but also to educate clients and the public about their rights.

In the rapidly evolving digital landscape, one thing is clear: **privacy is here to stay as a key consideration in social media and content creation.** Knowing GDPR and CCPA helps social media users safeguard their personal data and helps creators innovate responsibly. By complying with these laws and keeping privacy in focus, content creators can continue to thrive in the social media space while minimizing legal risks. And by exercising their rights, users encourage a healthier online ecosystem where privacy and creativity can coexist.

Sources:

- European Commission, **General Data Protection Regulation** (EU) 2016/679 – Articles 12-22 (data subject rights) and enforcement provisions.
- ICO (UK Information Commissioner's Office) – *Guide to GDPR Individual Rights* [2] [90] [91] (summarizing right of access, rectification, erasure, etc.).
- Usercentrics, *GDPR and Social Media: What Users and Marketers Need to Know* – discussion of consent and platform changes post-GDPR [11] [87].
- Reuters report, *Ireland fines Instagram €405 million over children's data* [20] [21]; EDPB News, *Meta (Facebook) fined €1.2B for data transfers* [24].
- California Consumer Privacy Act (2018) (Cal. Civ. Code §1798.100 et seq.), as amended by CPRA (2020) – California Privacy Protection Agency FAQs [37] [39] and Thomson Reuters Legal Guide [32] [92].
- California Dept. of Justice, Press Release on **Sephora CCPA Settlement** (Aug. 24, 2022) [50] [57] and explanation of GPC opt-out requirements [38].
- Privacy World blog, *First CCPA Settlement (Hanna Andersson breach)* – class action settlement details [67].
- Cookiebot, *CCPA vs GDPR* comparison – key differences in scope and rights [71] [72].
- Thomson Reuters (Practical Law), *CCPA vs GDPR* – compliance obligations and penalty provisions [42] [93].
- Epic.org, *Schrems v. Facebook case summary* – background on EU–US data transfer case [27].
- NetApp BlueXP, *GDPR vs CCPA Infographic* – highlights of major differences in consent and scope [94] [95].
- California Privacy Protection Agency, **CCPA Regulations and Guidance** – on consumer rights, business duties, and enforcement powers [47] [96].

1 34 35 36 37 39 47 48 70 77 96 Frequently Asked Questions (FAQs) - California Privacy Protection Agency (CPPA)
https://cppa.ca.gov/faq.html

2 3 4 5 6 90 91 A guide to individual rights | ICO
https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/individual-rights/individual-rights/

7 9 10 11 12 13 14 29 30 31 87 88 GDPR And Social Media: Everything Marketers Need To Know
https://usercentrics.com/guides/social-media-email-marketing-compliance/gdpr-and-social-media-for-marketers/

8 15 16 17 18 78 80 81 What is GDPR, the EU's new data protection law? - GDPR.eu
https://gdpr.eu/what-is-gdpr/

19 Laws for Social Media Influencers and Content Creators
https://www.legalfix.com/articles/laws-for-social-media-influencers-and-content-creators

20 21 22 23 Ireland fines Instagram a record $400 mln over children's data | Reuters
https://www.reuters.com/technology/irish-regulator-fines-instagram-400-million-over-chidrens-data-2022-09-05/

24 25 26 1.2 billion euro fine for Facebook as a result of EDPB binding decision | European Data Protection Board
https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en

27 Data Protection Commissioner v Facebook and Max Schrems (Standard Contractual Clauses) – EPIC – Electronic Privacy Information Center
https://epic.org/documents/data-protection-commissioner-v-facebook-and-max-schrems-standard-contractual-clauses/

28 79 84 85 Data protection under GDPR - Your Europe
https://europa.eu/youreurope/business/dealing-with-customers/data-protection/data-protection-gdpr/index_en.htm

32 33 40 41 42 43 44 45 49 62 69 74 75 76 82 83 86 92 93 Understanding the California Consumer Privacy Act (CCPA)
https://legal.thomsonreuters.com/blog/the-california-consumer-privacy-act/

38 46 50 51 52 53 54 55 56 57 58 59 60 61 63 64 Attorney General Bonta Announces Settlement with Sephora as Part of Ongoing Enforcement of California Consumer Privacy Act | State of California - Department of Justice - Office of the Attorney General
https://oag.ca.gov/news/press-releases/attorney-general-bonta-announces-settlement-sephora-part-ongoing-enforcement

65 66 California Privacy Protection Agency Announces 2025 Increases for CCPA Fines and Penalties
https://cppa.ca.gov/announcements/2024/20241217.html

67 68 First CCPA Settlement Reached in Hanna Andersson Case | Privacy World
https://www.privacyworld.blog/2020/12/first-ccpa-settlement-reached-in-hanna-andersson-case/

71 72 73 94 95 CCPA vs GDPR: Infographic & 10 Differences You Need To Know
https://www.cookiebot.com/en/ccpa-vs-gdpr/

89 Guide to GDPR Fines and Penalties | 20 Biggest Fines So Far [2025]
https://www.cookieyes.com/blog/gdpr-fines/