Twitter Thread by Cory Doctorow

Cory Doctorow
@doctorow

It's been eight years since @aaronsw took his own life. Aaron had been charged with 13 felonies under the Computer Fraud and Abuse Act (#CFAA) for violating the terms of service on the @JSTOR database of scholarly articles.

1/

Prosecutors Stephen Heymann and Carmen Ortiz didn't dispute that Aaron was allowed to access the articles he retrieved. Rather, they said that the WAY he accessed them (using a script instead of clicking on links) was a terms-of-service violation and hence a crime.

2/

In other words: any business could conjure a felony out of thin air by making you click through an unreadable garbage-novella of legalese proscribing the use of a service they granted you access to. Violate any of those terms and you face a prison sentence.

3/

This isn't law as we know it, it's Felony Contempt of Business Model, and the most alarming thing was that this interpretation of the CFAA wasn't completely ridiculous, given how badly drafted that law is.

4/

Ronald Reagan signed CFAA into law. Fed prosecutors had been seeking broad authority to punish "hacking" and had drawn up an absurdly broad definition of cybercrime that would give them latitude to go after anyone they didn't like.

5/

They wanted to define hacking as "exceeding your authorization" on a computer that didn't belong to you. Even in the mid-1980s, legal and technical scholars recognized the potential dangers of a definition this broad, but not Ronald Reagan.

6/

Then Reagan got spooked by the movie Wargames - yes, the one with Matthew Broderick - and urged the dimbulbs in the Congress and Senate to send the CFAA to his desk. They obliged, he signed it, and CFAA became law in 1986.

7/

In the decades since, CFAA has become a major source of cybersecurity mischief. Security researchers who audit systems and warn their users about defects in them are silenced with CFAA threats, giving companies a veto over who can criticize them and how.

8/

Monopolistic online businesses threaten their competitors with CFAA liability. Companies like Facebook have managed to prevail in court, interpreting CFAA the same way Aaron's prosecutors did, making terms-of-service violations into violations of the law.

9/

But cracks have appeared in this dangerous interpretation of CFAA. The @ACLU and a group of journalists have been litigating to overturn portions of the law since 2016:

https://t.co/JPut5Fgv7A

10/

And in 2019, the Ninth Circuit Court of Appeals produced a remarkably good ruling on CFAA in Hiq v Linkedin, splitting with its own (terrible) precedents in Power Ventures and Nosal II.

https://t.co/EKPpbIrqeT

11/

But the main event for CFAA-fighters has been at the Supreme Court this year, where the Van Buren case promised to make or break the worst elements of the CFAA for good.

12/

The truism "hard cases make bad law" was especially true in Van Buren. Nathan Van Buren was a crooked Georgia cop who took a bribe to look up a sex-worker's personal information in the state law-enforcement database in a FBI sting.

13/

Van Buren thought he was helping a criminal determine whether the sex-worker was an undercover cop.

Van Buren is a bad man and a bad cop.

But he isn't a hacker.

14/

Nevertheless, prosecutors charged him under the CFAA, saying that while he was allowed to access the database, doing so for an improper purpose was a hacking crime, because he "exceeded his authorization."

15/

This may sound sensible - or just expedient - to you. But if the prosecutors were right - if accessing a computer you were authorized to use, but in an unauthorized way - is a felony, then almost everyone is a felon.

16/

The DoJ's theory of the CFAA would make most terms-of-service violations into potential jailable offenses (think "sharing Netflix passwords"). If federal prosecutors gain the power to threaten prison for anyone - everyone - this won't be used to rid the world of dirty cops.

17/

Rather, it will be used against people who already bear the brunt of prosecutorial overreach, creating leverage over the victims of dirty cops.

Thankfully, the Supremes agreed. Yesterday, they handed down a good - if not great - ruling in Van Buren.

18/

The best analysis - as ever - comes from my @EFF colleagues @kurtopsahl and @aaron_d_mackey.

https://t.co/uOf9altGpw

19/

As they point out, the heart of the ruling is a ban on breaking into computer systems - not criminalizing entering the wrong command into a computer you're allowed to use.

20/

This correct interpretation (far narrower than the DoJ's) safeguards security researchers, competitors, and other researchers doing things like gathering data from a housing site to investigate racial bias in rental ads.

21/

As the court pointed out, the DoJ's interpretation was so broad that it could criminalize "embellishing an online-dating profile to using a pseudonym on Facebook."

22/

The ruling was good, but not perfect. A single footnote explains that the court isn't ruling on whether the CFAA only applies when someone bypasses a technical measure, which leaves the door open to turning policy and contract violations into crimes.

23/

SCOTUS got it (mostly) right here. They vindicated Aaron Swartz and all the other victims who were bullied, silenced and terrorized by the CFAA. They took a huge step towards undoing one of Ronald Reagan's many idiocies.

24/

Van Buren should be punished for corruption - under anti-corruption law, not under a definition of hacking so broad that it captures normal activities we all engage in several times, every day.

Image:
Sage Ross
https://t.co/v5DNkF72C4

CC BY-SA:
https://t.co/guhq1dyHz1

eof/

ETA - If you'd like an unrolled version of this thread to read or share, here's a link to it on https://t.co/iSBh8s9m7q, my surveillance-free, ad-free, tracker-free blog:

https://t.co/aXvTZ5o9d6