Silicon Valley Technology Lawyer Kristie Prinz to Speak at Upcoming Webinar

Press Release 2.1.19

Silicon Valley Software Lawyer Kristie Prinz to Speak at Upcoming Webinar on “Best Practices for Drafting SaaS Contracts & Managing SaaS Customer Relationships”

Press Release Best SaaS Practices 1.31.19

Silicon Valley Software & Technology Lawyer Kristie

Prinz to Speak at Upcoming Webinar on “Negotiating SaaS Agreements”

Press Release 1.31.19

Silicon Valley Tech Transactions Lawyer Kristie Prinz to Speak on “Drafting Master Service Agreements & Managing the Service Relationship”

Silicon Valley Tech Transactions attorney Kristie Prinz will present a webinar on “Best Practices for Drafting Master Service Agreements & Managing the Service Relationship” on Friday, March 8th from 10 a.m to 11 a.m. PST. The Prinz Law Office will be sponsoring the event, which will be intended for lawyers as well as businesspeople. To register, please sign up at http://prinzlawstore.com/2019/01/best-practices-for-drafting-master-service-agreements-managing-the-service-relationship/.

Silicon Valley Software Lawyer Kristie Prinz to Speak on “Best Practices for Drafting SaaS Contracts & Managing SaaS Customer Relationships”

Silicon Valley software attorney Kristie Prinz will be presenting a webinar on February 19, 2019 at 10 a.m. PST/1 p.m. PST on “Best Practices for Drafting SaaS Contracts & Managing SaaS Customer Relationships.” The program will be sponsored by The Prinz Law Office, and is intended for lawyers as well as businesspeople. To register to attend the program, please sign up at http://prinzlawstore.com/2019/01/drafting-saas-contracts-managing-saas-customer-relationships/.

Prinz Law Founder Kristie Prinz Joins Privacy Experts in Urging California to Make Serious Revisions to the

California Consumer Privacy Act (“CCPA”)

I was pleased to join Santa Clara Law School Professor Eric Goldman and other privacy experts in urging California to make revisions to the California Consumer Privacy Act (“CCPA”):

https://blog.ericgoldman.org/archives/2019/01/41-california-privacy-experts-urge-major-changes-to-the-california-consumer-privacy-act.htm

---

The Prinz Law Office Announces Opening of New Palo Alto Office

Press Release 1.14.19

The Prinz Law Office Announces Opening of Palo Alto Location

The Prinz Law Office is pleased to announce the opening of its new Palo Alto office. To read the press release announcing the opening, please click on the link: **Press Release 1.14.19**.

The Anticipated Impact of The Foreign Investment Risk Review Modernization Act of 2018 ("FIRRMA")

Legal commentators have been raising alarms about the significant potential impact of **The Foreign Investment Risk Modernization Act of 2018** ("FIRRMA"), since the legislation was signed into law in August, 2018. In case you are unfamiliar with FIRRMA, the legislation dramatically expanded the powers of the Committee on Foreign Investment in the United States ("CFIUS") to conduct national security reviews of business deals, which obviously could have significant implications on the business community's ability to close business transactions. The U.S. Treasury has developed a **website** that highlights for the public key points about FIRRMA and this review process.

In particular, FIRMMA now expands CFIUS review powers to include the following types of business deals:

- A purchase, lease, or concession by or to a foreign person of real estate located in proximity to sensitive government facilities.
- "Other Investments" by a foreign person in any unaffiliated U.S. business that owns, operates, manufactures, supplies, or services critical infrastructure; produces, designs, tests, manufactures, fabricates, or develops one or more critical technologies; or maintains or collects sensitive personal data of U.S. citizens that may be exploited in

a manner that threatens national security. “Other investments” is defined to mean an investment that affords a foreign person access to material, nonpublic technical information in possession of the U.S. business, membership or observer rights on the board of directors or equivalent governing body of the U.S. business, or the right to nominate an individual to a position on the board of directors or equivalent voting body, or any involvement other than the voting of shares in the substantive decisionmaking of the U.S. business; the use, development, acquisition, safekeeping, or release of sensitive personal data of U.S. citizens maintained or collected by the U.S. business; the use, development, acquisition or release of critical technologies; and the management, operation, manufacture, or supply of critical infrastructure.

- Any change in rights that results in foreign control of a U.S. business or an “other investment” as defined above.
- Any transaction, transfer, agreement, or arrangement, the structure of which is intended to evade the review of the Committee.

FIRRMA further defines “critical technologies” to include “specially designed and prepared nuclear equipment, parts and components, materials, software and technology covered by part 810 of title 10, Code of Federal Regulations (relating to assistance to foreign atomic energy activities)” as well as “emerging and foundational technologies controlled pursuant to section 1758 of the Export Control Reform Act of 2018. ” While the list of what constitutes an “emerging and foundational” technology has yet to be defined, most legal commentators are expecting the list to include software that does not relate to nuclear technology, particularly in the areas of artificial intelligence, autonomous mobility, augmented virtual reality, cybersecurity, and financial technology. So, while the legislation is new and the full scope of its application and

subsequent interpretation has yet to be determined, it is anticipated by most commentators that many software transactions involving foreign investment in a U.S. business will ultimately be deemed to be subject to the new CFIUS review powers.

What does this mean for the software and tech industry? Well, the full impact of the law is yet to be determined and is more the subject of extensive speculation in the legal industry at the moment, but it does mean that software and tech companies could be subject to more federal compliance obligations when they are doing deals that involve foreign investment, that these compliance obligations could slow down or even derail the closing of some deals, and that some companies could potentially be subject to significant fines up to the amount of the deal if they fail to comply with their new obligations. So, it certainly means that U.S. based software and tech companies need to be aware of FIRRMA and need to closely follow any future developments related to the law, in order to potentially comply with it on future deals.

Software Industry Warns of Fallout from Australia's Passage of New Anti-Encryption Legislation

The software industry is raising concerns about the potential consequences of Australia's recent passage of legislation to provide law enforcement with expansive new powers to compel the disclosure of encrypted data.

According to **ITPro**, the "Telecommunications and Other Legislation Amendment (Assistance and Access) Bill 2018" was approved by a 46-11 majority in the Australian parliament last month. As **The Verge** reports, the newly passed legislation grants to law enforcement new notice powers of mandatory technical assistance and technical capability, which "require companies to give access to encrypted data if available, or to build the capacity to provide such access if they are unavailable." Additionally, as reported by **The Verge**, the legislation grants a voluntary technical assistance request power "that does not have to be publicly reported." According to **The Verg**e, the fine for noncompliance can be up to $10 million AUD (approximately $7.2 million USD).

The Verge reports that the new law also uniquely enables the Australian government to approach individuals such as key employees in order to compel their cooperation rather than limiting the enforcement powers to merely compelling cooperation by institutions. The penalty for any individual's failure to cooperate could result in a prison sentence.

As **Wired** has reported, the legislation has been strongly opposed by the tech industry on the grounds that "if Australia compels a company to weaken its product security for law enforcement, that backdoor will exist universally, vulnerable to exploitation by criminals and governments far beyond Australia." Also, as **Wired** has noted, any company that complies with Australia's law is likely to then be required to provide the same access to another country. **Fortune** suggests that the legislation is particularly intended to target What'sApp and Signal.

According to **The Verge,** Apple's position on the legislation has been that "encryption is actually a defense against cyberattacks and terrorism" and that "more of it is needed to make citizens safe, not less." Apple took its concerns directly to the Australian parliament, according to **Threatpost**, which has posted a **letter** reportedly submitted by

Apple to parliament. **Threatpos**t also reports that Cisco and Mozilla have also been vocal in their opposition to the legislation. Commentator and human rights lawyer Lizzie O'Shea also observes to **The Verg**e that "once these [backdoor] tools exist, then it would be easy for Australian authorities to share them with their counterparts in allied nations," particularly since Australia is part of the Five Eyes intelligence sharing agreement in which Great Britain, Canada, New Zealand and the United States also participate.

The Australian government's position, according to **The Verge**, is that the powers are necessary to defend citizens against terrorism and crime and that the powers will not introduce a "systemic weakness" into the technology. However, a prevailing criticism has been that "systemic weakness" is not actually defined by the legislation. **Fortune** reports that the Australian Labor Party is already seeking to amend the legislation, particularly to define "systemic weakness."

Clearly, Australia's new legislation has the potential to have a far-reaching impact on software companies and individuals working in the software industry.

News Update on Australia's Anti-Encryption Law

News Update 1.8.19