FOSS FORCE
KEEPING TECH FREE

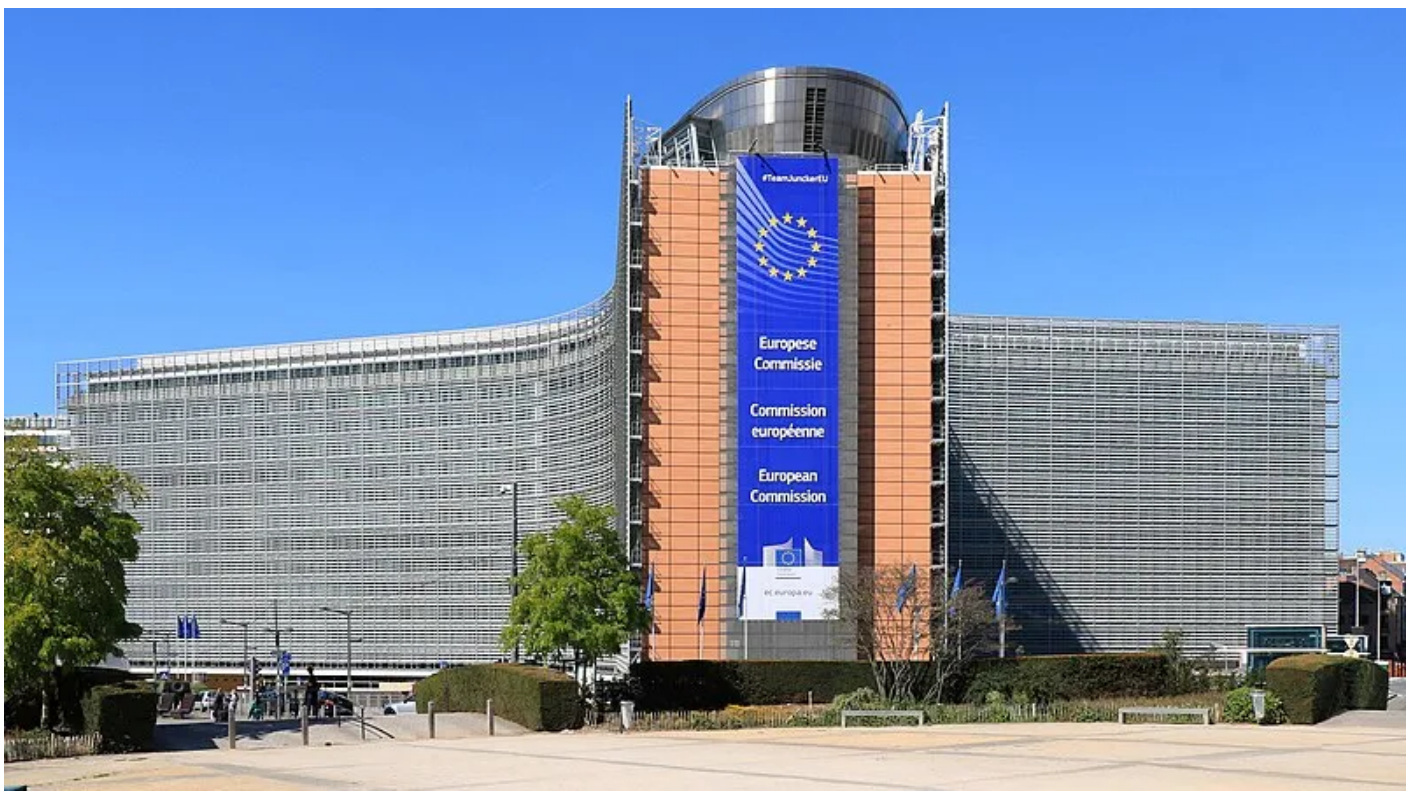
September 27, 2023



# Bad News for Open Source: EU Committee Approves the Cyber Resilience Act

BY CHRISTINE HALL ON JULY 21, 2023 | NEWS ANALYSIS AND POLITICS

*A large number of open-source organizations are saying that if this act is enacted into law, it will do damage to open-source, both in Europe and globally.*




EmDee, CC BY-SA 4.0, via Wikimedia Commons

On Wednesday the European Union approved a draft of the Cyber Resilience Act, which is supposed to make software safer. Many open-sourcers, however, think this passage is bad news and claim that, as written, the act would stymie open source development. The good news is that this approval doesn't make the act law — not yet, anyway.

What's happened so far is that the draft legislation has been approved by the EU's Industry, Research, and Energy Committee (ITRE). From here, the proposal moves into what the EU calls the "trilogue" phase, where it gets discussed with the EU Parliament in advance of a vote.

"I'm discouraged that the proposed legislation has made it this far, and concerned that industry response so far is not robust enough to counter what is likely to be very damaging if it is enacted," Joe Brockmeier, head of community at Percona said in a statement after the approval was announced.

It's not as if there's been a lack of response. So far, organizations speaking out against the proposed legislation included The Apache Software Foundation, Eclipse Foundation, GitHub, Linux Foundation, and others.

In addition, on July 11 four major industry associations (The Software Alliance, Computer & Communications Industry Associations, Developers Alliance, and Information Technology Industry Council) signed a three page letter titled "Joint Recommendations for a Feasible Cyber Resilience Act," outlining issues and fixes they think the act needs.

We here at FOSS Force have also been trying to get the word out. On July 15, we published an article called “Will the European Cyber Resilience Act Kill Open Source Software?” that was written by Gaël Duval, CEO of Murena and founder of both /e/OS and Mandrake Linux, and CEO at Murena.

“Critics argue that the CRA could impose increased legal and financial responsibilities on open source contributors, potentially stifling innovation and damaging the open source ecosystem,” Duval said. “Furthermore, the legislation’s vulnerability disclosure requirements could inadvertently expose software vulnerabilities to a larger audience, increasing the risk of malicious exploitation.”

## What’s Wrong With the Cyber Resilience Act?

The issues people are warning about have little to do with the act’s intent, but against what’s seen as an approach that’s designed to benefit large commercial software vendors while making life difficult for open-source projects that are largely developed within nonprofit foundations.

“While legislation could and perhaps should play an important role in cybersecurity, the legislation being considered has been rushed through and has not had sufficient time for affected organizations and individuals to respond,” Brockmeier explained. “The current draft poses a significant threat to open source software development. Its intended scope and impact is going to threaten open source development, disadvantage smaller players in the market, and will likely do more harm than good.”

Brockmeier knows his way around open-source. In addition to his current stint at Percona, he spend nearly nine years at Red Hat and more than 1 1/2 years as the VP of marketing and publicity at the Apache Software Foundation.



“Open source software development works best when developers are able to collaborate without taking into account employer or nationality,” he said. “We’ve seen problems before around encryption and U.S. regulations, as well as restrictions on collaboration with people in sanctioned countries. The EU requiring reporting of vulnerabilities to an EU institution is likely to lead to distorted reporting of security vulnerabilities. Projects that are subject to these restrictions, e.g. those that have European developers, will likely be routed around.”

Amanda Brock, CEO at OpenUK, a nonprofit organization that supports open source collaboration and open technologies within the United Kingdom, agrees.

“Their persistent focus on purely giving carve outs to SMEs [small to medium-sized enterprises] and failing to do the same for foundations shows a complete lack of understanding of how open source software works, despite having had an Open Source Program Office [European Commission Open Source Programme Office] for five years. The focus on SMEs rather than the nature of open source is extremely short-sighted and feeds into a cycle of perpetuating the lack of growth of European tech companies.”

## Is the EU Shooting Itself in the Foot?

Brockmeier and Brock recognize that there's a possibility that if the act is passed as it stands now, Europe could be the big loser. Brockmeier points to the "strong possibility" that developers might try, "to avoid doing development in Europe altogether. This is not something that would be easily achieved, but it is a real possibility that the CRA will drive some development and participation in open source out of Europe."

Brock makes nearly the same point.

"There is talk that providers will now simply block their code going into Europe in a similar approach to the way export control is managed," she said. "This could be deeply damaging to Europe's tech sector."

Although some organizations, such as Apache, are primarily advocating carving out a special niche for open-source projects that aren't under a single vendor's control, Brockmeier is advocating a more wholesale rethinking.

"Having to comply with these regulations will put startups and small businesses that ship software at a major disadvantage," he said. "In the rush to do 'something' about security, it's important that we don't destroy or damage a vital commons that serves everyone equally. If the CRA can't be stopped at this juncture, we must at least seek to ensure it is improved before it's too late."

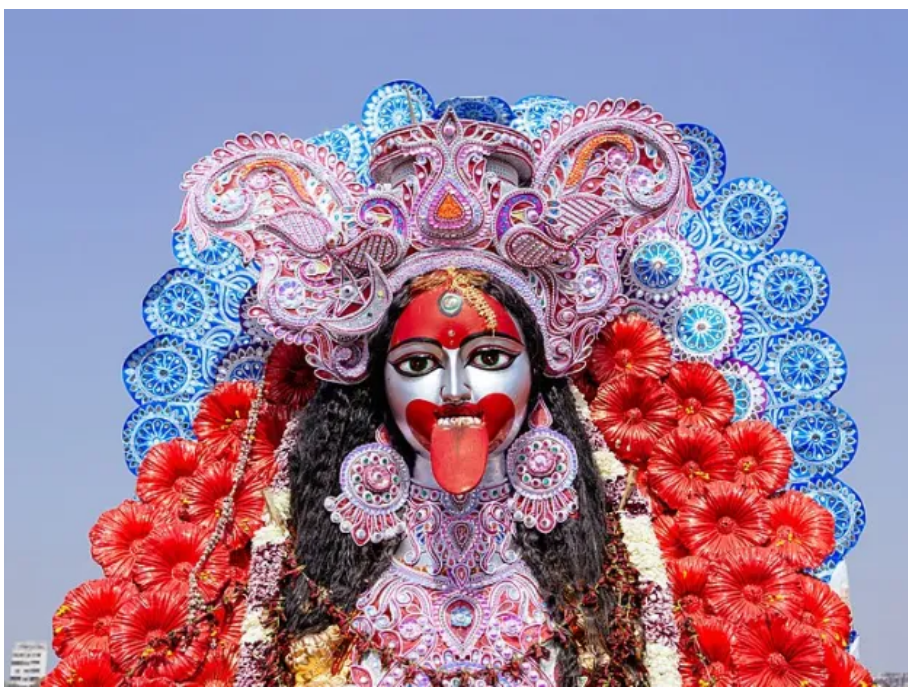

Christine Hall

Christine Hall has been a journalist since 1971. In 2001, she began writing a weekly consumer computer column and started covering Linux and FOSS in 2002 after making the switch to GNU/Linux. Follow her on Twitter: @BrideOfLinux

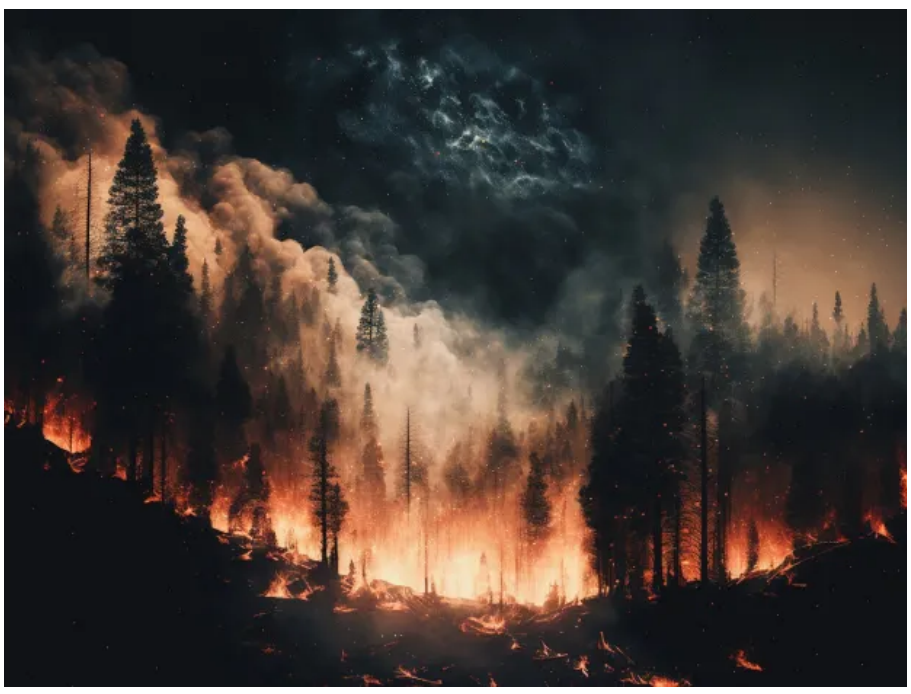
FOSSForce.com


*Published in News Analysis and Politics*


More from **News Analysis** More posts in News Analysis »

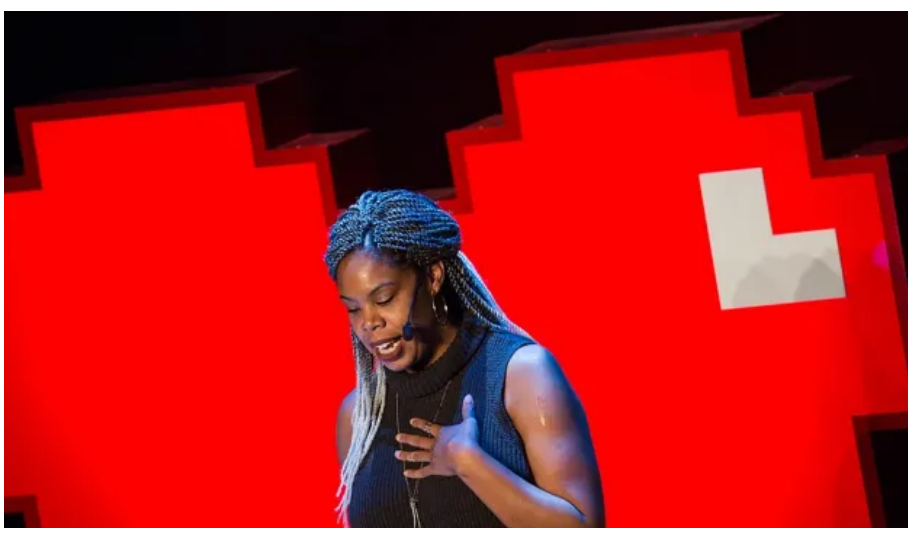


FOSS Week in Review: Kali Cleans House, Kalendar Becomes Merkuro, Brave's Unfree Assistant, & More...



Consequence of Ottawa's 'Link Tax' Dampens News on Canadian Wildfires

More from **Politics** More posts in Politics »



EFF's Two New Board Members Bring Equality and Security Cred to the Table

Consequence of Ottawa's 'Link Tax' Dampens News on Canadian Wildfires

*Keeping tech free*