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

Press Release for February 21, 2018 webinar

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

Press Release on January 23, 2018 Webinar

SaaS Lawyer Kristie Prinz to Present Webinar on “Negotiating Software as a Service Contracts”

Press Release for January 17, 2018 webinar

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.

SaaS Lawyer Kristie Prinz Presented on “Best Practices for Drafting SaaS Contracts”

SaaS Lawyer Kristie Prinz presented on “Best Practices for Drafting SaaS Contracts that Reduce the Sales Cycle and Avoid Disputes” on October 26, 2017. A copy of the video recording is available for viewing at this link: https://theprinzlawoffice.vhx.tv/products/best-practices-for-drafting-saas-contracts.

San Jose Lawyer Kristie Prinz to Speak on “Drafting SaaS Contracts” at Webinar Hosted by The Prinz Law Office

Prinz Law founder and San Jose software lawyer Kristie Prinz will speak at a webinar hosted by The Prinz Law Office on “Best Practices for Drafting SaaS Contracts that Reduce the Customer Sales Cycle & Avoid Disputes.” The webinar will take place on October 26, 2017 from 10:00 a.m. to 11:30 a.m. PST. The webinar will address such topics as:
-What makes an effective SaaS customer contract?
-What terms should SaaS customers expect?
-Common challenges with customer negotiations.

-What drafting problems frequently result in stalled contract negotiations? Customer disputes?
-How can better drafting close deals faster? Avoid subsequent customer disputes?
To register for the webinar, please sign up at this **link**.

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

Silicon Valley 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 “Negotiating Software as a Service Contracts”

Software 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.

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

Silicon Valley Software 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 Tuesday, September 12th from 12-1:15 p.m. PST.

Clear Law Institute is making available a special promotional discount of 35% off to attendees who sign up via The Prinz Law Office using this promo code: **krpri35.**

To register for the event, sign up at this link: http://clearlawinstitute.com/shop/webinars/negotiating-software-service-contracts-091217/.

The Prinz Law Office Announces Expansion of Silicon Valley Headquarters in San Jose

The Prinz Law Office is pleased to announce that it will be expanding its Silicon Valley headquarters in San Jose. The firm has entered into a two-year commitment on a fifth-floor office suite at 2033 Gateway Place effective September 1, 2017. In addition to being class A office space that has been recently renovated with a number of new upgrades, the property is conveniently located both to San Jose airport and all the major freeways, including 87, 101, and 880.

To read more about the Gateway Place office complex and scroll through photos of the property, please **click here**. To read the firm's press release on the announcement, please **click here**.

Prinz Law Announces Expansion of Silicon Valley Headquarters in San Jose

Press Release 8.31.17

Silicon Valley Lawyer Kristie Prinz Interviewed by IPWatchdog on Waymo v. Uber

IP Watchdog recently interviewed Prinz Law Founder Kristie Prinz regarding the *Waymo v. Uber* case. **Click here to read article**.

San Jose SaaS Lawyer Kristie Prinz to Speak on "Drafting SaaS Contracts" at 10.26.17 Webinar Hosted by The Prinz

Law Office

Prinz Law founder and San Jose SaaS lawyer Kristie Prinz will speak at a webinar hosted by The Prinz Law Office on “Best Practices for Drafting SaaS Contracts that Reduce the Customer Sales Cycle & Avoid Disputes.” The webinar will take place on October 26, 2017 from 10:00 a.m. to 11:30 a.m. PST. The webinar will address such topics as:
-What makes an effective SaaS customer contract?
-What terms should SaaS customers expect?
-Common challenges with customer negotiations.
-What drafting problems frequently result in stalled contract negotiations? Customer disputes?
-How can better drafting close deals faster? Avoid subsequent customer disputes?
To register for the webinar, please sign up at this **link**.

Silicon Valley Software Lawyer Kristie Prinz to Speak on “Best Practices for Drafting SaaS Contracts” in Webinar Hosted by The Prinz Law Office

Press Release for 10.26.17 webinar

Silicon Valley Technology Attorney Kristie Prinz to Speak on Upcoming Webinar on SaaS Agreements

Press Release 8.17.17

SaaS Agreements Lawyer Kristie Prinz to be featured speaker for “Negotiating Software as a Service Contracts” Webinar Hosted by Clear Law Institute

Silicon Valley Software 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 Tuesday, September 12th from 12-1:15 p.m. PST.

Clear Law Institute is making available a special promotional discount of 35% off to attendees who sign up via The Prinz Law Office using this promo code: **krpri35.**

To register for the event, sign up at this link: **http://clearlawinstitute.com/shop/webinars/negotiating-software-service-contracts-091217/.**

Silicon Valley SaaS Lawyer Kristie Prinz to Present Webinar on "Negotiating SaaS Agreements: Drafting Key Contract Provisions, Protecting Customer and Vendor Interests"

Silicon Valley SaaS Lawyer Kristie Prinz will be co-presenting a webinar on "Negotiating SaaS Agreements: Drafting Key Contract Provisions, Protecting Customer and Vendor Interests" with Kelley Miller of Reed Smith on August 8, 2017 at 10:00 a.m. PST/1:00 p.m. EDT. To register for this webinar, please sign up at: **https://www.straffordpub.com/products/negotiating-saas-agreements-drafting-key-contract-provisions-protecting-customer-and-vendor-interests-2017-08-08**.

Silicon Valley Software Lawyer Kristie Prinz to Speak at Upcoming Webinar on Negotiating SaaS Agreements

Press Release 8.1.17

Silicon Valley Software Lawyer Kristie Prinz to Present Webinar on "Negotiating SaaS Agreements: Drafting Key Contract Provisions, Protecting Customer and Vendor Interests"

Silicon Valley Software Lawyer Kristie Prinz will be co-presenting a webinar on "Negotiating SaaS Agreements: Drafting Key Contract Provisions, Protecting Customer and Vendor Interests" with Kelley Miller of Reed Smith on August 8, 2017 at 10:00 a.m. PST/1:00 p.m. EDT. To register for this webinar, please sign up at: **https://www.straffordpub.com/products/negotiating-saas-agreeme**

nts-drafting-key-contract-provisions-protecting-customer-and-vendor-interests-2017-08-08.

Bipartisan Bill Introduced in Senate that Seeks to Prevent Attacks on American Cyber-Networks

Democratic Senator Brain Schatz of Hawaii and Republican Senator Ron Johnson of Wisconsin have introduced the "Protecting Our Ability to Counter Hacking Act of 2017," also known as the "PATCH Act of 2017" in the U.S. Senate Homeland Security and Governmental Affairs Committee, following the recent "WannaCry" ransomware attack, with the intention of requiring government agencies to submit any security holes in software products they discover for independent review in order to determine any vulnerabilities that need to be secured, as reported by **HealthCare IT News** and **Reuters**. According to HealthCare IT News, the PATCH Act of 2017 is supported by Republican Senator Senator Corey Gardner of Colorado, Democratic Representative Ted. Lieu of California, and Republican Blake Farenthold of Texas, as well as McAfee, Mozilla, The Information Technology and Innovation Foundation, and New America's Open Technology Institute.

The text of the PATCH Act of 2017 is available for viewing **here**.

The bill would require the establishment of a Vulnerability

Equities Review Board comprised of permanent members, ad hoc members, and National Security Council members who are neither of the above, if approved by the President and requested by the Board. The permanent members would include the following:

- Secretary of Homeland Security or the designee of the Secretary, who shall be chair of the Board;
- Director of the Federal Bureau of Investigation or the designee of the Director;
- Director of National Intelligence or the designee of the Director;
- Director of the Central Intelligence Agency or the designee of the Director; and
- Secretary of Commerce or the designee of the Secretary.

The Ad Hoc Members would include:

- Secretary of State, or the designee of the Secretary, if the Board considers the matter under the jurisdiction of the Secretary;
- Secretary of the Treasury, or the designee of the Secretary, if the Board considers the matter under the jurisdiction of the Secretary;
- Secretary of Energy, or the designee of the Secretary, if the Board considers the matter under the jurisdiction of the Secretary; and
- Federal Trade Commission ("FTC"), or the designee of the Commission, if the Board considers the matter as relating the the FTC.

The purpose of the Board would be to establish policies relating to "whether, when, how, to whom, and to what degree information about a vulnerability that is not publicly known should be shared or released" by government to a non-government entity and the process by which such information should be shared or released to a non-governmental entity. In other words, as **Reuters** reported, the bill is intended an attempt to put the process "into civilian control" and remove

such decisions from the purview of the National Security Agency ("NSA").

According to reporting by **ThreatPost**, this bill codifies the process that the White House has long claimed to have in place to evaluate information on security vulnerabilities, but in fact rarely actually has utilized. According to **Threat Post**, in the particular case of the WannaCry attack, the NSA did in fact tip off Microsoft of the security issue, which allowed Microsoft to make the patch available to customers in advance of the attack.

While the WannaCry attack was initially reported only to have hit Windows machines, according to reports by **ThreatPost**, it is now known that medical devices and industrial control systems have also been hit by the attack, including equipment used in medical radiology facilities.

Reuters is reporting today that, for victims who have not paid the ransom and/or recovered their files, French Researchers have developed a last resort workaround, which will successfully unlock the encryption key for files hit by the attack in certain conditions. According to **Reuters**, Europol has stated on Twitter that its European Cybercrime Centre has tested this tool and confirmed it will successfully recover data in some circumstances. The technical details of this tool can be accessed through the **Reuters** article.

Bipartisan Bill Introduced in Senate that Seeks to Prevent

Attacks on American Cyber-Networks

The “PATCH Act of 2017” has just been introduced in the Senate, which would require government agencies to submit security holes in software products they identify for independent review in order to determine any vulnerabilities that need to be addressed. For more information on the bill, please check out the Silicon Valley Software Law Blog posting on the story:

http://www.siliconvalleysoftwarelaw.com/bipartisan-bill-introduced-in-senate-that-seeks-to-prevent-attacks-of-american-cyber-networks/.

BiPartisan Bill Introduced in Senate that Seeks to Prevent Attacks on American Cyber-Networks

The “Protecting Our Ability to Counter Hacking Act of 2017” or “PATCH Act of 2017” has just been introduced in the Senate. For more background on the bill, please check out this Silicon Valley Software Law Blog post:

http://www.siliconvalleysoftwarelaw.com/bipartisan-bill-introduced-in-senate-that-seeks-to-prevent-attacks-of-american-cyber-networks/

Negotiating the Purchase of SaaS Company Assets: Key Problems to Consider in Any Deal

If you are like many SaaS companies I see, if you are approached with an asset purchase that interests you, you will be in a hurry to get the deal closed. However, before you move forward, you should want to give the deal serious consideration. What are some of the concerns you should have? The Silicon Valley Software Law Blog addresses these issues in the following blog post:http://www.siliconvalleysoftwarelaw.com/negotiating-the-purchase-of-saas-company-assets-key-problems-to-anticipate-in-any-deal/

Investigation Reportedly Launched by Department of Justice into Uber's Use of

“Greyball” Software

The Department of Justice has launched an investigation into Uber’s use of the Greyball software program. For more information on the investigation, please check out the following Silicon Valley Software Law Blog posting on the story:

http://www.siliconvalleysoftwarelaw.com/investigation-reportedly-launched-by-department-of-justice-into-ubers-use-of-greyball-software/

Common Software Fee Drafting Problems and How to Fix Them

A common problem in software and SaaS agreements is that the fee terms in the contract make no sense. Why is this the case and how do you fix the terms? The Silicon Valley Software Law Blog addresses this issue in the following posting:

http://www.siliconvalleysoftwarelaw.com/common-software-agreement-fee-drafting-problems-and-how-to-fix-them/

Does Your Customer Software

License or SaaS Agreement Leave Your Company Vulnerable to a Dispute Over Implementation?

If your company is like most in the software space, your product requires some sort of initial set-up and configuration for customers that in an enterprise scenario can require a significant investment of time and resources. However, many software contracts are silent regarding what is involved in this initial phase of a business relationship, which results in many disputes. The Silicon Valley Software Law Blog discusses this issue in the following blogpost:

http://www.siliconvalleysoftwarelaw.com/does-your-customer-software-license-or-saas-agreement-leave-your-software-company-vulnerable-to-a-legal-dispute-over-implementation/

Could a Software Developer Whose Code is Used for Hacking Be Convicted of a Crime?

If you are a software developer and you develop code that hackers then use to commit crimes, then you may be a risk for criminal prosecution, as an Arkansas developer named Taylor Huddleston recently discovered according to an article

published by **The Daily Beast**.

According to **The Daily Beast**, Huddleston developed a remote administration tool called "NanoCore" that is popular with hackers but claims that he intended his tool to be adopted by "budget-conscious school IT administrators, tech support firms, server farms, and parents worried about what their kids are doing online." **The Daily Beast** reports Huddleston is now being prosecuted on federal charges of conspiracy and aiding and abetting computer intrusions.

Could going after developers of software used by hackers be a new trend in law enforcement?

T**he Daily Beast** article suggests that this could in fact be a new strategy in law enforcement, and points to the government's 2012 prosecution of Michael "xVsiceral" Hogue, who had participated in "creating and selling a remote access program called Blackshades" which constituted ransomware, as possible motivation for the strategy, since the government subsequently entered into a deal with Hogue, which enabled U.S. & European authorities being able to successfully prosecute 100 users of the software over a two-year long investigation.

The bottom line is that developers who create code or products that may have legitimate as well as hacking applications should be on notice that they could become the target of a federal investigation or even be federally prosecuted as a result of their development activities. The Huddleston case certainly suggests that software innovators should be considering how their innovations may be utilized once developed before they actually follow through with the development, and certainly should be seeing outside legal counsel on these issues prior to engaging in the development of a product that may have both innocuous and criminal applications. Developers in such circumstances also may want to re-consider the wisdom of engaging in independent

development and seek out corporate support for their development project.

Could a Software Developer Whose Code is Used for Hacking be Convicted of a Crime?

If you are a developer and you develop code that hackers then use to commit crimes, then you may be at risk for criminal prosecution. Could prosecution of developers for code used by hackers be a new trend in law enforcement? For more information on the risks to software developers, please check out this Silicon Valley Software Law Blog posting:

http://www.siliconvalleysoftwarelaw.com/could-a-software-developer-whose-code-is-used-for-hacking-be-convicted-of-a-crime/

SaaS Lawyer Kristie Prinz Presents on “Best Practices for Drafting SaaS Contracts

that Reduce the Sales Cycle”

SaaS Lawyer Kristie Prinz presents on “Best Practices for Drafting SaaS Contracts that Reduce the Sales Cycle” in March 2017. A copy of the video recording is available for viewing at this link: https://theprinzlawoffice.vhx.tv/products/draft-saas-contract-to-reduce-customer-sales-cycle

---

SaaS Contract Lawyer Kristie Prinz to Speak on “Best Practices for Drafting SaaS Contracts that Reduce the Customer Sales Cycle & Avoid Disputes”

Silicon Valley attorney Kristie Prinz will be speaking on “Best Practices for Drafting SaaS Contracts that Reduce the Customer Sales Cycle & Avoid Disputes” at a webinar hosted by The Prinz Law Office on March 24, 2017 at 10 a.m. to 11:30 a.m. PST. To sign up for the event, please register at the following link: http://prinzlawstore.com/saas-customer-agreements/.

Service Level Agreements: What is a Service Level Agreement or “SLA” and When Do You Need One?

If you are in the software industry, you probably have heard of a “service level agreement” or “SLA” but do you really understand what a service level agreement is or why you might need one? The Silicon Valley Software Law Blog addresses this issue in the following blogpost:

http://www.siliconvalleysoftwarelaw.com/service-level-agreements-what-is-a-service-level-agreement-or-sla-and-when-do-you-need-one/

Recent Class Actions Provide Valuable Lesson on Why SaaS Contracts Should Be Drafted to Fit A Company’s Business Model

If your company is like most, you may be using a software agreement that has nothing to do with your company’s business practices or business model. Why is this a bad idea? Well, several recent class action suits provide a recent example of why this can be very problematic for a software company. The

Silicon Valley Software Law Blog addresses this issue in the following blogpost:

http://www.siliconvalleysoftwarelaw.com/recent-software-class-actions-provide-valuable-lesson-on-why-saas-contracts-should-be-drafted-to-fit-companys-business-model/

Recent Software Class Actions Provide Valuable Lessons

When SaaS companies and start-ups first contact me, they are often doing so with the idea that there are a few really well SaaS template contracts circulating in the SaaS industry and they seeking the" right" attorney to provide that industry-standard template to them. Alternatively, they contact me telling me that they've already put together a draft SaaS contract, and that they just want me to look over and "bless" what they've already written based on a particular SaaS company's contract available for download on the Internet.

In these cases, which are the norm rather than the exception, I often encounter significant push-back when I first suggest to them that they are approaching the SaaS contract drafting process entirely the wrong way. I always explain that a well-drafted SaaS contract should be tailored to their specific business model, and then I proceed to ask them a number of questions about their business model, which they generally aren't prepared to answer. They often then proceed to get frustrated by all the questions about their business, when all they are actually looking for is the "right" contract template.

If you are in the SaaS industry and have created your customer

contract in a similar fashion, or committed the other common software contracting "sin" of caving into pressure exerted by a potential customer and just agreed to their standard agreement terms because you wanted to close a deal with them, then you may want to consider the example of recent litigation against an industry leader, which adopted contract language which was then alleged not to match the company's business practices.

The litigation at issue involves class action suits against the McAfee brand security software: **Williamson v. McAfee, Inc.,** No. 5:14cv00158 (N.D. Cal. Aug. 30, 2016) and **Kirby v. McAfee, Inc**., No. 5:14cv02475 (N.D. Cal. May 29, 2014). Both cases focus on the company's business practices surrounding its use of automatic renewal clauses—a standard practice widely adopted throughout the SaaS industry. The litigation is ongoing: while the court granted final approval of a **settlement** in both cases, an appeal has been filed. (See **posted notice**).

The particular contract clause at issue in the Williamson case is a common clause routinely included in SaaS contracts that stated at autorenewal customers would be charged the "then-current" price for the product. However, the Williamson complaint alleged that the actual practice of the company was to charge customers upon autorenewal a higher price for the product than the price that the customer could have purchased the product for elsewhere.

The particular contract clauses at issue in the Kirby case stated that customer would be automatically enrolled in the autorenewal program and that a customer's credit or debit card could be charged at autorenewal even after it had expired. The Kirby complaint alleged that the actual practice of the company was to import into its billing system updated customer credit or debit card information provided by Visa or MasterCard rather than procuring a new authorization from client when the prior authorization became invalid, and to

charge the customer at autorenewal at a higher price than originally paid without the customer's express consent.

While there are a number of allegations made against McAfee in these class action suits, a fundamental problem alleged was that the terms of service binding the customer did not match the company's actual business practices, and that the customer did not provide consent to the company's actual autorenewal practices.

While these particular suits were filed against McAfee, the business practices alleged in these cases are perhaps the current standard of conduct for today's software industry. Furthermore, I would argue that more often than not terms of service are adopted by companies without any consideration whatsoever of the actual technology and business model for the software or SaaS product, so it is probably rare for the terms of service to match the company's actual business practices. Thus, it is my assertion that these cases provide an excellent primer of the risks of adopting terms of service that do not match the actual practices of the business. It's still not clear what the ultimate price tag on this matter will reach on the part of the company, but it's clear it will be multiple millions of dollars in costs and expenses.

Moreover, these cases demonstrate the importance of consent to having an effective autorenewal clause. State laws applicable to these cases did require the procurement of clear and conspicuous consent to autorenewal, which McAfee is alleged not to have had in these particular sets of facts. Obviously, any deficiency with consent could have easily been addressed through the adoption of better business practices and terms that would demonstrate clear customer consent in compliance with applicable state laws.

The bottom line is that terms of service should not be adopted by a SaaS company without a thorough consideration of the technology, the business model, and the business practices of

the company. Even common business concepts like autorenewal accepted across the board within the industry may lead to costly lawsuits if insufficient consideration of business practices is contemplated in conjunction with the drafting of terms of service.

FTC Enforcement Actions Should Provide Warning to Software Industry about Privacy

If your software company is like most, you have probably spent little or no time contemplating what needs to be in your company's privacy policy. In fact, what your company is currently calling its privacy policy was likely copied from a third party website years ago and never given much thought since. Meanwhile, your company is likely collecting and aggregating user data and looking for new opportunities to monetize it. Sound familiar?

Well, if this is your company's situation, you may want to rethink how you are operating in light of recent enforcement action by the FTC on corporate data collection practices.

On February 6, 2017, the FTC announced that VIZIO, Inc. had agreed to pay $2.2 million to settle charges by the FTC and Office of the New Jersey Attorney General that it installed software on its TVs to collect data regarding consumer viewing without their knowledge or consent. In its **complaint against**

VIZIO, the FTC alleged that VIZIO had manufactured televisions that continuously tracked consumer viewing on the television and transmitted this information back to VIZIO, and also had remotely installed the same proprietary software on previously sold televisions. In addition to collecting information about consumer viewing, the **FTC alleged in its complaint** that the software had collected information about the television, IP address, wired and wireless MAC addresses, WiFi signal strength, and nearby WiFi access points. The **FTC further alleged in its complaint** that VIZIO had then entered into third party contracts to sell the data collected to third parties for the purpose of measuring the audience, analyzing advertising effectiveness, and targeting advertising to particular consumers. While VIZIO's contracts had provided only aggregate data to the third parties, those contracts did provide segmented demographic information by sex, age, income marital status, household size, education, home information, and household value. According to the **FTC Complaint,** VIZIO did make a privacy policy available on its website, but the only onscreen notifications provided to consumers were vague and timed out after 30 seconds, never sufficiently informing consumers as to VIZIO's data collection practices with the software installed on their televisions. **The FTC alleged** that VIZIO's actions in deceptively omitting material facts constituted deceptive acts or unfair practices prohibited by Section 5(a) of the FTC Act.

In the **stipulated order**, VIZIO was ordered to take all the following actions before collecting any further data from consumers:

- Prominently disclose to consumers **"separate and apart"** from the privacy policy specifics on the data to be collected, what would be shared with third parties, the categories of third parties who would receive the data, and the purpose for which the third parties would receive the data.

- Obtain affirmative express consent from consumers at the time of disclosure and upon any material changes.
- Provide instructions at the time of obtaining consent to how consumers may revoke consent.

The **stipulated order** then gave specific guidelines on what would constitute "prominent" disclosure

The **stipulated order** also required the destruction of the previously collected data, the mandated creation of an internal privacy program meeting certain requirements, and third party oversight going forward regarding the privacy controls in place at the company.

Clearly, the FTC intended to send a message to the software industry about the collection of consumer data in the case of this particular enforcement action.

However, the FTC's recent enforcement activities against software companies did not end with VIZIO. In a separate statement, the **FTC announced** settlements with three other companies in the industry over allegations that they had made deceptive statements in their privacy policies about their participation in an international privacy program. The companies charged in those cases were, Sentinel Labs, Inc., a software company providing endpoint protection software to enterprise customers; SpyChatter, Inc., a company marketing a private messaging app; and Vir2us, Inc., a distributor of cybersecurity software. The FTC alleged in each complaint that the companies violated the FTC Act by making deceptive statements about their participation in privacy programs. Attached are the complaints against **Sentinel Labs**, **SpyChatte**r, and **Vir2us**. In these cases, the proposed settlements merely prohibited the companies from making further misrepresentations about their participation in third party privacy or security programs, but are not final orders and still subject to possible amendment.

What conclusions should you as a software company take away from the FTC's recent enforcement activities against software companies? Clearly, the FTC is cognizant of the trends in the software industry to monetize data collected from software, to adopt privacy policies without actually customizing them to the practices of their particular company, and to bury privacy notices on websites without actually obtaining clear end user consent to actual business data collection practices. So, if your company is like most in this space, you are on notice that your practices need to change. Your privacy policy needs to be customized to the business practices of your particular company, which means that you actually need to take the time to consider each and every piece of information that you are collecting from the public and disclose what you are doing with it. If your customers expect you to be a part of an international privacy program before they do business with you, you need to actually take the steps requirement to receive the appropriate certification from that organization before you advise consumers and the public that you are a member. And if your software collects information, you need to make sure that not only your customers but also the parties from whom the information is collected have given their clear consent to your collection practices. A privacy policy buried in your website is probably not sufficient to cover you legally.

If you do not change your privacy practices, you are on notice that you may soon be hearing from the FTC.

Recent FTC Enforcement

Actions Should Serve as a Warning to Software Industry Regarding Privacy Practices

If your company is like most and you have given little or no thought to your company's privacy policy while also collecting data and looking for ways to monetize it, then you may want to rethink how you are operating in light of recent enforcement actions by the FTC in the user data space. The Silicon Valley Software Law Blog addressed these developments in the following blogpost:

http://www.siliconvalleysoftwarelaw.com/recent-ftc-enforcement-actions-should-serve-as-warning-to-software-industry-about-privacy-practices/

Silicon Valley Software Lawyer Kristie Prinz to Speak at Upcoming Webinar on SaaS Contracts

Prinz Law Office Press Release 3.7.2017

Silicon Valley Software Lawyer Kristie Prinz to Speak at Webinar on “Best Practices for Drafting SaaS Contracts that Reduce the Customer Sales Cycle & Avoid Disputes”

Silicon Valley software attorney Kristie Prinz will be presenting a webinar sponsored by The Prinz Law Office on “Best Practices for Drafting SaaS Contracts that Reduce the Customer Sales Cycle & Avoid Disputes” on March 24, 2017 from 10:00 a.m. to 11:30 a.m. PST. To register, please sign up at the following link: **http://prinzlawstore.com/saas-customer-agreements/.**