# Comment: Online civil rights enforcement could hinge on Section 230 showdown in US Fourth Circuit

29 Oct 2021 | 22:36 GMT | **Comment**
By Dave Perera

A US appeals court will examine whether Section 230 trumps another law guaranteeing consumers' access to their digital dossiers held by the background-check industry. Regulators and civil rights advocates are concerned.

Whether the lucrative background-check industry can play by the same online liability rules as Facebook and Twitter is set to be fought in a US appeals court case that's drawn the worried attention of federal regulators and civil rights advocates.

Apply for a job or rent an apartment and prospective employers and landlords almost certainly will pay for a background check. Much hinges on the accuracy of those reports, and a federal law guarantees individuals the right to obtain and correct their dossiers.

A federal district judge has thrown those rights into doubt after ruling that another federal statute takes precedent — the same statute that shields online platforms against countless lawsuits provoked by the content appearing on their networks.

Opponents say the May ruling from Henry E. Hudson — the Richmond, Virginia, judge known as "Hang 'Em High Henry" — won't just unleash background checks from safeguards meant to ensure accuracy and transparency.

The logic behind Hudson's ruling places any business governed by civil rights laws beyond the reach of enforcers, they argue, so long as the violation occurs on the Internet and the violator isn't the direct author. A racist restaurant owner could post in his online menu a picture depicting segregated access to service taken during the Jim Crow era and claim the same legal immunity as online platforms with user-generated content.

The case underscores how deeply the Internet has permeated everyday life, making almost any significant life event such as a new job or new home impossible without online intermediation. It raises questions about how a corpus of civil rights law designed for an analog world applies to the digital universe. It yet again throws a spotlight on the 1996 law that freed online platforms from liability when hosting third-party content: Section 230 of the Communications Decency Act.

In a world where practically everything is online, judges in the US Court of Appeals for the Fourth Circuit will have to answer the question of whether Section 230 entitles nearly every website to duck responsibility for what appears on it.

— The plaintiffs —

Hudson's ruling stems from a case brought by three Virginia men who accuse a Texas public data aggregator of selling online rap sheet reports linking them to an inaccurate criminal past.

The Source for Public Data, they asserted, should have responded to multiple requests for a copy of their file and complied with disclosure and certification requirements under the Fair Credit Reporting Act.

One of the men, a former truck driver named Tyrone Henderson, Sr., says he's been followed for more than a decade by erroneous background checks linking him to the felony conviction of a stranger in western Pennsylvania with almost the same name and the same birthday. It's made obtaining employment exceedingly difficult (see here).

A consequence of concerns that employers, creditors and insurers were relying on false and subjective information collected by credit bureaus, the 1970 Fair Credit Reporting Act was the first federal law to regulate how businesses use personal information.

The statute put a stop to an era when credit bureaus paid investigators pressured into finding dirt to poke into individuals' drinking habits and sexual orientation. It was supposed to put a stop to stories like Henderson's. A 1971 article by Time Magazine celebrating the act's passage into law noted the eight year "Kafkaesque nightmare" of a New York salesman who couldn't get a job because the Retail Credit Co. — known today as Equifax — falsely reported him as dishonorably

discharged from the military.

The Virginia men's suit seeks statutory and punitive damages for violations of duties owed by consumer reporting agencies on behalf of similarly affected Virginia residents. Aided by the Internet and low barriers to entry, the US background report industry has grown to nearly $3 billion annually, according to analysis from market research firm IBISWorld. "Anyone with a computer and access to records can start a business," complained the National Consumer Law Center in the 2019 release of a report asking for more oversight over the industry.

The men also allege that Public Data is the outer surface of a succession of shell companies designed by Bruce Stringfellow of Irving, Texas.

— Public Data —

Stringellow, the man at the heart of Public Data, is no stranger to litigation. Should he convince the Fourth Circuit to uphold Hudson's ruling, it wouldn't be the first time he walks away from a lawsuit seeking Public Data's compliance with the Fair Credit Reporting Act.

His position is that Public Data isn't covered by the statute since the company is not a consumer reporting agency. "Public Data is in compliance with FCRA," he said during a 2013 deposition. "It's not applicable." Stringfellow maintains that Public Data is merely a searchable database of public documents, including criminal records, compiled under contract by another company called ShadowSoft.

Stringellow identifies himself in court documents as the president and owner, with his wife, of ShadowSoft and another company that all share the same Irving, Texas, office address as Public Data. UPS claims the address as store No. 2732. Stringellow's Public Data title is one of "limited partner." He didn't respond to attempts to reach him by email, telephone and text message.

Public Data successfully challenged in appeals court a 2017 civil investigative demand from the Consumer Financial Protection Bureau looking for evidence that the company violated the Fair Credit Reporting Act. The company was a co-defendant in two Florida lawsuits against Waffle House that ended in settlements after alleging consumer reporting violations. Public Data settled or defeated similar lawsuits in filed in Virginia and Texas.

In the 2013 deposition, Stringfellow estimated Public Data returns at least 50 million results annually regarding individuals. He also said Public Data was incorporated during the 1990s in the Caribbean island of Anguilla in a bid to avoid compliance with another federal statute, the Driver's Privacy Protection Act. The 1994 law limits the disclosure of driver's license data.

— The Hudson opinion —

In dismissing Henderson's putative class action, Hudson relied on arguments that Public Data isn't the origin of the data contained in its servers.

Correctly attributing authorship of the content appearing on websites is key to unlocking the protections of Section 230. Hosts of user-generated content such as social media platforms, cloud computing providers and search engines use the legal shield when faced with litigants who say these digital intermediaries are responsible for what their users post, create or do.

Section 230 is responsible in large measure for the shape of today's Internet. Without it, there would be no Google, Amazon or Facebook — at least not in their current, world-shaking configurations.

Mounting levels of criticism against Section 230 focus on the downside of intermediary liability protection: filter bubbles, algorithmically amplified disinformation and the fraying of laws meant to guarantee equal access to housing, employment or credit (see here). Under a legal system in which online platforms can divert liability for discrimination to third parties, advocates already worry that civil rights enforcement is taking a step backwards.

Hudson's ruling supercharges those worries. Section 230 says online intermediaries can't legally be treated as the publisher or speaker of information "provided by another information content provider."

For Hudson, that was enough to dismiss the lawsuit against Public Data. Stringfellow's companies "upload the information onto their servers for their clients to access on the Internet," he wrote. The information originates with state governmental agencies and courthouses, so Public Data isn't the author.

The ruling overlooks the role that Stringfellow's companies play in obtaining and displaying public records, say critics. Records don't appear on Public Data passively the way a users' tweet does on Twitter. Public Data must actively obtain them by exercising agency, whether by itself or through ShadowSoft.

Public Data isn't an intermediary for user-generated content, argued plaintiffs' attorney Leonard Bennett during January oral argument in Hudson's Eastern District of Virginia courtroom. The company is metaphorically "going into a mine, it is finding different metals, it is taking it to its factory and assembles it into a database," Bennett said.

The implications from Hudson's reasoning are potentially immense, and that's what's gotten the attention of regulators and civil rights organizations.

Letting it stand could undermine the Fair Credit Reporting Act by allowing consumer reporting agencies to claim a Section 230 defense. They, too, rely on data generated by a third party.

Hence an amicus brief from the Federal Trade Commission, the Consumer Financial Protection Bureau and the North Carolina attorney general arguing to the Fourth Circuit that "Public Data is wholly responsible 'for the creation' of its reports — they would not exist if Public Data did not affirmatively undertake to gather information from public sources and compile that information into reports" (see here). A group of 20 states led by Texas filed a similar brief (see here).

Then there's the broader impacts to anti-discrimination laws, warned the Lawyer's Committee for Civil Rights Under Law and the National Fair Housing Alliance. Hudson's original authorship analysis would permit a business owner to copy and paste a racist manifesto written by someone else without incurring liability for breaching public accommodations law, the organization wrote in a brief.

— Fourth Circuit runs deep with Section 230 —

This case isn't the first Section 230 lawsuit before the Fourth Circuit to have vast potential for shaping the online world.

It was the Fourth Circuit in 1997 that published the defining legal interpretation of Section 230 in the decision of Kenneth Zeran versus America Online.

Zeran was victim of online harassment on AOL that falsely advertised him as selling T-shirts making light of the 1995 bombing of the Alfred P. Murrah Federal Building in Oklahoma City. The hate calls and death threats came into his Seattle home at a rate of approximately one every two minutes. Local police had to protect his safety. Zeran argued AOL had a duty to remove the defamatory speech. A three-judge panel decided imposing onto online services tort liability for users' speech would have chilling effects.

"It would be impossible for service providers to screen each of their millions of postings for possible problems," wrote Judge Harvie Wilkinson.

We live in the world the Zeran ruling created. Now the Fourth Circuit must decide whether we should also live in the world that Public Data wants.

*Please email editors@mlex.com to contact the editorial staff regarding this story, or to submit the names of lawyers and advisers.*

**Related Portfolio(s):**
Regulation - Henderson, Sr. et al - Fair Credit Reporting Act (US)

**Areas of Interest:** Data Privacy & Security, Sector Regulation

**Industries:** Communication Services, Information Technology, Interactive Media & Services, Media, Media & Entertainment, Software and Services

**Geographies:** North America, United States

**Topics:**

Data Privacy | Section 230