Court case probes open-source licenses as movement stands at crossroads

The Software Freedom Conservancy's lawsuit against TV-maker Vizi begins trial in California, raising questions about open-source license and the risks posed by adhering to them.

By Emma Hilary Gould
29 Mar 2024

It was February 1989, and on the fifth floor of 51 Franklin Street in Boston, Richard Stallman, then a 36-year-old programmer and graduate of MIT and Harvard, was writing the **first version** of the GNU General Public License. Stallman had founded the Free Software Foundation, the first open-source nonprofit, just four years earlier.

Better known as GPL, the license introduced the concept of copyleft, a stipulation that any modification made to GPL code, or any code generated from it, must also be licensed under GPL. Everyone had

permission to modify and redistribute GPL, Stallman wrote, but no distributor had permission to restrict further redistribution—in other words, any piece of GPL-licensed code must be able to be made public.

In a trial that began on March 25, another open-source non-profit, the Software Freedom Conservancy (SFC), is battling television manufacturer Vizio, alleging that the budget TV-maker **violated the terms of GPL** by failing to make its GPL-derived source code public. Previous cases of a similar vein were typically brought by the original copyright holder of the code, meaning that federal courts in the US could dismiss the claims under the fair use doctrine that allows courts to excuse instances of copyright infringement if it deemed it was in the public interest.

The genie's kind of out of the bottle on that

Nick Kolba, Connectifi

If the SFC is successful, the case could change the way open-source licenses are litigated, setting a precedent for anyone to bring a case against a company found to be in violation of GPL.

Nearly 35 years after Stallman's original draft of the GPL, about **90% of all software** depends on open-source code, according to widely cited numbers from Sonatype, a vendor of software supply chain management solutions, with the GPL license being the most common.

Despite widespread usage, some in the open-source community worry it is a pyrrhic victory, as corporations—especially Big Tech—have profited heavily from open source. Tensions within this niche community can be felt in the finance and broader tech industries, where new cybersecurity regulations and **increased focus on third-party risks** are casting a harsher glow on open-source software.

Folie à deux

The relationship between the open-source and financial communities is almost ironic. Gabriele Columbro, the executive director of the Fintech Open Source Foundation (Finos), says he sometimes wonders what to wear to conferences. “A suit, to show similarity with the finance people? Or should I play [Mark] Zuckerberg and come in pajamas or my hoodie?” he says.

When Finos was founded in 2018, most banks were not aware of how much open-source software their developers were using, Columbro says. But since then, open source has gone from a non-starter or taboo, to an **openly sought skillset**. Banks have set up open-source program offices to act as centralized authorities with policies that govern the use of open source. Often, Columbro says, the primary goal is to ensure license compliance.

According to statistics from Black Duck, a frequently cited vendor of open-source detection software, 53% of codebases the company consulted on in 2023 **contained a license conflict**. Black Duck general manager Philip Odence, whose team oversaw the report, estimates that the overall number of companies with some license violation is likely closer to 85%, given that companies typically employ multiple codebases.

“The open-source world is watching closely,” Odence says of the Vizio trial. He notes that the “lion’s share” of code today is open source, used for “the wheels you don’t want to reinvent. … That’s a good thing, not a bad thing.”

Even in finance, where the risks of open-source software may appear greater, it is difficult to program without it. “There’s a reason why the internet looked like it did in the early 2000s,” harkening back to broken links, static webpages, and error codes, says Nick Kolba, the founder and CEO of **Connectifi**, a provider of cloud-based **desktop interoperability**.

Kolba is also the creator of the FDC3 protocol, a set of codified specifications for writing APIs and for messaging that enables traders’

desktop applications to interoperate and share information that is now an open standard under the auspices of Finos.

Despite most corporations viewing GPL as a "poison pill," financial companies would have a hard time disentangling themselves from it. Most developers would not be able to function without it. "The genie's kind of out of the bottle on that," Kolba says.

Given this reliance, license compliance has become especially important as **regulators turn their gaze** to third-party risk and the practice of outsourcing. In the EU, one stipulation of the recent Digital Operational Resilience Act (Dora) is a requirement for open-source analyses, in which companies must take stock of their dependencies on open source as part of the act's testing program.

John Salmon, a partner at London-based law firm Hogan Lovells, says Dora's broad definition of an information communication technology service has brought basic software licensing into the fold. "Dora is much bigger than people realize," he says.

Some suggest the renewed attention on open-source licensing, both from open-source activists and financial regulators and governments, is a by-product of the generative AI boom, which has placed greater scrutiny on the relationship between copyright and technology.

In late February, the **White House asked for public comments** on whether AI models should be open source or closed. The statement came a month after it published **the first report** of its recent Open Source Security Initiative, a part of the Biden administration's **2021 Executive Order** on cybersecurity.

Across the Atlantic, the European Commission's **Cyber Resilience Act** has garnered consternation from some in the open-source community as it has stretched regulatory scrutiny deeper into the software supply chain. "The sort of legislation we're seeing, like the Cyber Resilience Act, is hugely problematic," says Amanda Brock, CEO of OpenUK and a former lawyer.

Questions raised by the Vizio case and by adjacent legislation have placed open source at a crossroads. Brock says she thinks the open-source industry is still in a good position at this juncture, but is experiencing what she calls “growing pains.”

“We’re at a point in time where we’re seeing people move away from open source because they’re having business concerns. … There are some really meaty, interesting questions that need to be answered around whether open source will survive. It will be very difficult to pull [the open-source code] out, but it would be easier over a longer period of time to replace it, if necessary,” she says.

In finance, where license compliance—especially in the case of GPL—can be a cybersecurity concern in and of itself, some feel they could be caught in a catch-22, where users must balance open-source license compliance, such as sharing source code, with preventing hackers and competitors from accessing proprietary or sensitive code.

“This is where SFC coming in is interesting—bad, if you’re an unwitting user of open source,” Hogan Lovells’s Salmon says. “The obvious question clients then ask is, ‘Well, so what, John? What if we don’t do it?’ This is where we come back to the *SFC v. Vizio* case.” If the proprietary code is out in the open, Salmon says, it likely does make it easier for hackers to enter the mobile app or the core banking system.

Finos’s Columbro says he does not expect the case to generate massive backlash or a retreat from open source but that it is a big deal, all the same.

“I think what it really underlines is that open source is everywhere,” he says.
