FTC Announces Final “Click to Cancel” Rule for Subscriptions, Memberships

The Federal Trade Commission (“FTC”) has just announced the final version of its “Click to Cancel” Rule for consumer subscriptions. The Rule will go into effect 180 days after it is published with the Federal Register. This Rule will directly apply to all SaaS, digital health, tech, and non-tech companies selling on a subscription basis to consumers.

Full Text of FTC Rule

The full text of the FTC Rule is linked here, at pages 222-230.

Fact Sheet of FTC Rule

The FTC has also made available a fact sheet which briefly summarizes key provisions of the “Click to Cancel Rule,” which is attached here.

Key Provisions of the FTC Rule

According to the FTC announcement, the “Click to Cancel” Rule will apply to “almost all negative option programs in any media.” The key provisions of the FTC Rule will prohibit:

- misrepresenting any material fact made while marketing goods or services with a negative option feature;
- failing to “clearly and conspicuously disclose” material terms prior to obtaining a consumer’s billing information in connection with a negative option feature;
- failing to obtain a consumer’s express informed consent to the negative option feature before charging the consumer; and

- failing to provide a simple mechanism to cancel the negative option feature and immediately stop the charges.

Revisions to Final Version of the FTC Rule

Also according to the FTC announcement, the FTC dropped from its final Rule an annual reminder requirement that would have required vendors to provide annual reminders to consumers advising them of the negative option feature of their subscription, as well as a requirement that vendors had to ask canceling consumers for approval before a vendor could tell a canceling subscriber about reasons to keep the existing agreement or of possible modifications that could be made without canceling the subscription.

Reasons for Adoption of the Rule

Why did the FTC adopt a Click to Cancel Rule? According to the FTC Announcement, the FTC was receiving 70 consumer complaints per day over negative option programs, and this number was "steadily increasing over the past five years."

The FTC's announcement follows a recent California enactment of a more comprehensive "Click to Cancel" law.

Does the FTC Rule Supersede California Law?

The FTC Rule should not supersede California's more comprehensive law; in fact, the Rule specifically states in its text that the Rule will not be construed to supersede any State statute, regulation or order "except to the extent that it is inconsistent with the provisions of this part, and then only to the extent of the inconsistency." The expected impact of the FTC Rule is primarily to bring federal regulatory law closer to California regulatory law as it pertains to subscriptions and memberships.

What do SaaS, Digital Health, Tech, and other Companies Utilizing the Subscription Model Need to do in Response to this Announcement?

All companies utilizing a subscription model should revise consumer contracts and processes to comply with the FTC Rule over the next 180 days. Companies utilizing the subscription model with a business-focused customer base should similarly consider what changes to make to their contracts and processes as public policy will likely change regarding subscriptions generally along with the new FTC Rule and California law changes.

If you have questions or concerns about how new FTC "Click to Cancel" Rule or the new California "Click to Cancel Law" will impact your digital health company, please schedule a consultation at https://calendly.com/prinzlawoffice.

California's Safe and Secure Innovation for Frontier Artificial Intelligence Models Act Advances to Adoption in State Legislature

California is currently considering the adoption of a bill that would impose unprecedented new regulations on the development of AI. The bill under consideration is SB 1047, the Safe and Secure Innovation for Frontier Artificial Intelligence Models Act. A full copy of the bill is linked here.

SB 1047, the Safe and Secure Innovation for Frontier Artificial Intelligence Models Act

The Safe and Secure Innovation for Frontier Artificial Intelligence Models Act or SB 1047 would create a new Frontier Model Division within California's Department of Technology which would have oversight powers over the training of new AI models. Pursuant to SB 1047, developers of AI models would be required to build a so-called kill switch into the AI model and to potentially shut down the model until the Frontier Model Division deems that the AI model is subject to a "limited duty exemption," which would be defined as:

> *a determination. . . . that a developer can provide reasonable assurance that the covered model does not have a hazardous capability, as defined, and will not come close to possessing a hazardous capability when accounting for a reasonable margin for safety and the possibility of posttraining modifications.*

A "covered model" under SB 1047 would be defined to mean an AI model "that was trained using a quantity of computing power greater than 10^26 integer or floating-point operations, and the cost of that quantity of computing power would exceed one hundred million dollars ($100,000,000) if calculating using average market prices of cloud compute as reasonably assessed by the developer at the time of training."

As currently proposed, "derivative" AI models would be exempt from the new compliance obligations: only "non-derivative" AI models would be subject to the obligations.

Under SB 1047, a "derivative model" is defined to constitute an artificial intelligence model that is derivative of another AI model, including either " a modified or unmodified copy of an artificial intelligence model" or "a combination of an artificial intelligence model with another software. The "derivative model" is defined not to include "an entirely

independently trained artificial intelligence model" or an "artificial intelligence model, including one combined with other software, that is fine-tuned using a quantity of computing power greater than 25 percent of the quantity of computing power, measured in integer or floating-point operations, used to train the original model."

What constitutes a "hazardous capability" under the proposed legislation?

SB 1047 would define "hazardous capability" to constitute the capability of a covered model to be used in one of the following harms:

- the creation or use of a chemical, biological, radiological, or nuclear weapon in a manner that results in mass casualties
- at least $500 million dollars of damage through cyberattacks on critical infrastructure via a single incident or multiple related incidnts
- at least $500 million dollars of damage by an AI that autonomously engages in conduct that would violate the Penal Code if taken by a human
- bodily harm to another human
- the theft of or harm to property
- other grave threats to public safety and security that are of comparable severity to the harms described above.

Penalties for noncompliance with this legislation would include punitive damages and a civil penalty for a first violation not to exceed ten percent of "the cost of the quantity of computing power used to train the covered model to be calculated using average market prices of cloud compute at the time of training" and 30 percent of the same in case of a second violation. The legislation authorizes joint and several liability against the developers directly where

(1) steps were taken in the development of the corporate

structure among affiliated entities to purposely and unreasonably limit or avoid liability.

(2) The corporate structure of the developer or affiliated entities would frustrate recovery of penalties or injunctive relief under this section.

If passed, damages could be awarded for violations occurring as of January 1, 2026.

The reaction to SB 1047 from the Silicon Valley start-up community

As you might expect, the Silicon Valley start-up community is raising concerns about SB 1047.
Bloomberg has been reporting on the Silicon Valley reaction, and indicated that that a key concern is that this law is going to "place an impossible burden on developers—and particularly open-source developers, who make their code available for anyone to review and modify— to guaranteed their services aren't misused by bad actors." **Bloomberg** also reported that a general partner at Andreessen Horowitz indicated that some startup founders are so concerned that they are wondering if they should leave California because of the bill.
Bloomberg also reported that the a key point of contention in the startup community is the idea that AI developers are responsible for people who misuse their systems, pointing to Section 230 of the Communications Decency Act of 1996, which has shielded social media companies from liability over content users create on platforms.

Author **Jess Miers** of the Chamber of Progress criticized the legislation on the basis that it would "introduce a high degree of legal uncertainty for developers of new models, making the risks associated with launching new AI technologies prohibitively high."

The Prinz Law Office will continue following legislative developments relating to SB 1047 as this bill advances.

If you have questions regarding your software company's potential compliance obligations under SB1047, please schedule a consultation with The Prinz Law Office at this link.

California Law to Mandate Release of VC Investment Diversity Information

Governor Newsom has just signed **SB 54**, which will require venture capital firms in the state of California to annually report the diversity of founders they are backing. According to **Tech Crunch's reporting**, SB 54 will result in amendments to the Business and Professional Code and also will amend part of the Government Code pertaining to venture capital.

What is California SB 54?

SB 54 goes into effect as of March 1, 2025, and requires the following aggregated information to be reported on all VC investments:

- *The gender identity of each member of the founding team, including nonbinary and gender-fluid identities.*
- *The race of each member of the founding team.*
- *The ethnicity of each member of the founding team.*
- *The disability status of each member of the founding team.*
- *Whether any member of the founding team identifies as LGBTQ+.*
- *Whether any member of the founding team is a veteran or a disabled veteran.*

- *Whether any member of the founding team is a resident of California.*
- *Whether any member of the founding team declined to provide any of the information described above.*

Failure to timely comply with the reporting requirement may result in the assessment of a penalty of One Hundred Thousand Dollars ($100,000.00) to be assessed against a "covered person." **SB 54** defines "covered person" as any person who does both of the following:

- *Acts as an investment adviser to a venture capital company.*
- *Meets any of the following criteria: (i) Has a certificate from the Commissioner of Financial Protection and Innovation pursuant to Section 25231 of the Corporations Code. (ii) Has filed an annual notice with the Commissioner of Financial Protection and Innovation pursuant to subdivision (b) of Section 25230.1 of the Corporations Code. (iii) Is exempt from registration under the Investment Advisers Act of 1940 pursuant to subsection (l) of Section 80b-3 of Title 15 of the United States Code and has filed a report with the Commissioner of Financial Protection and Innovation pursuant to paragraph (2) of subdivision (b) of Section 260.204.9 of Title 10 of the California Code of Regulations.*

SB 54 provides that reports will be due by March 1st of each year.

What is the Argument in Favor of SB 54?

Tech Crunch reports that supporters of SB 54 have argued that this law will make venture capital more "transparent." According to **Tech Crunch**, less than 3 % of all venture capital investments go to women or black founders.

Tech Crunch reported that SB 54 was opposed by the National Venture Capital Association and TechNet, though both organizations professed to support generally the concept of diversity in venture capital.

What is the Anticipated Impact of SB54?

Although the impact of SB 54 will go beyond just the software industry, this new law is likely to have a significant impact on software and SaaS companies, particularly those having diverse founders, as mandated reporting will likely incentivize venture capital firms to further focus on considering diversity in investment. If your software company has diverse founders, you will definitely want to keep this law on your radar screen going forward.

California Considers Adoption of Controversial Veterinary Telehealth Bill

The California legislature is currently considering a controversial new telehealth bill that would dramatically expand the access to veterinary care for animal patients located in California. **AB 1399** would change California's existing law to permit a veterinarian-client-patient-relationship to be established solely via telemedicine. Existing California law limits the practice of veterinary telemedicine to existing veterinarian-client-patient-relationships only, where the animal has previously been examined by the veterinarian, except in cases where the advice is given in an emergency. See the attached link to view the bill in its entirety: Bill Text – AB-1399 Veterinary medicine:

veterinarian-client-patient relationship: telehealth. (ca.gov)

Proponents of AB 1399 argue that passage of this bill is necessary to make permanent the COVID-era relaxation of California's existing regulations, which permitted care virtually when local veterinary practices were inundated with new patients and human caretakers were dealing with challenging personal circumstances. They argue that California continues to deal with a shortage of veterinarians and telemedicine improves access to care for California animals, many of whom would not otherwise receive care at all. Attached are links to arguments and statements in support of the bill by Dr. Christie Long and the SFSPCA.

However, critics of AB 1399 warn of the unintended consequences of relaxing the existing regulations to California animals. In particular, the American Veterinary Medical Association has opposed the bill on this ground (**see the attached link**). While the California Veterinary Medical Association had also opposed AB 1399 (**see the attached link**), it just recently amended its position after several new amendments were made to the bill. Attached is a copy of the letter published by the CVMA explaining the change of position: AB-1399-Friedman-NEUTRAL-position.pdf (cvma.net).

For the digital health community, the adoption of AB 1399 and permanent relaxation of existing veterinary care restrictions in California would be a clear win for digital health providers seeking to expand access to veterinary care to more of the state's animal residents. The adoption of AB 1399 in this state could also have the effect of influencing other states with similar restrictions in place to also consider relaxing their regulations.

The Veterinary Virtual Care Association, a global nonprofit association dedicated to developing standards for veterinary virtual care, is actively tracking the current status of veterinary telehealth laws around the country at the following

website: The VVCA Telemedicine Regulatory Map – Veterinary Virtual Care Association. According to the VVCA's **regulatory reporting map**, Michigan, Connecticut and the District of Columbia are currently the only states not requiring that telemedicine be tied to a veterinarian-client-patient-relationship. If accurate, this means that California's adoption of AB 1399 would set an important national precedent for veterinary telemedicine law.

Last Minute Tips for Procrastinators: What Your Company Needs to Know about the California Consumer Privacy Act ("CCPA")

If your company is like many, you have known about the upcoming effective date of the California Consumer Privacy Act ("CCPA"), but are still making last minute preparations in advance of it going into effect.

If you are one of many procrastinators out there just starting to think about the law, here is a recap of some highlights for you:

- Your business is subject to the law, regardless of its location, if any one of the following is true:
    - Your company has gross annual revenues in excess of $25 million.
    - Your company buys, receives, or sells the personal information of 50,000 or more consumers,

households, or devices.
    - Your company derives 50 percent or more of its revenues from selling consumers' personal information.

- The CCPA creates new rights for California consumers: (a) the right to know; (b) the right to delete; (c) the right to opt out; and (d) the right to non-discrimination.
- You must provide notice to consumers at or before the point of data collection of the personal information to be collected and the purposes it will be used.
- You must provide clear and conspicuous notice to consumers of the right to opt out of the sale of personal information, which includes providing a "Do Not Sell My Personal Information" link on the website or mobile application.
- You must respond to requests for consumers to know, delete, and opt-out within specified timeframes (generally 45 days). Privacy settings to opt out must be treated as a validly submitted opt out request.
- You must verify the identity of consumers who make requests to know or to delete, regardless of any password-protected account settings with the business.
- You must disclose any financial incentives offered in exchange for the retention or sale of a consumer's personal information, explain how the value of the personal information is calculated, and explain how the incentive is permitted under the CCPA.
- You must make available to consumers at least two or more designated methods for submitting requests, including at a minimum a toll-free phone number, and if you maintain a website, a website address by which to submit requests. However, a business that operates exclusively online and has a direct relationship with the consumer from who it collects personal information is only required to provide an email address.

- You must make your privacy policy accessible to consumers with disabilities, or to provide consumers with disabilities information on how they can access the policy in an alternative format.
- You must make your privacy policy available in a format where consumers can print it out in a separate document.
- You must ensure that the privacy policy explains how a consumer can designate an authorized agent to make a request on the consumer's behalf.
- You must retain records of all requests and responses to requests for at least 24 months; provided that businesses that buy or sell personal information of more than 4 million consumers annually have additional reporting obligations.

Also, if your business qualifies as a "data broker" you are required to register with the Attorney General by January 1, 2020. How do you know if your business is a "data broker"? Your business knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship. Three categories of businesses are excluded from these obligations: (i) consumer reporting agencies to the extent they are covered by the Fair Reporting Act; (ii) financial institutions to the extent they are covered by the Gramm Leach Bliley Act; and (iii) entities covered by the Insurance Information and Privacy Protection Act.

The CCPA, its amendments, and regulations define more compliance obligations that businesses should be familiar with, but this list is a good starting point in advance of the effective date.

Obviously, even if your business is not subject to these laws, these privacy requirements will now constitute the best practices for doing business in California, so all businesses should seriously consider incorporating these privacy practices into their standard privacy practices and

procedures.

California Passes New Data Broker Law In Anticipation of January 1, 2020 Effective Date of California Consumer Privacy Act ("CCPA")

SaaS companies in the business of brokering data are on notice: the state of California intends to keep you on a tight leash.

In anticipation of the January 1, 2020 effective date of the California Consumer Privacy Act ("CCPA"), California took yet another bold step to protecting the personal information of Californians when it passed a new data broker law on October 11, 2019, which applies to anyone in the business of collecting and selling the personal information of consumers: **AB-1202** establishes a new compliance framework for data brokers.

What is California's New Data Broker Law?

Under the new law, data brokers will be required to register with the Attorney General, pay a registration fee, and provide their name, physical address, email, and website address, which will be publicly displayed online. Any data broker who fails to register will be (a) subject to injunction and liable for civil penalties, fees, and costs at a rate of $100 for each date that the data broker fails to register; (b) liable

for an amount equal to the fees due during the period it failed to register; and (c) the expenses incurred by the Attorney General in the investigation and prosecution of the action.

What is a Data Broker under the California Law?

What businesses are defined as "data brokers" under the law? The law defines "data broker" to mean a "business that knowingly collects and sells to third parties the personal information of a consumer with whom the business does not have a direct relationship." The law specifically excludes three categories of businesses from the definition of "data broker": (i) consumer reporting agencies to the extent they are covered by the Fair Reporting Act; (ii) financial institutions to the extent they are covered by the Gramm Leach Bliley Act; and (iii) entities covered by the Insurance Information and Privacy Protection Act. "Personal information" is defined to have the meaning provided in subdivision (o) of Section 1798.140, so publicly available information may be excluded to the extent the data is used for a purpose that is compatible with the purpose for which the data is maintained and made available in the government records or for which it is publicly maintained

California's New Data Broker Law Applies to Companies Selling Data

So, if your company is in the business of selling data in any capacity, not only do you need to prepare for the January 1, 2020 launch of the CCPA, you also need to prepare to register with the state of California as a data broker. Businesses will be required to register on or before January 31st following each year when your business meets the definition of a "data broker."

California Finalizes California Consumer Privacy Act ("CCPA")

In anticipation of the **California Consumer Privacy Act** ("CCPA") going into effect on January 1, 2020, California Governor Gavin Newsom has just signed into law seven amendments to the statute, and the California Department of Justice published the text of its new regulations to be adopted in furtherance of the CCPA.

The signed bills are as follows: **AB 25**, **AB 874**, **AB 1146**, **AB 1355**, **AB 1564,** and **AB 1130.** The text of the published regulations are made available **here**. The deadline to submit written comments is 5 p.m. on December 6, 2019. California is accepting comments submitted in accordance with the instructions posted on this Office of the Attorney General website: **https://www.oag.ca.gov/privacy/ccpa.**

So now that there is a little more statutory and regulatory clarity on what exactly will be going into effect on January 1st, 2020, SaaS and tech companies are in a better position to start preparing for the law to take effect.

CCPA Compliance Requirements

So, what does your SaaS or tech company need to know about complying with the California law as of January 1, 2020, as the California privacy laws collectively stand today?

First of all, your business will be subject to the law if at least one of the following are true:

- Your company has gross annual revenues in excess of $25

million;
- Your company buys, receives, or sells the personal information of 50,000 or more consumers, households or devices;
- Your company derives 50 percent or more of its revenues from selling consumers' personal information.

"Consumer" is currently defined as a natural person who is a California resident. "Personal information" is currently defined as any information that "identifies, relates to, describes, is capable of being associated with, or could reasonably be linked, directly or indirect, with a particular consumer or household" and includes not only name, address, and social security number, but also purchasing history or tendencies, biometric information, internet activity, geolocation data, employment information, and education information. However, publicly available information and de-identified or aggregate consumer information is now specifically excluded from the definition. "Business" is currently defined to include for-profit businesses as well as other legal entities.

CCPA Consumer Rights

Second all, California consumers are going to have certain new rights that your business will be responsible for ensuring:

- A **Right to Know** (a) the specific pieces of personal information the business has collected about the consumer; (b) the categories of personal information it has collected or sold about that consumer; (c) the purpose for which it collected or sold the categories of personal information; and (d) the categories of third parties to whom it sold the personal information.
- A **Right to Delete** personal information held by your business or by a service provider of your business; provided that, however, there will be some exceptions, where it is necessary for your business or service

provider to do any of the following: (a) complete the transaction for which the personal information was collected, fulfill the terms of a written warranty or product recall conducted in accordance with federal law, provide a good or service requested by the consumer, or reasonably anticipated within the context of a business' ongoing business relationship with consumer, or otherwise perform a contract between the business and the consumer; (b) detect security incidents; protect against malicious, deceptive fraudulent, or illegal activity; or prosecute those responsible for that activity; (c) debug to identify and repair errors that impair existing functionality; (d) exercise free speech, ensure the right of another consumer to exercise that consumer's right of free speech, or exercise another right provided for by law; (e) comply with the California Electronic Communications Privacy Act; (e) engage in public or peer-reviewed scientific, historical, or statistical research in the public interest that adheres to all other applicable ethics and privacy laws, when the deletion of the information is likely to render impossible or seriously impair the achievement of such research, if the consumer has provided informed consent; (f) to enable solely internal uses that are reasonably aligned with the expectations of the consumer based on the consumer's relationship with the business; (g) to comply with a legal obligation; or (h) to otherwise use consumer's personal information, internally, in a lawful manner that is compatible with the context in which the consumer provided the information. If you or your service provider does not delete consumer's information upon request, you must inform the consumer as to why and notify the consumer of any rights he or she has to appeal the decision, and you must do it within the timeframe you would have had to delete the information.

- A **Right to Opt Out of the Sale** of personal information.

"Sale" is defined to include selling, renting, releasing, disclosing, disseminating, making available, transferring, or otherwise communicating orally, in writing, or by electronic or other means, a consumer's personal information by the business to another business or a third party for monetary or other consideration. The proposed regulations provide more clarification on the practices businesses should follow to ensure this right to opt out of the sale. In the case of children under the age of 16, your business cannot sell their personal information unless they have opted-in to the sale. In the case of children under 13, a parent or guardian must opt-in on behalf of the child. The proposed regulations further define the rules related to the protection of children.

- A **Right of Non-Discrimination**. Your business will be prohibited from discriminating against a consumer for exercising his or her rights under the CCPA. Discrimination will be defined to include denying goods or services to the consumer, charging different prices or rates for goods or services, providing a different level or quality of goods or services to the consumer, or suggesting that the consumer will receive a different price or quality of goods or services; provide that you will be able to charge a different price or rate, provide a different level or quality of goods or services, or offer financial incentives if the difference is reasonably related to the value provided to the business by the consumer's personal data, so long as the business practice is not unjust unreasonable, coercive, or usurious in nature. The proposed regulations further define how the right of non-discrimination will be implemented.

CCPA Business Obligations

Third, businesses will now have other new business obligations

to consumers, including the following:

- Provide notice to consumers at or before the point of collection of the categories of personal information to be collected from them and the purposes they will be used.
- Provide clear and conspicuous notice to consumers of the right to opt-out of the sale of personal information in the form of a "Do Not Sell My Personal Information" link on their website or mobile application.
- Respond to requests from consumers to know, delete, and opt-out within the specified timeframe (generally 45 days). The proposed regulations require businesses to treat privacy settings to opt out selected by a consumer as a validly submitted opt out request.
- Make available to consumers at least two or more designated methods for submitting requests for information, including at a minimum, a toll-free phone number, and also specify other business practices for handling requests by consumers.
- Verify the identity of any consumer making a request to know or delete. Password protected account settings are not considered sufficient verification. The proposed regulations require a business unable to verify a request to comply to the greatest extent it can even if it denies a request.
- Disclose financial incentives offered in exchange for the retention or sale of consumer's personal information (as specified by the proposed regulations), including a short summary of the incentive, a description of the summary and the categories of personal information impacted, an explanation of how a consumer can opt-in to the incentive, a notice to consumer that he or she has the right to withdraw at any time and how he or she can exercise this right, and an explanation of why the incentive is permitted under California privacy law.
- Retain records of all requests and responses to those

requests for at least 24 months; provided that businesses (alone or in combination) collecting, buying or selling the personal information of more than 4 million consumers annually are subject to extra recordkeeping obligations.

- Disclose a privacy policy which describes consumer's rights under California privacy law, how to submit requests to exercise rights under California privacy law, and information regarding their data collection and sharing practices. The proposed regulations define additional requirements for the privacy policy, including that it must be accessible to consumers with disabilities or provide consumers with disabilities information on how they can access the policy in an alternative format; that it must be in a format where consumers can print it out as a separate document; it must explain the right of a consumer not to receive discriminatory treatment; and it must explain how a consumer can designate an authorized agent to make a request on the consumer's behalf under California privacy law.
- Train employees or contractors handling consumer requests on compliance with California privacy law and directing consumers to exercise their rights under California privacy law; provided that businesses collecting, buying or selling the personal information of more than 4 million consumers are subject to higher training obligations.

CCPA Conflicts with GDPR

Fourth, businesses are now going to have to reconcile the requirements of the European Union's General Data Protection Regulation ("GDPR") with California's privacy laws. In particular, California's Department of Justice has advised businesses to be wary of the following:

- Data inventory and mapping of data flows to demonstrate

compliance with the GDPR may have to be re-worked to reflect the different requirements of California.

- Processes and/or systems set up to respond to individual requests for access to or erasure of personal information will need to be reviewed in order to apply different definitions of what constitutes personal information and different rules on verification of consumer requests.
- Contracts with service providers or data processors adopted to comply with the GDPR may need to be rewritten to reflect the requirements under California law.

Regardless of whether your SaaS or tech company is going to meet the threshold to be subject to the new California law when it goes into effect, it would be prudent to start incorporating these new requirements into your company's privacy practices and procedures, since they will at the very least become the new best practices for businesses serving California consumers effective January 1, 2020. It goes without saying that companies who will be subject to the law when it goes into effective need to take steps to become compliant immediately, as the law is set to go into effect in less than 75 days.

If you have questions regarding the CCPA and your company's compliance obligations, schedule a consultation with today at this link.

Software Industry Concerned About the Potential Impact of

AB-5 on Gig Economy

The Software Industry is closely following legislation in California that, if passed, could have a huge impact on Gig workers and the software companies that rely on them.

The legislation at issue is AB 5, which would codify and expand the California Supreme Court's recent decision in **Dynamex Operations v. Superior Court** (2018) 4 Cal. 5th 903. The text of the proposed legislation is available **here**.

According to **The Intercept**, the bill was sponsored by Lorena Gonzalez, a Democratic assemblywoman from San Diego. **The Intercept** reports that that California is losing an estimated $7 billion in payroll tax annually due to the misclassification of employees as independent contractors, so the state is eager to close the loophole.

Obviously, Uber and Lyft, directly oppose the legislation, since it would directly impact their current Gig worker business model. In fact, **The Los Angeles Times** has reported that Uber and Lyft have actually paid drivers to organize protests against the legislation.

For Uber and Lyft, the obvious concern is that the passage of AB-5 in California could prompt other states to pass their own versions of the legislation, or even, that similar legislation could be passed at the federal level, which could potentially expand the impact of the legislation far beyond the borders of California.

Both **The Intercept** and **The Los Angeles Times** are reporting that Uber and Lyft have each warned investors of this potential risk in recent regulatory filings. Indeed, an investment publication, **Investorplace**, warns that the passage of the bill will have a very detrimental impact on both companies.

The bottom line is that software companies who have built business models around the Gig worker model may soon be forced to either cease operations in California or, alternatively, to change their models for the state, if AB-5 is passed and signed into law, so if your company has been developed around this model or you are building a company relying on this model, you will want to follow this legislation closely as it moves through the California legislature.

The Prinz Law Office Announces Launch of New Alternative Billing Plans

Press Release 10.3.18

News Update on California Legislature Considering Passage of SB 822 to Restore Net Neutrality

News Update on SB 822

California Adopts Smartphone Killswitch Law

California has adopted a law that require smartphones sold in the state to have smartphone kill settings enabled as the default settings on the phone. The Silicon Valley Software Law Blog explores the impact of this legislation in the link set forth below:

http://www.siliconvalleysoftwarelaw.com/california-adopts-smartphone-kill-switch-law

---

California Lawyer Reporter Jeanette Borzo Interviews Internet Lawyer Kristie Prinz in “The Search for Intelligent Life in the Blogosphere”

Click here to read interview.

Biotech and Life Sciences IP Licensing Lawyer Kristie Prinz to speak at PepTalk IP Panel Presentation on Biotech/ Pharma Processes

Biotech and Life Sciences IP Licensing Lawyer Kristie Prinz speak on January 11, 2008 on the IP Panel for Process Management—*Route to Success* at PepTalk which will be held at Hotel Del Coronado, San Diego.

For more details about the event, please click here.

Patent Licensing Attorney Kristie Prinz Shares Presentation on A Tale of Two Patent Infringement Cases and Their Impact on the VoIP Industry

A Tale of Two Patent Infringement Cases and Their Impact on the VoIP Industry (Powerpoint Presentation 160 Kb)

Internet Lawyer Kristie Prinz Speaks on Hottest Topics in Cyberspace—Verizon v. Vonage and Sprint v. Vonage: A Tale of Two Patent Infringement Cases and Their Impact on the VoIP Industry

Internet Lawyer Kristie Prinz will speak at the State Bar of California Annual Meeting in Anaheim on September 29, 2007.

Please click here to view the Powerpoint presentation.

Internet Lawyer Kristie Prinz Shares PowerPoint on Recent Developments in Blog Law

Recent Developments in Blog Law (PDF, 160Kb)

Silicon Valley Internet Lawyer Kristie Prinz to Speak on Recent Developments in Blog Law

Silicon Valley Internet Lawyer Kristie Prinz will be speaking on Recent Developments in Blog Law on June 14, 2007 at the Silicon Valley Capital Club.

State Bar of California, Business Section Cyberspace Committee. Please click here to view the Powerpoint presentation.

Internet Lawyer Kristie Prinz Shares PowerPoint on Hottest Topics in Cyberspace: Cyberinsurance, Blogs, and On-Line Advertising

Hottest Topics in Cyberspace: Cyberinsurance, Blogs, and On-Line Advertising (PowerPoint Presentation 114Kb)

Silicon Valley Internet Attorney Kristie Prinz to Speak on Hottest Topics in Cyberspace: Cyberinsurance, Blogs, and On-Line Advertising

Silicon Valley Internet Attorney Kristie Prinz to Speak on Hottest Topics in Cyberspace on January 20, 2007 at the Section Education Institute, State Bar of California, Claremont Resort and Spa, Berkeley, CA. Please click here for details. Please click here to view the PowerPoint presentation.

Internet Lawyer Kristie Prinz to Speak on What You Need to Know about CAN-SPAM

Internet Lawyer Kristie Prinz will be speaking on a panel presentation on “What You Need to Know About CAN-SPAM” on June 8, 2004 at Pillsbury Winthrop LLP. The event is a brown bag lunch co-sponsored by the Santa Clara County Bar Association and California State Bar Business Section Cyberspace Law Committee.