When does a journalist become a hacker?



Some laws operate like hidden trap doors — everyone walks across the trap at one point or another, but only a handful of us actually fall through. For the rich, it's the law against insider trading; for the rest of us plebs, it's the Computer Fraud and Abuse Act.

On Thursday, federal law enforcement arrested journalist Tim Burke and arraigned him in court in handcuffs. Twelve of the 14 charges levied against him in the since-unsealed indictment are under the Computer Fraud and Abuse Act (CFAA), the federal anti-hacking statute.

The story begins with Tucker Carlson's extremely cursed interview of Kanye West in 2022. Most interviews are edited for clarity; in this case, the interview was cut to exclude a rambling, antisemitic rant. That unaired clip and others made their way to *Vice* and Media Matters through Burke, who downloaded them from LiveU, a streaming service that media companies use to share video files. The FBI raided Burke's home last year, seizing phones, laptops, hard drives, and

notes.

The indictment is an incredible example of how the CFAA tortures the English language. It accuses Burke of "repeatedly utiliz[ing] the compromised credentials to gain unauthorized access to the Victim Entities' protected computers." Burke and his lawyers have maintained that he found the video clips after using demo login credentials that had been posted publicly on the internet, and that the files could be shared via unsecured, public URLs.

If so, that probably wasn't the ideal IT setup for the media outlets that were using LiveU. They may have, in fact, objected very strongly to strangers being able to access their outtakes. But is that enough to establish "unauthorized access"? Should it be?

For a good long time, it was ambiguous whether violating a website's terms of service could be a felony

The universe of wack CFAA prosecutions is rich and diverse because the CFAA is so easy to weaponize. The statute hinges on access "without authorization" or access that "exceeds authorization." It doesn't really specify what a "protected computer" is. (A better question might be: *what's an unprotected computer?*) For a good long time, it was ambiguous whether violating a website's terms of service could be a felony with serious jail time. The 2021 Supreme Court decision in *Van Buren v. United States* narrowed the CFAA down enough that that's no longer a concern. (The timing was inadvertently clutch, as shortly thereafter Netflix began to crack down on password sharing *and* everyone started getting whipped up over AI companies scraping websites against operators' wishes.)

Because Burke is a journalist, what may come to mind first is the case against journalist Matthew Keys, convicted in 2015 after he posted the content management system credentials for his erstwhile employer into a public chatroom while urging

others to deface the website. Keys, whose actions there resemble neither hacking nor journalism, was prosecuted under a provision of the CFAA prohibiting "damage without authorization." It's a different section of the law, though the same sticky problem with the meaning of "authorization" pops up yet again.

But Burke's case is much more analogous to those of much-lamented and admired Aaron Swartz (sometimes called "the internet's own boy") or the unlamented and less-admired Andrew "weev" Auernheimer (often called "a notorious troll" and "a terrible person"), both of whom were famously prosecuted under the CFAA for scraping readily available information.

Auernheimer's conviction stemmed from a script that automatically accessed a series of public URLs that unfortunately contained AT&T customer information. Swartz was prosecuted for scraping JSTOR, a paywalled academic database that could be freely accessed on MIT's campus network. Theoretically, his access began to "exceed authorization" when he signed into the network as Gary Host (G. Host, or Ghost), and then when, after campus IT attempted to block his computer for excessive server requests, he spoofed his DNS.

Swartz and Auernheimer aren't known as journalists, though both are associated with media publications — Swartz was a contributing editor to the left-wing magazine *The Baffler*, and Auernheimer sometimes writes for the Daily Stormer, a white supremacist website he has helped manage on the technical side. Their respective prosecutions speak to that side of their personalities. Swartz scraped JSTOR in hopes of liberating scholarship for the whole world; Auernheimer, who did not write any of the code he was jailed for, acted as the official hype man for the AT&T breach because he loves attention.

Auernheimer's conviction was overturned in 2014 by an appeals court on a technicality; Swartz's case never went to trial

because he died in 2013. Aaron’s Law — a bill to reform the CFAA — was proposed in the wake of his suicide but stalled in Congress.

If these two men had been written into a novel, their characters would be derided as ham-fisted symbols of the noble and ignoble instincts that drive journalism. As it is, it’s maybe shocking that journalists aren’t being prosecuted all the time. When you define “authorization” that loosely, of course a journalist will end up on the hook — journalism in the modern day is the act of using your computer in a way someone somewhere would really rather you did not.

The case against Tim Burke is almost a bizarre historical throwback. On all sides — the legislature, the courts, and even the DOJ — people seem to know that there is something wrong with the CFAA. It’s a law that can be made to fit a dizzying array of scenarios, to take down progressive idealists and literal neo-Nazis with equal efficacy. And here we are again, squinting at websites and asking, “Is this a protected computer?”

https://www.theverge.com/2024/2/23/24081656/tim-burke-journalism-hacking-cfaa