Recording Released of “Best Practices for Launching a Software Development Project”

The Prinz Law Office is pleased to announce that the recording of the recent presentation by Tech Business Lawyer Kristie Prinz on “Best Practices for Launching a Software Development Project” is now available at this link: https://theprinzlawoffice.vhx.tv/products/best-practices-for-a-software-development-project.

Kristie Prinz Welcomes Audience to Updated Silicon Valley Software Law Blog

Kristie Prinz welcomes audience to the updated Silicon Valley Software Law Blog in this video recorded October 2021.

Software Lawyer Kristie Prinz Presented on “Legal Developments in the Software Industry”

Software Lawyer Kristie Prinz presented a webinar on “Legal Developments in the Software Industry” on November 21, 2019. A copy of the video recording is available for viewing at this link: https://theprinzlawoffice.vhx.tv/products/legal-developments-in-the-software-industry-2019.

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.

The Prinz Law Office Announces Opening of San Francisco Office

Press Release 5.1.19

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**.