You're So Vain, You Probably Think This Software's About You...

Mar 29, 2023

Categories:

Publications
Technology Blog

Authors:

Matthew R. Schantz
Gene F. Price

...And you're probably right.

On March 2, the Biden administration issued its long-awaited National Cybersecurity Strategy. The "strategy" is bold, calling for a number of initiatives and reforms to the nation's cyber infrastructure. Among these are that state and federal regulators must set higher cybersecurity requirements for critical infrastructure and harmonize more stringent regulations with those already in force.

One particularly striking recommendation the strategy asserts is to "**shift liability onto those entities that fail to take reasonable precautions to secure their software** ...." (Strategic Objective 3.3.) If you felt the ground figuratively move beneath your feet, it was for good reason.

Currently, companies that develop software for operating systems, embedded systems, applications and other uses contractually limit their liability if the software doesn't perform well or leads to damage or loss of data or computing equipment. Most of us routinely agree to those terms without reading the multipage master service agreements or end-user license agreements (EULAs). EULAs in particular are often not available until after the software is purchased, which some say makes them contracts of adhesion, but courts have still routinely enforced them.

The strategy's recommendation to shift liability from buyers to sellers has so far been met with a yawn. This is largely due to Congress being split between the political parties, making new laws less likely, especially any that implement such major policy (and cost) shifts. Conventional wisdom also indicates that a shift implementing the recommendation would cause upheaval in the software ecosystem, chilling innovation in a sector thus far dominated by American companies.

Yet this reaction overlooks recent evolutions of law in the United States. Until the 1960s, a disclaimer of liability (comparable to those

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

in EULAs) was effective to protect a manufacturer from liability claims by individuals injured by their products. In the California Supreme Court matter of Greenman v. Yuba Power Products, Inc. (1963), the court adopted strict liability in tort for defective products, a standard that eventually spread across the country. Likewise, the country currently has no comprehensive national privacy law. In this vacuum, several state legislatures have implemented legal privacy frame works or are in that process, and those are now often followed even by companies based in other states.

Like strict liability and privacy, the states could achieve the strategy's recommended change using approaches that have been successful in the past. But what would it mean if California or some other state-issued legislation held software companies liable for failing to take reasonable precautions to secure their software, or if an influential state Supreme Court simply refused to enforce disclaimers in a EULA as against public policy or because the EULA is a contract of adhesion?

While we are following no current litigation that seeks that outcome, many believe that change is overdue, as evidenced by the strategy. Consequently, any company selling software should be aware of this White House policy recommendation and consider how it might need to prepare for such a change. Whether you are—or represent—a retailer, software developer or especially anyone supplying software to the federal government, anticipating the effects of the recommendation would be prudent. In the near term, one might achieve market differentiation. In the longer term, there is an opportunity to change one's processes and agreements before the costs of security talent and tools skyrocket.

Retailers have direct contact with consumers and are likely to be on the front line of claims for defective products where the defect comes from bad software. Parents who buy baby monitors from a big box store—only to find out that the audio and video feeds are made wide open to the internet—are sure to make the retailer the key defendant in their complaint. Retailers might start by screening their suppliers for best software development practices, negotiate broader indemnification obligations and ensure their vendors' ability

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

to fund those obligations. In addition, retailers tend to have access to a wide range of personal information of consumers, so every contract that involves the retailer sending or receiving data should be negotiated with privacy risks in mind. Retailers' software-related and cloud vendor agreements warrant extra scrutiny from both directions.

Software developers may face the most drastic and immediate changes and, in the near-to-middle term, have the most to gain or lose. If a developer has not yet adopted privacy-by-design and security-by-design principles, they may be behind the curve. If they are delivering embedded software or code for reuse or integration in a regulated field, but have not yet begun including a software bill of materials in their deliverables, an update of their processes would be prudent. And if they have not yet done so, developers should start considering what security folks think of their code—even automating security integration—throughout the development process (known as "DevSecOps"). This "quality control" mindset is widely used to mesh code development with operations, but security should no longer be considered afterward. Appreciating the importance of "baking in" security should be the way forward, understanding that a company's profitability may hinge more and more on the security of their work product.

For companies that are—or work with anyone—involved with sales of software to the government, objects in this mirror may be closer than they appear. Under President Biden's Executive Order 14028, federal agencies must ensure the integrity of any third-party software they use, including firmware, operating systems, applications and application services (e.g., cloud-based software), as well as other products containing software later this year.

This requirement will give visibility to software publishers' and users' mistakes, placing a spotlight on what could have been done to prevent or mitigate them. Software service and development agreements must be negotiated and managed to ensure that required reports can be prepared. And responsibility-shifting does no good if the software/service provider is unable to pay for that liability, so credit screening, bonding and insurance may need to be (re-)negotiated into those agreements.

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

FBT Gibbons

The strategy has fired the first serious salvo at shifting liability to software developers. In our view, it is fairly conceivable that one state, and then more, will accept this policy recommendation and push it forward before Congress ever acts. Given that prospect, retailers, developers and critical infrastructure players who start to plan adaptable strategies should now get ahead of the news, achieve market differentiation and lower their costs to adapt to the new playing field.

For more information, please contact any attorney with Frost Brown Todd's Data, Digital Assets & Technology practice group.

This article was originally published in The Indiana Lawyer.

© 2026 FBT Gibbons LLP. May be considered attorney advertising in some jurisdictions.

2026 FBT Gibbons LLP. All rights reserved. ADVERTISING MATERIAL.

FBT Gibbons