The Prinz Law Office's Kristie Prinz to Present Upcoming Webinar on SaaS Contracts

The Prinz Law Office will be sponsoring a webinar on October 8, 2019 on "Best Practices for Negotiating SaaS Contracts & Managing SaaS Customer Relationships." The firm's own Silicon Valley SaaS attorney, Kristie Prinz, will be presenting this webinar, which will address such issues as:

- *What makes an effective SaaS customer contract?*
- *What are the essential terms in a well-drafted SaaS contract?*
- *What are the common issues that arise in SaaS negotiations? What are the best strategies to resolve them?*
- *What are the best practices to manage the customer relationship?*

To register to attend, please sign up at **The Prinz Law Store** website at **https://prinzlawstore.com/2019/08/saas-contracts/**.

Is a Company Liable for Software Defects, when a

Vulnerability is Discovered but Not Exploited?

If you are in the software business, you likely recognize that you can be sued for materially breaching contracts, infringing third party IP, and data breaches but you may not realize the extent of your liability just for making the sale of a software product deemed to contain a security flaw in the first place, even if the security flaw was never exploited and only identified.

Increasingly, however, just the act of selling software later deemed to be "defective" due to security flaws has resulted in liability to companies.

The Federal Trade Commision (the "FTC") has recently imposed fines and put in place ongoing oversight on companies for this type of issue.

But as Cisco just discovered, if the sales were made to a federal or state agency, the mere act of making the sale can also result in significant liability. Cisco has agreed to pay $8.5 million to settle a case originally filed in New York Western District Court in 2011 involving the sale of video surveillance technology to a variety of government organizations, including but not limited to Homeland Security, the Secret Service, the Army, the Navy, the Marines, the Air Force and the Federal Emergency Management Agency.

According to **The New York Times**, the Cisco case was initiated by the Justice Department in the Federal District Court for the Western District of New York, and the allegations were based on violations of the False Claims Act, which addresses fraud and misconduct in federal government contracts. Fifteen states and the District of Columbia joined in the suit. As **The New York Times** reported, the argument made by the

government was that the software had no value because if failed to serve its primary purpose of security enhancement. According to **The New York Times**, the flaw was identified back in 2008 by a Cisco subcontractor, who brought it to the company's attention at that time. However, as **The New York Times** reported, the subcontractor was subsequently terminated, and when he realized two years later that the vulnerability was still not fixed, he contacted the FBI. **The New York Times** reported that Cisco continued to sell the software with the flaw until July 2013, when if finally notified customers and fixed the flaw.

While the Cisco case applies only to sales made to government, a class action suit is pending right now on similar facts, where the sales were made to non-government consumers. The class action lawsuit was initiated late last year against Symantec for critical defects in its security products under the Norton Brand. It is not clear as to the status of that litigation.

The bottom line: if you are selling software that provides security functionality, you need to have internal systems in place to identify security flaws and quickly fix the flaws, particularly if the software is being sold to a government organization. However, if you are selling to the general public, you may still be liable for sales of the software containing security flaws, whether liability is assessed through the FTC or through class action litigation, regardless of the terms of your contract for those sales.

Can Your Company Be Sued Over a Software Update?

When your company releases its next software update, you may want to consider the potential legal implications of the release. There seems to be a new trend in class action litigation: suits over software updates.

As **Reuters** first reported, an owner of a Tesla vehicle has filed a lawsuit against Tesla, Inc. claiming that a software update fraudulently limited the battery range of older vehicles, which reduced the distance that they can travel without recharging the vehicles. **Reuters** reported that the lawsuit was filed in a Northern California federal court and seeks class action status for owners of Model S and X vehicles around the world.

According to **Reuters**, the lawsuit claims that the software update was released with the intention of avoiding liability for defective batteries.

CNET reports that the affected owners claim to have lost some eight kilowatt hours of capacity after the software update, which occurred back in May, 2019, and that the affected cars are older model S and X vehicles, which have batteries that should still be covered under the eight (8) year warranty on the batteries. **InsideEvs** explained the argument as Tesla "enter[ing] [owners'] garages and replac[ing] a 40-gallon tank for a 20-gallon tank."

Tesla is not the first company to be sued for a software update and how the update affected the performance of a device. Apple has also been the subject of numerous suits in the past few years on a similar issue. This Business Insider article reports on the legal controversy involving Apple regarding **an update** affecting battery performance. Class

action suits were also filed against Microsoft over its Windows 10 upgrade strategy. See this **Consumeraffairs.com** article.

While these cases all pertain to software that controlled performance of a device, whether batteries or computers, it seems clear that with the increasing reliance on software functionality across so many industries, lawsuits over software updates are likely to continue.

So, the next time your company contemplates a software update or upgrade, it may be prudent to to contemplate the legal implications of the release and whether or not it is likely to result in litigation. You also may want to reconsider the sufficiency of your legal agreements in place with the parties to whom you are sharing the updates or upgrades before making available the new software. Software companies are clearly on notice that they may be sued for updates or upgrades, if they are alleged to have a negative impact on customers or users after the release.

Silicon Valley SaaS Lawyer Kristie Prinz to Speak on "Negotiating SaaS Agreements" for Clear Law Institute

Silicon Valley SaaS Lawyer Kristie Prinz will present a webinar on "Negotiating SaaS Agreements: Drafting Key Contract Provisions, Protecting Customer and Vendor Interests" on August 9, 2019 at 10:00 a.m. PST/1 p.m. EST. The program will be sponsored by Virginia-based Clear Law Institute. To

register, please sign up at https://clearlawinstitute.com/.

PPrivate Coalition of Health Insurers and Major Tech Companies Announce New Standard for Claims Data S

The CARIN Alliance, which is a coalition of companies from the health and tech industries, has just announced the release of a new standard for sharing health claims data in conjunction with the Blue Button Developers Conference. The announcement is linked **here.**

The newly released standard is linked here: **CARIN Blue Button Implementation Guide CI Build.**

According to **FierceHealthcare**, the standard was developed by working group comprised of alliance members and includes more than 240 claim data elements. **FierceHealthcare** reports that 20 organizations, including Apple, Anthem, Blue Cross Blue Shield, Cambia Health Solutions, Google, and Humana have agreed to test an application programming interface ("API") employing the standard in anticipation of a product lunch of the standard next year.

CNBC reports that the significance of the news is that this is the first time that industry has agreed to standards for sharing claims data to third party developers, and the Alliance aspires not only to make the data available to consumers but also to provide fraud detection functionality and functionality to help consumers avoid paying bills with

errors in them.

FierceHealthCare reports that the new standard "builds" on Blue Button 2.0, which was released by the Centers by Medicare and Medicaid Services ("CMS") last year and is an API enabling Medicare beneficiaries to access to their Medicare claims data. A web page dedicated to Blue Button 2.0 is linked **here**. FierceHealthCare reported on the Blue Button 2.0 initiative by CMS here.

Obviously the development of new digital health standards is a victory for the digital health industry, which has arguably been slow to develop industry standards along the lines of what exist in the tech industry generally.

For more information on how to join The Carin Alliance, **click here**. For a list of alliance members, please click **here.**