Proskauer

Two Notable Tech Law Decisions That Closed Out the Summer: CDA Immunity Protections for a Software Platform, CFAA "Authorized Access" Issues, Passwords as Trade Secrets

New Media and Technology Law Blog on **October 24, 2025**

In the closing days of August, two federal appeals courts issued noteworthy decisions at the intersection of workplace conduct, computer law and online platforms. The two opinions were released during a period of time this past summer amidst the continuing flurry of AI-related case developments and perhaps did not get wide media attention (but which might prove to be important cases in the future).

- **Second Circuit – CDA Section 230**. The court ruled that a software platform was not entitled to CDA Section 230 immunity – at least at the early stage in the case – based on allegations that it actively contributed to the unlawful software content at issue by manufacturing and distributing an emissions-control "defeat devices." (*U.S. v. EZ Lynk, SEZC*, No. 24-2386 (2d Cir. Aug. 20, 2025)). The opinion's discussion of what it means to be a "developer" of content has implications for future litigation that might involve generative AI, app stores, marketplaces, and IoT ecosystems, where certain fact patterns could blur the line between passive hosting and active co-development.
- **Third Circuit – CFAA and Trade Secrets**: Days later, the Third Circuit issued an important decision (subsequently amended, with minor changes that did not change the holding) that further develops CFAA case law post-*Van Buren*. The court held that CFAA liability, an anti-hacking statute, does not extend to workplace computer use violations. (*NRA Group, LLC v. Durenleau*, No. 24-1123 (3d Cir. Aug. 26, 2025) (vacated by Oct. 7, 2025 amended opinion), *reh'g en banc denied* (Oct. 7, 2025)). The court also addressed and rejected a novel claim of trade secret misappropriation based on access to account passwords.

Together, the cases show how courts continue to interpret the reach of technology-related statutes in contexts never contemplated when those laws were first enacted.

Second Circuit – CDA Section 230 Immunity Denied for Software Platform

The Second Circuit *EZ Lynk* case centered on whether a platform that connects vehicles to cloud-based diagnostic and customization software could be held liable under Section 203 of the Clean Air Act, 42 U.S.C. § 7522(a)(3)(B), which prohibits the manufacture and sale of devices used to defeat vehicle emissions controls. The government argued that the EZ Lynk System, which consists of an electronic device, a mobile app and third party software (or "defeat tunes"), was an illegal "defeat device" because it enabled car owners to download and install "delete tunes" that disable manufacturer-installed emissions controls. EZ Lynk countered that its system was a neutral tool that, by itself, has no effect on emissions controls and therefore EZ Lynk should be shielded from liability by CDA Section 230 because it merely hosted the third-party software at issue.

In March 2024 the lower court dismissed the government's case on the main count on CDA grounds, reasoning that even if the EZ Lynk System was a defeat device, EZ Lynk was only acting as a publisher of third party content. The lower court concluded that EZ Lynk's alleged collaboration with defeat tune creators and EZ Lynk's employees' social media interactions with users to assist in installation and use did not amount to "material contributions" that would defeat Section 230 immunity.

The Second Circuit reversed. It found the complaint adequately alleged that EZ Lynk "directly and materially contributed to" the creation of delete tunes and may not have acted as a neutral intermediary. Among other things, the court pointed to allegations that EZ Lynk worked closely with major "delete tune" creators (e.g., previewing devices with them before launch and ensuring compatibility) and administered a social media forum where its employees and partners advised customers on using delete tunes. At this early stage, the court held such allegations were sufficient to defeat EZ Lynk's CDA Section 230 defense as it may have been an "information content provider" in part.[1]

The decision reaffirms that Section 230 immunity may not apply where a platform "directly and materially contributed to the underlying illegal conduct." Although the context of this government enforcement was a novel one for interpreting CDA immunity, the reasoning may resonate in other settings, including software platforms that promote and directly assist app developers with unlawful functions or modifications (e.g., for IoT devices) and marketplaces that facilitate illegal product use, raising the risk of being treated as a co-developer of unlawful content.

Third Circuit – CFAA and Trade Secret Claims Against Employees

In *NRA Group*, the company argued that two employees violated the CFAA when one of them, while home sick, asked a colleague to log into her work computer to retrieve a spreadsheet of system passwords to help her remotely access a work document, all in violation of workplace computer policies.

CFAA Issue

The Third Circuit held that the employees' conduct did not violate the CFAA because: (1) The statute targets "hacking" or code-based unauthorized access, not workplace policy violations by current employees; (2) Both employees were authorized users of the employer's computer systems; even though the employees may have violated computer use policies (e.g., sharing credentials, emailing passwords), the court found they acted within their granted access rights. The Third Circuit affirmed dismissal of the company's action against the employees. [Note: This holding is reminiscent of a prior Ninth Circuit decision rejecting CFAA liability against an employee that emailed internal documents to himself after being given credentials to do so from a colleague].

Applying the Supreme Court's *Van Buren* decision, the Third Circuit held that the CFAA's "exceeds authorized access" provision covers those who obtain information from computer networks or databases to which their computer access does not extend. As such, the court stated that "absent evidence of code-based hacking, the CFAA does not countenance claims premised on a breach of workplace computer-use policies by current employees." In the *Van Buren* decision's most cited metaphor, the Supreme Court characterized the CFAA "authorization" scheme as a "gates-up-or-down" approach where the CFAA prohibits accessing data one is not authorized to access. Under this understanding, one either can or cannot access a computer system, and one either can or cannot access certain areas within the system, as some areas are fully "off limits." Following this rationale, the Third Circuit held: "Under *Van Buren*, the 'gates' of access were 'up' for both women—neither hacked into NRA's systems. […] No one hacked anything by deploying code to enter a part of NRA's systems to which they had no access."

The *Van Buren* decision continues to shape CFAA litigation beyond the employment context. Its reasoning has featured prominently in disputes over web scraping (e.g., in this closely-watched litigation) where courts must decide whether a website's "authorization gates" are open or closed to scrapers and whether technical measures suffice to close those gates.

Trade Secret – Passwords Issue

In an issue we don't ever recall seeing in recent years – even the court found caselaw on this point was "thin and undeveloped" – the Third Circuit also considered the company's trade secret claim based on the allegation that the creation and emailing of the password spreadsheet at issue constituted trade secret misappropriation. The court rejected the claim, finding that the passwords themselves are "letters and numbers" and are not protectable trade secrets because they lack independent economic value apart from what they protect. Under general law, trade secrets must have independent economic value, and while the passwords were a compilation of data, they were not bundled with other, presumably protectable information like raw customer information or pricing strategies. Unlike a proprietary formula or customer list, the value of a password lies only in its role as a barrier, one that can be eliminated simply by changing it.

---

[1] In pertinent part, Section 230(c) states: "No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider." 47 U.S.C. § 230(c)(1). The Complaint alleges the EZ Lynk Cloud is a platform on which people exchange information in the form of software. As a side note, the appeals court noted that it was not ruling on whether software is "information" under Section 230 – in most cases, "information" typically pertains to content, in many forms. Though, it did cite other decisions that found that software could be "information provided by another content provider," including one decision where an app store was protected by CDA immunity for losses from a fraudulent crypto wallet app (a ruling that was later affirmed by the Second Circuit).

View original.

Related Professionals

- **Jeffrey D. Neuburger**