SaaS Contracts Attorney Kristie Prinz to Present on “Negotiating SaaS Agreements” for Clear Law Institute

Silicon Valley SaaS Contracts Lawyer Kristie Prinz will present a webinar on “Negotiating SaaS Agreements: Drafting Key Contract Provisions, Protecting Customer and Vendor Interests” on February 8, 2019 at 10:00 a.m. PST/1 p.m. EST. The program will be sponsored by Virginia-based Clear Law Institute, which is making available a 35% discount off the registration fee if you use the discount code KPrinz148075. To register, please sign up here: https://clearlawinstitute.com/shop/webinars/negotiating-saas-agreements-drafting-key-contract-provisions-protecting-customer-and-vendor-interests-020819/.

Recent FTC Enforcement Provides Warning to Other Tech Companies

If your company has either pursued Privacy Shield certification, or publicly claimed to be in pursuit of Privacy Shield certification, recent enforcement action by the Federal Trade Commission (“FTC”) should put your company on notice that failure to maintain your certification may render you subject to FTC enforcement activity if you continue to make representations on the Internet or in advertising

materials related to Privacy Shield.

The FTC has just **announced** settlements with four companies, IDmission, LLC, mResource LLC (doing business as Loop Works LLC), SmartStart Employment Screening, Inc., and VenPath, Inc. on allegations related to EU-U.S. Privacy Shield compliance.

The FTC's **complaint** against IDmission, LLC, which is a cloud-based technology platform, focuses on the company's website representations of compliance with the EU-U.S. Privacy Shield framework despite the company's failure to actually complete the certification process. In contrast, FTC's complaints against **mResource**, **SmartStart**, and **VenPath**, which are companies providing talent management and recruiting services, employment and background screening services, and data analytics services respectively, all focus on the companies' website representations of Privacy Shield certification despite failing to maintain the certification.

The settlements now render these four companies subject to direct FTC oversight and monitoring with respect to their advertising and compliance activities going forward.

From this enforcement action, it is clear that the FTC is on the lookout for companies who are making claims about the EU-U.S. Privacy Shield that they are not actually meeting, and that the FTC is prepared to exercise its enforcement authority against any company that fails to meet its representations as they pertain to Privacy Shield.

So, software companies, the FTC is putting you on notice: you need to self-monitor your Privacy Shield certification and ensure that you maintain the certification at all times, and to ensure that you are compliant with certification requirements, particularly if you are making advertising-related representations related to Privacy Shield. The FTC is watching.

Are Unethical App Subscription Prices ruining the App Store?

Tech Crunch and **Forbes** recently reported on a problem plaguing the App Store: unethical subscription practices.

According to **Tech Crunch**, commonly utilized unethical practices include as follows:

- that the apps are too aggressive in obtaining subscriptions;
- that the apps offer little functionality without upgrading;
- the apps provide no transparency around how free trials work;
- and the apps make it difficult to stop subscription payments.

Both **Tech Crunch** and **Forbes** note that the App Store has established published **Guidelines for App Store Review**, which specifically includes a **Developer Code of Conduct** that states:

> *Customer trust is the cornerstone of the App Store's success. Apps should never prey on users or attempt to rip-off customers, trick them into making unwanted purchases, force them to share unnecessary data, raise prices in a tricky manner, charge for features or content that are not delivered, or engage in any other manipulative practices within or outside of the app.*

So, if Apple requires adherence to a code of conduct, why is it alleged that unethical subscription practices are still so

rampant on the App Store? And why hasn't the Federal Trade Commission ("FTC") stepped in, or more state attorney general offices intervened? It is unclear, since as **Forbes** argues, the more these practices are allowed to continue, the more the practices are likely to detrimentally affect the entire App Store market. As both **Tech Crunch** and **Forbes** have pointed out, the App Store is full of reviewer complaints about the specific practices of various apps, so at least Apple has definitely been on notice that there was a problem. Presumably the FTC and at least one or two state attorney general's offices have been made aware of these issues as well.

As a Silicon Valley SaaS and software licensing attorney, however, I would encourage App developers profiting off practices that seem questionable or are the targets of a significant number of annual complaints to consider modifying those practices as quickly as possible, as you and your business run the risk of not only attracting a lawsuit by the FTC or an attorney general's office but you also run the risk of attracting a class action suit on behalf of subscribers who were allegedly harmed by your App. This type of suit is not without precedent, and could come with a significant damage award. Your subscription terms do matter and they need to be viewed as fair and reasonable to your subscribers. You are on notice: these practices are being brought under scrutiny by the press and scrutiny by regulators, states, and class action attorneys is likely to soon follow.

California Agrees to Delay

Enforcement of Net Neutrality Law

The State of California has just agreed to delay the enforcement of S. B. 822, also known as the California Internet Consumer Protection and Net Neutrality Act of 2018, until litigation is decided regarding whether the FCC can preempt state net neutrality laws is decided by the US Court of Appeals for the District of Columbia Circuit. Attached is a copy of the **stipulation and agreement** filed in the US District Court for the Eastern District of California. As **Ars Techica** reported, California has agreed to refrain from enforcement of the law until after the US Court of Appeals case has been decided and any appeals have been exhausted.

As the **Washington Post** reports, the outcome of the case before the D.C. Circuit could result in the rejection of the FCC's 2017 rule change, which then would mean that S.B. 822 would become redundant. However, both the **Washington Post** and **Fortune** are reporting that the D.C. Circuit could rule on the issue of preemption as well, which could potential impact S. B. 822 and other similar state laws.

Silicon Valley SaaS Attorney Kristie Prinz to Speak at Webinar on "Negotiating SaaS

Agreements: Drafting Key Contract Provisions, Protecting Customer and Vendor Interests”

Silicon Valley SaaS Attorney Kristie Prinz will present a webinar on “Negotiating SaaS Agreements: Drafting Key Contract Provisions, Protecting Customer and Vendor Interests” on October 26, 2018 at 10:00 a.m. The program will be sponsored by Virginia-based Clear Law Institute. To register for the event, sign up at https://clearlawinstitute.com/shop/webinars/negotiating-saas-agreements-drafting-key-contract-provisions-protecting-customer-and-vendor-interests-102618/. Clear Law Institute has made available a discount code for the course: you can receive a 35% discount with the promo code: KPrinz119433.

Why SaaS Companies Need to Anticipate Insurance Requirements in Advance of Negotiations

If your SaaS company is like most, you postpone the procurement of insurance policies until you absolutely have to obtain them, expecting to be able to obtain whatever you need on demand.

However, if your SaaS company anticipates a significant deal is on the horizon, you should be anticipating your needs in advance of actually starting those negotiations, or you may find yourself in a situation where you have to commit to maintaining insurance during the relationship that you may not actually be able to buy on the open market. Why is this a problem? Well, this puts you in the position of potentially breaching the terms of the "significant" deal before you ever start performing those terms, which can obviously have serious consequences for your company's business if your breach is ever discovered. Since the usual insurance terms in these types of deals require the submission of certificates of insurance as proof of coverage, any failure to procure the insurance required is not likely to stay undiscovered for an extended period.

Notwithstanding the foregoing, even if you do not breach the terms of the negotiated deal, it is far better to negotiate the scope of indemnification risks you will be incurring with advance knowledge of the terms of the insurance policies you already have in place, as you can then negotiate limits of liability within the coverage of the insurance coverage previously obtained.

So, what types of insurance requirements should a SaaS company anticipate when it goes to negotiate a significant deal?

First and foremost, SaaS companies should anticipate the requirement of a general commercial liability policy. This is a standard commercial insurance policy that every business, regardless of whether or not in the software industry, should keep.

Second of all, SaaS companies should anticipate the requirement of a commercial auto insurance policy to cover the risk that employees or contractors may have an accident while traveling back and forth to a customer or business partner's work site.

Third of all, SaaS companies should anticipate the requirement of an errors & omissions policy to cover the risk that company workers will intentionally or negligently act in a way that harms the customer or business partner.

Fourth, SaaS companies should anticipate the requirement of a cyberinsurance policy to cover the risks of hack attacks, data breaches, and third party cybercrimes, as well as notification costs and other costs to remedy a breach after it occurs.

Fifth, SaaS companies should anticipate the requirement of an umbrella policy to cover losses in excess of the insurance limits available.

What types of limits of coverage should a SaaS company anticipate? In my experience, larger deals will come with larger expectations, so the more significant the deal, the more insurance your company should be lining up in advance.

The bottom line is that doing some advance planning with respect to insurance before your software company commences negotiations on a significant deal will save your company the worry down the road of being discovered to be in breach of the deal you just closed if you find that meeting the insurance requirements you agreed to is not quite as easy as you anticipated. Furthermore, it will enable you to go into negotiations better prepared to be able to negotiate terms that actually protect your company.

If you have questions about your SaaS company’s insurance planning, please schedule a consultation today at **https://calendly.com/prinzlawoffice**.

California Governor Signs Net Neutrality Law

Governor Jerry Brown has signed into law **S.B. 822,** also known as the California Internet Consumer Protection and Net Neutrality Act of 2018. The law is intended to go into effect on January 1, 2019 and, according to **CNN**, will establish the "strictest net neutrality protections in the country."

However, the U.S. government has responded to the California action by seeking a preliminary injunction to block the law from going into effect. A DOJ press release announcing the suit is attached **here,** in which the DOJ asserts that "Once again the California legislature has enacted an extreme and illegal state law attempt to frustrate federal policy."

However, according to the **Electronic Frontier Foundation**, the core argument by the DOJ and FCC articulated in the court filings is not that states cannot pass net neutrality laws but that a pending lawsuit in the D.C. Circuit filed by the California Attorney General challenging the FCC's repeal of net neutrality should be decided before the legality of the passage of the California Internet Consumer Protection and Net Neutrality Act of 2018 can be decided.

Wired reports that the dispute between California and the federal government "raises novel questions about the relationship between the federal government and the states." At the heart of the dispute is whether California has the legal right to pass a law on net neutrality, and whether the FCC has the legal right to prevent states from adopting net neutrality laws. While in general pre-emption only occurs when there are incompatible state and federal rules, **Wired** reports that "[i]t's not unheard of for the federal government to preempt state or local regulations when those regulations conflict with federal policy, even when the federal policy is

not to regulate." In contrast to the current facts, however, **Wired** reports that the past example of this type of pre-emption involved a decision by Congress as opposed to a federal agency.

Clearly, California and the federal government are now headed for a legal show-down in federal court. The Silicon Valley Software Law Blog will keep you posted as the legal battle further develops.

Why Big Development Projects Can Equal Big Legal Headaches without Well-Drafted Agreements

If your company has just landed a big tech or software development project for a third party, do not underestimate the importance of the agreement in protecting the revenue stream you are being offered in exchange for your development services.

The typical tech or software development agreement requires lump sum payments in installments throughout the term of the relationship. Also, the typical development agreement will have at most a statement of work connected with the project and will rarely be accompanied by technical specifications or milestones, with respect to which approval can be sought at the various phases of the development.

Why can this be a problem? Well, if your company agrees to take on a large tech or software development project and has

not defined contractually in detail the technical specifications and standards required to be performed, or developed detailed milestones that can be tied to satisfaction of particular phases of the project, how exactly can you prove that you earned the money paid in installments if the customer pulls the plug on the project at any stage? How exactly do you prove that you fulfilled your responsibilities with respect to the development project if you never actually reached agreement as to the technical terms of the development project?

The reality is that it can be very hard to enforce an agreement when the key terms of the relationship were never actually memorialized in writing. While the risk of not being able to enforce your agreement may be low in low dollar value development projects, that risk escalates dramatically as the dollar value of the project also increases into the hundreds of thousands of dollars or even millions.

In general, when I see disputes involving tech or software development projects, the dispute can almost always be attributed to a poorly drafted agreement between the parties.

So, what can you do to minimize your risks of taking on a tech or software development project?

First and foremost, obtain help from experienced technology transactions counsel when your company is first approached with a potential development project. An experienced attorney in this space can guide you through the negotiation process at the early stages, so that you don’t have to renegotiate terms that have already been agreed to by the potential development partner. It can be very hard to get partner buy-in on developing and memorializing good technical terms when the parties are already weeks or months into the negotiation the deal.

Second of all, ensure that the technical specifications and

requirements for the project have been defined in detail, and develop milestones throughout the development process, which can be approved. Also, develop a process that is very well-defined within the contract to obtain that approval. If a specific timeline is required at any part of the process, develop terms that reflect the agreed upon timeline as well.

Third, instead of merely requiring payment by installments through the development work, develop payments that are tied to the accomplishment of specific well-defined milestones, in order to ensure that your company is can prove that any payment received was earned a s a result of the successful accomplishment of the applicable milestone(s).

The bottom line is that a big tech or software development project should be accompanied by a very detailed, technically-specific development agreement if a company prefers to avoid big legal headaches down the road. It is in your company's best interest to ensure that any development agreement that the parties execute is drafted to protect the anticipated revenue stream from the development project.

If your company is contemplating a tech or software development project and is concerned about avoiding future legal headaches, schedule a consultation today at **https://calendly.com/prinzlawoffice**.

The Prinz Law Office Announces Adoption of New

Subscription Billing Plan

Prinz Law Announcement 10.3.18

Advertisement for Upcoming Webinar on Negotiating SaaS Agreements Sponsored by Clear Law Institute

Webinar Mailer 10.26.18

The Prinz Law Office Announces Launch of New Alternative Billing Plans

Press Release 10.3.18

The Prinz Law Office to Launch New Alternative Billing Solution

The Prinz Law Office is pleased to announce the launch of a new alternative legal billing solution for our clients in the software/SaaS, tech and health tech/digital health, and IT/healthIT industries: the subscription billing model. We have been following the recent popularity of this model with California companies, and have decided to adopt our own version. We believe that it may be a good fit for clients with ongoing firm needs, particularly in the transactional space. Our new plans will be based on daily and half-daily billing, eliminating traditional hourly timekeeping for clients who choose this option. For more information on how a subscription solution would work, please contact Kristie Prinz at kprinz@prinzlawoffice.com or 408.884.854.

Top Mistakes Made in SaaS Customer Deals

What are the top mistakes the average company will make when it enters into a SaaS deal, when the company has not involved an experienced SaaS lawyer early in the negotiations?

Companies Negotiate with the Wrong Technology Contract

First and foremost, the most common mistake with all types of technology negotiations, but especially with negotiations in

the SaaS space, is that companies handling their own SaaS negotiations often end up negotiating with the wrong contract as the starting point. For example, the parties may negotiate from a software license template when they need a SaaS agreement template instead, or they may negotiate from a master services agreement or a hosting agreement when the deal they were doing actually involved SaaS terms. A knowledgeable software attorney will know and understand that the terms of a well-drafted template will be completely different based on the technology model under negotiation and will be able to ask the right questions in order to identify the right technology model and therefore the necessary baseline terms that need to be addressed in a well-drafted agreement.

Companies Negotiate with the Right Technology Contract But One that was Written for a Different Product or Relationship

Another common issue is that even if the parties choose the right initial type of contract to begin the negotiations with, they begin the negotiation with a template that was designed for an entirely different product or relationship than what is currently being contemplated: a SaaS agreement transaction. Obviously, it is going to require less negotiation to reach a good deal when the starting point for the negotiation is a set of proposed terms that applies to the right type of technology transaction and the particular product or relationship under negotiation. Also, the terms of the signed contract are far more likely to be meaningful when they were developed around the right product and services. Otherwise, they are likely not to include the key deal terms or contemplate any of the issues that could come up between the parties. The firm sees many signed contracts that are little better than a handshake because the terms agreed to are almost completely irrelevant to the transaction. An experienced SaaS attorney is going to be able to ask the right questions to determine whether the contract terms were written for the appropriate product or

services.

The Contracts Do Not Sufficiently Contemplate how the Relationship will Evolve

A third issue is that the contracts do not sufficiently contemplate how the relationship will evolve over time. A standard practice in the industry is to rely exclusively on a list of prices to determine on the fee-related issues in the agreement. What is typically missing is all the terms that explain how the pricelist will be implemented. While this might not be fatal to the relationship if there is some sort of initial agreement on the price to be paid overall, few SaaS business relationships are up-front, fixed price relationships. Most relationships now are intended to generate recurring revenue streams and anticipate new fees as new seats, services, and functionality are added. So, a mere pricelist is almost never adequate to support an ongoing relationship. Thus, if an experienced SaaS attorney is not involved with the deal, there is a high likelihood that the contract signed will not have all the necessary terms to explain precisely how all the fees will be assessed going forward.

They Overlook the Technical Concerns About the Transaction

A fourth issue typically overlooked by a SaaS contract negotiated without the assistance of experience SaaS counsel are all the technical concerns about the transaction. In many software deals, the service level is absolutely critical to the transaction. However, more often than not, the service level agreement being relied on by the parties was copied off the Internet and has absolutely no significance or relevance to the service being offered or provided. Also, even where the service level agreement was obtained in a more thoughtful way, it is very common to find the agreement full of terms that are so poorly written or that have so many carve-outs

that it is completely unenforceable. In addition, many relationships contemplate the performance of a variety of services which are never addressed in the contract at the technical level required to reach any sort of understanding regarding those services. An experienced SaaS counsel will be able to ask the right questions to understand all the technical aspects of the deal between the parties and will be able to determine all the terms that have been omitted from the contract before it is executed.

They Fail to Contemplate the Possibility of Suspension of Services

A fifth issue typically missed when a contract is negotiated without the assistance of experienced counsel is the contemplation of all the issues that could arise with regard to the suspension of services. Today, the service provider frequently has the ability to "suspend" a company's access to the software and the data stored therein at any time and could just as easily erase all of that data. However, few contracts that the firm sees really address the issue of suspension at the level required to address all possible issues that could arise between the parties. An experienced SaaS counsel will ask the right questions to identify these issues and address them in the contract.

They are Overly Focused on the Negotiation of the Indemnification Clause

A sixth mistake is contracts that contain elaborately negotiated indemnification clauses but never really contemplated all the related issues such as whether the indemnification could ever be enforced and whether the focus of the indemnification clause negotiated was on the liabilities most relevant to the transaction. An experienced SaaS counsel will be knowledgeable about software indemnification clauses and all the issues relevant to the clauses in order to ensure that the maximum amount of

protection is in place.

The bottom line is that an experienced SaaS counsel understands technology sufficiently to ask enough questions about the relationship envisioned to determine all the key terms that were never contemplated in the agreement, and can add that additional level of skill and expertise to the negotiation of the deal that a general business lawyer or business person simply cannot. Technology deals are fundamentally technical and only someone that understands technology and technical deals sufficiently is going to be able to evaluate proposed terms sufficiently to negotiate them appropriately in order to look after the party's best interests.

Does your company have a SaaS deal on the table right now that you are trying to negotiate? Schedule a consultation with experienced SaaS counsel today at this link.

Should a Federal Privacy Bill Pre-empt California Data Privacy Law?

USA Today is reporting that multiple technology and telecommunication companies are lobbying Congress to pass federal privacy legislation that would pre-empt the new privacy law recently passed in California which grants sweeping protections to consumers. In particular, **USA Today** reports that Amazon, AT&T, Apple, Google, Twitter and Charter Communications are leading the lobbying effort and argue that inconsistent state laws will "make it tough for companies to operate" and would "threaten innovation."

Of course, as **USA Today reports**, the lobbying companies are seeking weaker regulations than exist in the European Union or that were just passed in California, with the sole exception of Apple, which relies on a different business model and was reportedly the only company "at the hearing to argue that the bar for federal legislation should be set "high enough" to protect consumers." As **The New York Times** reported, the goal of the tech industry is to institute federal rules that would give technology companies wide leeway over how personal information is handled. **The Electronic Frontier Foundation** describes the tech industry's goal as "neuter[ing]" California for a weaker law at the federal level.

According to **The New York Times**, however, the tech industry's efforts are not limited to just federal lobbying efforts. In fact, **The New York Times** reported that lobbying efforts are underway in California as well, and that the California Chamber of Commerce and other business and tech groups have just submitted nineteen pages of bill edits to State Senator Bill Dodd, one of its authors. In addition, **The New York Times** reports that the groups are also asking California to delay enactment for a year.

The bottom line is that the tech and telecommunication industries are actively lobbying at both the federal and state levels to ensure that California's new privacy law never goes into effect in its current form. Convincing Congress to pass a federal law that they hope to be able to influence and s

---

Should Your Company Utilize a

Source Code Escrow Agreement in your next SaaS Customer Contract?

If your company is a SaaS company, you may come across a customer or prospective business partner who insists on the inclusion of a source code escrow agreement as part of the deal terms. If this scenario arises, you may be inclined to immediately agree to the prospective customer or business partner's terms in order to close the deal you are negotiating. However, what are the five things your SaaS company needs to know about source code escrow before you agree to include source code escrow in the terms of a transaction?

Choose a Source Code Escrow Product Intended for SaaS Companies

First of all, you should know that the standard source code escrow product was not designed for SaaS and is probably not going to be very effective for a customer or business partner if they ever need to rely on it. The traditional source code escrow offering was intended for a traditional software product, which is downloaded to hardware and is updated or upgraded on a periodic basis. In the traditional source code escrow agreement, the deposit materials are generally only updated a few times a year. However, in the SaaS product scenario, the product is often updated on a continuous basis, so updating the deposit materials only a few times a year is unlikely to be sufficient. Similarly, in a traditional source code escrow agreement, the backup and storage of the data is unlikely to be addressed. However, in the SaaS agreement scenario, the customer or business partner is unlikely to have access to the data in the cloud, so the party receiving access to the deposit materials is more likely to expect the backup

and storage of SaaS data to be a key component of the escrow relationship.

For this reason, many technology escrow companies are offering a special escrow products intended for SaaS only, which provide for the continuous update of deposit materials and include data as part of the deposit materials. The SaaS version of the escrow product is more likely to provide uninterrupted access to the full set of materials that the customer or business partner previously had access to in the cloud, so it is likely to be the better fit for the customer or partner seeking source code escrow as part of the deal terms.

Anticipate that SaaS Source Code Escrow Products Will be More Expensive

Secondly, you should know that the SaaS version of the source code escrow product will likely be more expensive than the traditional product since it is going to be a more labor-intensive solution. A source code escrow company can expect in a SaaS product scenario to perform significantly more services to ensure that the escrow works if needed than it would have had to perform in a traditional software scenario, given the ongoing nature of the updates and upgrades. As a result, the costs of SaaS escrow are likely to be significantly higher than traditional software escrow, which should certainly be contemplated in the allocation of escrow costs between the parties.

Obtain License Rights to Use the Escrowed Source Code in a Release Scenario

Third, you should know that you may not be able to obtain the rights you are seeking to use the escrowed code in a release scenario. In SaaS, users typically receive access rights rather than license rights to the use of the intellectual property. As a result, a SaaS provider can build products

that incorporate open source code and offer access rights to the end product, even though the provider is prohibited from distributing the software otherwise. The SaaS provider can also incorporate third party code into the product that cannot be sublicensed to third parties, even in an escrow scenario. So, it is certainly possible that the SaaS provider will not have the necessary rights in the SaaS product to be able to authorize the license grant to the escrowed materials, which could potentially result in the customer or business partner receiving physical copies of the source code and data but not having the rights necessary to use the copies procured.

Address Transitioning Services and Know-How Transfer in Source Code Escrow Agreement

Fourth, you should consider that mere possession of a functional copy of the source code and data may not be sufficient for a customer or business partner to continue using the software and applicable data in the event of a release condition. In fact, the customer or business partner may require transitioning services or access to the SaaS provider's know-how before it is able to resume use of the software. Consequently, transitioning services and know-how transfer may be important considerations that need to be addressed in any escrow terms.

Contemplate the Responsibilities and Liabilities of the Respective Parties Regarding Data and Potential for Data Breach as Well as the Availability of Cybersecurity Insurance

Fifth, you should consider that the very nature of SaaS escrow may result in the escrow provider having control over any collected data uploaded to the SaaS product and that the escrow provider could be vulnerable to a data breach arising from the acts or omissions of an employee or third party. Thus, the deal terms should contemplate the responsibilities and liabilities of the respective parties regarding the data

and the potential for a data breach, as well as any available insurance coverage to protect against this risk.

Will SaaS Source Code Escrow Will Meet Your Needs?

All in all, while escrow products are now available and on the market, which may meet the needs of a prospective customer or business partner seeking source code escrow to a SaaS product, a SaaS provider will have a variety of considerations to contemplate before acquiescing to such demands in a negotiation. In the end, the decision of whether or not to agree to escrow terms should be based on a careful evaluation of all of the above considerations.

If your SaaS customer is asking to include source code escrow in a transaction, or you are contemplating the pros and cons of proposing it to close a customer deal, schedule a consultation today to discuss how source code escrow agreements might work in your transaction at this link.

What SaaS Companies Need to Know about Source Code Escrow Agreements

If you run a SaaS company, you may come across a negotiation where a prospective customer or business partner insists on the inclusion of source code escrow in the deal terms. However, the traditional source code escrow product is unlikely to provide the protections that your prospective customer or business partner is seeking. The Silicon Valley Software Law Blog addresses the issue of source code escrow products designed for SaaS products and what SaaS companies

need to know about them in the following blogpost:

http://www.siliconvalleysoftwarelaw.com/what-saas-companies-need-to-know-about-source-code-escrow-agreements/

News Update on California's Enactment of Landmark Data Privacy Law

News Update 6.29.18

In the Aftermath of GDPR, California Passes Consumer Privacy Act of 2018

Software companies are still taking steps to comply with the European Union's General Data Privacy Regulation ("GDPR"), which just recently went into effect, but they now are facing the prospect of having to comply with a law closer to home: California's New Consumer Privacy Act of 2018. The Silicon Valley Software Law Blog discusses this development at the following blogpost:

http://www.siliconvalleysoftwarelaw.com/in-aftermath-of-gdpr-california-passes-consumer-privacy-act-of-2018/

Silicon Valley Software & Technology Lawyer Kristie Prinz to Speak at Upcoming Webinar on “Negotiating SaaS Agreements”

Press Release 6.26.18

SaaS Contracts Lawyer Kristie Prinz to Speak on “Negotiating SaaS Agreements”

Silicon Valley SaaS Contracts Lawyer Kristie Prinz will present a webinar on “Negotiating SaaS Agreements: Drafting Key Contract Provisions, Protecting Customer and Vendor Interests” on October 26, 2018 at 10:00 a.m. The program will be sponsored by Virginia-based Clear Law Institute. To register for the event, sign up at https://clearlawinstitute.com/shop/webinars/negotiating-saas-agreements-drafting-key-contract-provisions-protecting-customer-and-vendor-interests-102618/. Clear Law Institute has made available a discount code for the course: you can receive a 35% discount with the promo code: KPrinz119433.

SaaS Lawyer Kristie Prinz to Speak on “Negotiating SaaS Agreements: Drafting Key Contract Provisions, Protecting Customer and Vendor Interests”

SaaS Lawyer Kristie Prinz will present a webinar on “Negotiating SaaS Agreements: Drafting Key Contract Provisions, Protecting Customer and Vendor Interests” on June 11, 2018 at 10:00 a.m. The program will be sponsored by Virginia-based Clear Law Institute. To register for the event, sign up at the Clear Law Institute website.

News Update on California Supreme Court Ruling Establishing New Independent Contractor Test

News Update 5.3.18

California Supreme Court Ruling To Have Long Term Impact on Silicon Valley Reliance on Gig Workers

If your Silicon Valley company relies on Gig workers as part of its business model, then the California Supreme Court's ruling is likely to have significant consequences for your business. The Silicon Valley Software Law Blog discusses this ruling at the following blogpost:

http://www.siliconvalleysoftwarelaw.com/california-supreme-court-strikes-blow-to-software-industry-reliance-on-gig-workers/

News Update on the U.S. Supreme Court Decision Affirming the Constitutionality of Inter Partes Reviews

News Update 4.25.18

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

News Update on SB 822

News Update Regarding Challenge to the EU-U.S. Privacy Shield Framework

News Update

News Update on Recent Webcast by Kristie Prinz: “Drafting Software Agreements for ASP &

SaaS Hosting”

Drafting Software Hosting Agreements for ASP & SaaS Hosting

California Contemplates Passage of State Net Neutrality Bill

With the impending repeal of net neutrality at the federal level, California is currently considering the passage of a net neutrality bill to restore net neutrality at the statewide level. The Silicon Valley Software Law Blog discusses the proposed bill at the following blogpost:

http://www.siliconvalleysoftwarelaw.com/california-to-consider-bill-that-restores-net-neutrality/

European Court to Hear Challenge to Privacy Shield: Will the Framework Survive Court Review?

If your software company has pursued Privacy Shield certification and is relying on the certification to comply

with EU data privacy regulations, then you will be interested to know that a challenge to the framework is to be heard by a European High Court. The Silicon Valley Software Law Blog has addressed this development and what it may mean for the Privacy Shield framework in the following blog post:

http://www.siliconvalleysoftwarelaw.com/irish-court-has-referred-case-to-european-court-which-challenges-privacy-shield-will-the-eu-u-s-privacy-shield-framework-withstand-scrutiny-by-the-european-high-court/

SaaS Attorney Kristie Prinz to Present Webinar on "Negotiating SaaS Agreements"

SaaS Attorney Kristie Prinz will present a webinar on "Negotiating SaaS Agreements: Drafting Key Contract Provisions, Protecting Customer and Vendor Interests" on June 11, 2018 at 10:00 a.m. The program will be sponsored by Virginia-based Clear Law Institute. To register for the event, sign up at the Clear Law Institute website.

What Software Companies Need

to Know about the GDPR

The European Union's General Data Protection Regulation (the "GDPR") will go into effect on May 25, 2018. In case you are not up to speed on the law already, what do you need to know about it before it goes into effect? The Silicon Valley Software Law Blog addressed the highlights of the regulation in the following blogpost

:http://www.siliconvalleysoftwarelaw.com/what-software-companies-need-to-know-about-the-eu-general-data-protection-regulation/

Kristie Prinz to Speak on "Drafting Software Hosting Agreements for ASP and SaaS" for Live Webcast

Software Contracts Lawyer Kristie Prinz will give a live webcast for Florida-based MyLawCLE on "Drafting Software Hosting Agreements for ASP and SaaS" on March 15, 2018 from 1 to 3 p.m. PST.

Software Lawyer Kristie Prinz to Speak at Clear Law Institute Webinar on “Negotiating SaaS Contracts”

Press Release 3.15.18

Software Agreements Lawyer Kristie Prinz to Speak on “Drafting Software Hosting Agreements for ASP and SaaS”

Software Contracts Lawyer Kristie Prinz will give a live webcast for Florida-based MyLawCLE on “Drafting Software Hosting Agreements for ASP and SaaS” on March 15, 2018 from 1 to 3 p.m. PST.

Six Signs You Are Reviewing a Poorly Written Software

Contract

How do you identify a poorly written software contract, whether it is supposed to be a software license, a SaaS contract, or another type of agreement? Firm Founder Kristie Prinz provides tips on how to identify bad software contracts in the following Silicon Valley Software Law Blog post:

http://www.siliconvalleysoftwarelaw.com/signs-you-are-reviewing-a-poorly-written-software-contract

---

Software Lawyer Kristie Prinz to Speak on “Negotiating SaaS Agreements: Drafting Key Contract Provisions, Protecting Customer and Vendor Interests”

Software Lawyer Kristie Prinz will be featured as a speaker on “Negotiating SaaS Agreements: Drafting Key Contract Provisions, Protecting Customer and Vendor Interests” for a webinar hosted by Arlington, Virginia-based Clear Law Institute on Wednesday, February 21, 2018 from 10-11:15 a.m. PST.

Software Lawyer Kristie Prinz to Speak on “Drafting Software Hosting Agreements: Service Availability, Performance, Data Security, Other Key Provisions”

Silicon Valley Software Lawyer Kristie Prinz will be featured as a speaker for the webinar “Drafting Software Hosting Agreements: Service Availability, Performance, Data Security, Other Key Provisions” for the Atlanta, Georgia-based Strafford on January 23, 2018.

Silicon Valley SaaS Lawyer Kristie Prinz to Speak on “Negotiating Software as a Service Contracts” for Clear Law Institute

Silicon Valley SaaS Lawyer Kristie Prinz will be featured as a speaker for the webinar “Negotiating Software as a Service Contracts” for the Arlington, Virginia-based Clear Law Institute on Wednesday, January 17th from 10-11:15 a.m. PST.