Is the Justice Department Even Following Its Own Policy in Cybercrime Prosecution of a Journalist?

Andrew Crocker ⋮ 4-5 minutes ⋮ 2/22/2024

Following an FBI raid of his home last year, the freelance journalist Tim Burke has been arrested and indicted in connection with an investigation into leaks of unaired footage from Fox News. The raid raised questions about whether Burke was being investigated for First Amendment-protected journalistic activities, and EFF joined a letter calling on the Justice Department to explain whether and how it believed Burke had actually engaged in wrongdoing. Although the government has now charged Burke, these questions remain, including whether the prosecution is consistent with the DOJ's much-vaunted policy for charging criminal violations of the Computer Fraud and Abuse Act (CFAA).

The indictment centers on actions by Burke and an alleged co-conspirator to access two servers belonging to a sports network and a television livestreaming service respectively. In both cases, Burke is alleged to have used login credentials that he was not authorized to use, making the access "without authorization" under the CFAA. In the case of the livestream server, he is also alleged to have downloaded a list of unique, but publicly available URLs corresponding to individual news networks' camera feeds and copied content from the streams, in further violation of the CFAA and the Wiretap Act. However, in a filing last year seeking the return of devices seized by the FBI, Burke's lawyers argued that the credentials he used to access the livestream server were part of a "demo" publicly posted by the owner of the service, and therefore his use was not "unauthorized."

Unfortunately, concepts of authorization and unauthorized access in the CFAA are exceedingly murky. EFF has fought for years—with some success—to bring the CFAA in line with common sense notions of what an anti-hacking law should prohibit: actually breaking into private computers. But the law remains vague, too often allowing prosecutors and private parties to claim that individuals knew or should have known what they were doing was unauthorized, even when no technical barrier prevented them from accessing a server or website.

The law's vagueness is so apparent that in the wake of *Van Buren v. United States*, a landmark Supreme Court ruling overturning a CFAA prosecution, even the Justice Department committed to limiting its discretion in prosecuting computer crimes. EFF felt that these guidelines could have gone further, but we held out hope that they would do some work in protecting people from overbroad use of the CFAA.

Mr. Burke's prosecution shows the DOJ needs to do more to show that its charging policy prevents CFAA misuse. Under the guidelines, the department has committed to bringing CFAA charges only in specific instances that meet all of the following criteria:

- the defendant's access was not authorized "under any circumstances"
- the defendant knew of the facts that made the access without authorization
- the prosecution serves "goals for CFAA enforcement"

If Mr. Burke merely used publicly available demo credentials to access a list of public livestreams which were themselves accessible without a username or password, the DOJ would be hard-pressed to show that the access was unauthorized under any circumstances and he actually knew that.

This is only one of the concerning aspects of the Burke indictment. In recent years, there have been several high-profile incidents involving journalists accused of committing computer crimes in the course of their reporting on publicly available material. As EFF argued in an amicus brief in one of these cases, vague and overbroad applications of computer crime laws threaten to chill a wide range of First Amendment protected activities, including reporting on matters of public interest. We'd like to see these laws—state and federal—be narrowed to better reflect how people use the Internet and to remove the ability of prosecutors to bring charges where the underlying conduct is nothing more than reporting on publicly available material.