United States Court of Appeals

FOR THE DISTRICT OF COLUMBIA CIRCUIT

Argued September 12, 2022 Decided December 6, 2022

No. 21-5195

MATTHEW D. GREEN, ET AL.,
APPELLANTS

v.

UNITED STATES DEPARTMENT OF JUSTICE, ET AL.,
APPELLEES

Appeal from the United States District Court
for the District of Columbia
(No. 1:16-cv-01492)

Corynne McSherry argued the cause for appellants. With her on the briefs were *Kit Walsh*, *Brian M. Willen*, and *Lauren Gallo White*.

Rebecca Tushnet and *Catherine Crump* were on the brief for *amici curiae* Copyright Scholars Pamela Samuelson and Rebecca Tushnet in support of appellants.

Jack I. Lerner was on the brief for *amici curiae* Kartemquin Educational Films and International Documentary Association in support of appellants.

Jonathan Skinner-Thompson was on the brief for *amicus curiae* Accessibility, Security, and Repair Fair Users in support of appellants.

Daniel Tenny, Attorney, U.S. Department of Justice, argued the cause for appellees. With him on the brief were *Brian M. Boynton*, Principal Deputy Assistant Attorney General, and *Scott R. McIntosh*, Attorney. *Sonia M. Carson* and *Adam C. Jed*, Attorneys, entered appearances.

Eleanor M. Lackman and *John Matthew DeWeese Williams* were on the brief for *amici curiae* Association of American Publishers, Inc. et al. in support of appellees.

David Jonathan Taylor was on the brief for *amici curiae* DVD Copy Control Association, Inc. et al. in support of appellees.

Before: WALKER, *Circuit Judge*, and ROGERS and TATEL, *Senior Circuit Judges*.

Opinion for the Court filed by *Senior Circuit Judge* TATEL.

TATEL, *Senior Circuit Judge*: In this digital age, when content creators choose to make their copyrighted materials—like books, movies, and music—available online, they employ computer code to block unauthorized access, copying, and use. To fortify the protection offered by that code, Congress enacted the Digital Millennium Copyright Act, which makes it unlawful to bypass such technological measures. The question in this case, which comes to us at the preliminary injunction stage, is whether the statute is likely to violate the First Amendment rights of two individuals who write computer code designed to circumvent those measures. The district court answered no, and we agree.

I.

In the 1990s, a growing number of digital tools facilitated "massive piracy" by increasing "the ease with which digital works [could] be copied and distributed worldwide virtually instantaneously." S. Rep. No. 105-190, at 8 (1996). Congress feared that "copyright owners [would] hesitate to make their works readily available on the Internet without reasonable assurances that they [would] be protected." *Id.* In order to provide that protection and adapt copyright law to the digital age, Congress enacted the Digital Millennium Copyright Act (DMCA), 17 U.S.C. §§ 1201 et seq., which "backed with legal sanctions the efforts of copyright owners to protect their works from piracy behind digital walls such as encryption codes or password protections." *Universal City Studios, Inc. v. Corley*, 273 F.3d 429, 435 (2d Cir. 2001).

The DMCA accomplishes its goal through two principal provisions. First, the statute's anticircumvention provision prohibits "circumvent[ing] a technological measure that effectively controls access to a [copyrighted work]." 17 U.S.C. § 1201(a)(1)(A). A "technological measure," also called a "technological protection measure," effectively controls access to a work if it, "in the ordinary course of its operation, requires the application of information, or a process or a treatment, with the authority of the copyright owner, to gain access to the work." *Id.* § 1201(a)(3)(B). For example, Netflix requires a password to access its digital movie catalog, and electronic books contain code that prevents readers from copying the book into another format. Circumvention occurs when someone descrambles a scrambled work, decrypts an encrypted work, or otherwise avoids, bypasses, removes, deactivates, or impairs a technological measure, without authority from the copyright owner. *Id.* § 1201(a)(3)(A). The statute's second principal provision—the antitrafficking provision—works together with the anticircumvention provision to target the technological tools that facilitate circumvention. It prohibits "manufacturing, importing, offering to the public, providing, or otherwise trafficking in any technology, product, service, device, component, or part thereof" if it (1) "is primarily designed or produced for the purpose of circumventing a technological measure that effectively controls access to a [copyrighted] work;" (2) "has only limited commercially significant purpose or use other than to circumvent;" or (3) "is marketed . . . for use in circumventing." *Id.* §§ 1201(a)(2)(A)–(C) (cleaned up). Those who violate either the anticircumvention or antitrafficking provision are subject to civil actions and criminal sanctions. *Id.* § 1203(a).

In order to ensure that the DMCA does not interfere with the fair use of copyrighted digital content, Congress included a "'fail-safe' mechanism." H.R. Rep. No. 105-551 (Part 2), at 36 (1998). Every three years "the Librarian of Congress, upon the recommendation of the Register of Copyrights," determines in a rulemaking proceeding "whether persons who are users of a copyrighted work are, or are likely to be in the succeeding 3-year period, adversely affected by [the anticircumvention provision]." 17 U.S.C. § 1201(a)(1)(C). If so, the statute instructs the Librarian to grant an exemption for such uses for a three-year period. *Id.* § 1201(a)(1)(D).

The Register also monitors "changes to the copyright system spurred by digital technologies" and their impact on the DMCA. U.S. Copyright Office, *Section 1201 of Title 17* i (2017). In 2017, in order to address "deep and widespread debate among copyright stakeholders" regarding the continued value of the statute, the Register conducted a "comprehensive public study on the operation of section 1201." *Id.* at ii–iii. Emphasizing that "digital [content] marketplace[s] . . . succeed only if copyright owners have the legal right to prohibit persons from evading electronic paywalls or other technical measures," the Register declined to recommend "broad changes" to the DMCA. *Id.* at 44, 152. "[T]he statute's overall structure and scope," it concluded, "remain sound." *Id.* at iii.

Plaintiff Matthew Green, a security researcher and computer science professor at Johns Hopkins University, wants to publish an academic book "to instruct readers in the methods of security research," which will include "examples of code capable of bypassing security measures." Green Decl. ¶ 20. He is concerned that including "instructions in both English and in software code" for "circumvent[ing] technological protection measures" would likely violate the DMCA. *Id.* ¶¶ 20–21. Plaintiff Andrew "bunnie" Huang, an inventor and electrical engineer, wants to create and sell a device called "NeTVCR." Huang Decl. ¶ 12. His device contains computer code capable of circumventing High-Bandwidth Digital Content Protection, a technological protection measure that prevents digital content from being copied or played on unauthorized devices. *Id.* ¶¶ 4–6, 12. He also intends to publish that computer code to "communicate to others how the technology works and encourage them to discuss edits to improve the code." *Id.* ¶ 16. Huang fears that distribution of the code contained in his NeTVCR device "could [risk] prosecut[ion] under Section 1201(a)(1) or (a)(2)." *Id.* ¶ 11.

Claiming that the code they write qualifies as speech protected by the First Amendment, Green and Huang brought a pre-enforcement action challenging the DMCA on facial and as-applied First Amendment grounds. The government moved to dismiss all claims, and the district court partially granted the motion. Concluding that Green and Huang failed to allege "facts sufficient to state a claim that DMCA provisions are unconstitutionally overbroad because they 'have failed to identify any significant difference'" between their facial and

DOCKET ALARM

Explore Litigation Insights

Docket Alarm provides insights to develop a more informed litigation strategy and the peace of mind of knowing you're on top of things.

Real-Time Litigation Alerts

Keep your litigation team up-to-date with **real-time alerts** and advanced team management tools built for the enterprise, all while greatly reducing PACER spend.

Our comprehensive service means we can handle Federal, State, and Administrative courts across the country.

Advanced Docket Research

With over 230 million records, Docket Alarm's cloud-native docket research platform finds what other services can't. Coverage includes Federal, State, plus PTAB, TTAB, ITC and NLRB decisions, all in one place.

Identify arguments that have been successful in the past with full text, pinpoint searching. Link to case law cited within any court document via Fastcase.

Analytics At Your Fingertips

Learn what happened the last time a particular judge, opposing counsel or company faced cases similar to yours.

Advanced out-of-the-box PTAB and TTAB analytics are always at your fingertips.

API

Docket Alarm offers a powerful API (application programming interface) to developers that want to integrate case filings into their apps.

LAW FIRMS

Build custom dashboards for your attorneys and clients with live data direct from the court.

Automate many repetitive legal tasks like conflict checks, document management, and marketing.

FINANCIAL INSTITUTIONS

Litigation and bankruptcy checks for companies and debtors.

E-DISCOVERY AND LEGAL VENDORS

Sync your system to PACER to automate legal marketing.

WHAT WILL YOU BUILD? | **sales@docketalarm.com** | **1-866-77-FASTCASE**

fastcase®
Smarter legal research.