

12-1-2022

HACKING COPYRIGHT: HOLDING COPS ACCOUNTABLE FOR ABUSING YOUTUBE'S COPYRIGHT FILTER SYSTEM

Tyler Bloom

Follow this and additional works at: <https://brooklynworks.brooklaw.edu/jlp>



Part of the [First Amendment Commons](#), [Internet Law Commons](#), [Legislation Commons](#), and the [Science and Technology Law Commons](#)

Recommended Citation

Tyler Bloom, *HACKING COPYRIGHT: HOLDING COPS ACCOUNTABLE FOR ABUSING YOUTUBE'S COPYRIGHT FILTER SYSTEM*, 31 J. L. & Pol'y 55 (2023).

Available at: <https://brooklynworks.brooklaw.edu/jlp/vol31/iss1/2>

This Note is brought to you for free and open access by the Law Journals at BrooklynWorks. It has been accepted for inclusion in Journal of Law and Policy by an authorized editor of BrooklynWorks.

HACKING COPYRIGHT: HOLDING COPS ACCOUNTABLE FOR ABUSING YOUTUBE'S COPYRIGHT FILTER SYSTEM

*Tyler Bloom**

The forces and directions of the Internet are so new,
so protean, and so far reaching that courts must be
conscious that what they say today might be obsolete
tomorrow.¹

Inside we both know what's been going on
We know the game and we're gonna play it
And if you ask me how I'm feeling
Don't tell me you're too blind to see.²

*This Note both explores the mechanisms and incentive structures
that make “copyright hacking” possible and explains the legal
system’s failure to provide recourse for victims of successful
“copyright hacks” by police officers. Because the DMCA has
failed to keep pace with the internet’s exponential growth, OSPs,
such as YouTube, have developed filtering systems that can be*

* J.D. Candidate, Brooklyn Law School, 2023. B.A., University of Pennsylvania, 2018. I would like to thank my family and friends, who watched me disappear during the months-long writing process and welcomed me back into society with open arms. I am incredibly grateful to the members of the Journal of Law and Policy staff and executive board for all that they did to make my Note publishable. I also owe a huge shoutout to Dexter Thomas (@dexdigi) of Vice News – for reporting on “copyright hacking” and for being a foundational resource during the research process. I dedicate this Note to those who record and post without fear or favor.

¹ Packingham v. North Carolina, 137 S. Ct. 1730, 1736 (2017).

² RICK ASTLEY, *Never Gonna Give You Up*, on WHENEVER YOU NEED SOMEBODY (RCA Recs. 1987), <https://www.youtube.com/watch?v=dQw4w9WgXcQ>.

exploited to “copyright hack” users and ultimately suppress their speech. A victim of “copyright hacking” by a police officer currently has no recourse; the doctrine of qualified immunity functionally precludes them from suing for violating their First Amendment rights. This Note proposes two possible solutions to “copyright hacking.” First, the Copyright Office should require that OSPs register their proprietary copyright filtering systems to ensure that they comply with the standards of fair use. Second, the Supreme Court should hold that recording public police activity is protected speech under the First Amendment; by doing so, plaintiffs who are “copyright hacked” would avoid having their claims dismissed due to a defendant officer’s use of qualified immunity.

INTRODUCTION

On February 5th, 2021, Sennett Devermont, a Los Angeles activist with more than 300,000 Instagram followers, entered an office of the Beverly Hills Police Department to file a form to obtain body camera footage from a prior incident.³ After realizing that Devermont was livestreaming their interaction with his phone, the officer to whom he was speaking took out his phone and began playing “Santeria” by Sublime. He ignored Devermont’s requests to turn the music off.⁴ Though it may seem bizarre, this same interaction had happened before: while speaking to the “Santeria” officer on a city sidewalk a few weeks earlier, a different officer took his phone out and played “Yesterday” by The Beatles while Devermont was livestreaming.⁵

³ Dexter Thomas, *Is This Beverly Hills Cop Playing Sublime’s ‘Santeria’ to Avoid Being Live-Streamed?*, VICE NEWS (Feb. 9, 2021, 1:49 PM), <https://www.vice.com/en/article/bvxb94/is-this-beverly-hills-cop-playing-sublimes-santeria-to-avoid-being-livestreamed> [https://perma.cc/E65D-HC6E].

⁴ *Id.*

⁵ Dexter Thomas, *New Video Shows Beverly Hills Cops Playing Beatles to Trigger Instagram Copyright Filter*, VICE NEWS (Feb. 11, 2021, 9:34 PM), <https://www.vice.com/en/article/bvxa7q/new-video-shows-beverly-hills-cops-playing-beatles-to-trigger-instagram-copyright-filter> [https://perma.cc/GRE5-AQEC].

On February 25th, 2021, in Ottawa, Illinois, YouTuber “Accountability Angel” tried to record herself filing a complaint at the LaSalle County Sheriffs’ Office.⁶ Although Angel insisted that she had previously been allowed to film, a member of the staff told her that she was not allowed to bring her phone into the building.⁷ A man with a court security badge then started playing “Nobody But You” by Blake Shelton.⁸ As Angel explained why she was there, the man held up the speaker to mask Angel’s voice.⁹ Finally, Angel caught on, telling the audience of her livestream “Oh, guys, you know what they’re doing! They’re trying to get me kicked off of YouTube for the copyright thing!”¹⁰ After an extended standoff, Angel left the office without being able to file her complaint.¹¹ In an incident report obtained by *Vice News*, the court security officer explained that he had been recently been advised to play music in those situations.¹²

On July 1st, 2021, outside of a courthouse in Oakland, California, a sergeant with the Alameda County Sheriff’s Office asked a member of the Anti Police-Terror Project, a group that was demonstrating outside the hearing of a former police officer, to move a banner.¹³ Upon noticing that another group member was filming their interaction, the sergeant used his phone to play “Blank

⁶ Dexter Thomas, *It Sure Looks Like This Cop Played Country Music to Avoid Being Filmed*, VICE NEWS (Mar. 2, 2021, 3:31 PM), <https://www.vice.com/en/article/wx89kn/it-sure-looks-like-this-cop-played-country-music-to-avoid-being-filmed> [<https://perma.cc/A7CW-VE9C>].

⁷ *Id.*

⁸ *Id.*

⁹ *Id.*

¹⁰ Accountability Angel, *TYRANTS at the sheriffs office. Complete abuse of power!!!! Impeding the complaint process!!*, YOUTUBE (Feb. 25, 2021), <https://youtu.be/pSteGkNO-ZE> [<https://perma.cc/B8KD-XVZA>].

¹¹ *Id.*

¹² Matthew Gault, *Cop Was Instructed to Use Music to Disrupt Filming*, VICE NEWS (Sept. 9, 2021, 9:39 AM), <https://www.vice.com/en/article/93y77y/cop-was-instructed-to-use-music-to-disrupt-filming> [<https://perma.cc/9KQM-568Y>].

¹³ Emma Ockerman, *Watch Sheriff’s Sergeant Play Taylor Swift to Avoid Ending Up on YouTube*, VICE NEWS (July 1, 2021, 4:15 PM), <https://www.vice.com/en/article/dyv48q/watch-this-sheriffs-sergeant-play-taylor-swift-to-avoid-ending-up-on-youtube> [<https://perma.cc/5BEQ-CQZF>].

Space” by Taylor Swift.¹⁴ Confused, the group member questioned him:

MEMBER 1: I don’t know why we’re – are we having a dance party now?

SERGEANT: No, sir.

MEMBER 2 (off-camera): Did you – are you playing pop music to drown out the conversation?

SERGEANT: No.

MEMBER 1: He doesn’t want you recording so he’s playing music in the back.

MEMBER 2: Why? What do you have to hide?

SERGEANT: You can record all you want – I just know it can’t be posted to YouTube.

MEMBER 1 (pointing to the Sergeant’s phone): This is the new – this is the new hotness right here, is that the recording *inaudible* so they can get a copyright strike –

MEMBER 2: I don’t understand – if it’s completely legal, why would you worry about it being recorded?

MEMBER 3 (off-camera): You’d only do that if you knew you were being an asshole, dude.¹⁵

The back-and-forth between the officer and the protestors continued.¹⁶ When asked whether playing music was routine procedure at the Alameda County Sheriff’s office, the sergeant stated that it was “not specifically outlined.”¹⁷ Unlike the earlier incidents, the sergeant was very clear about his motives; he said, directly to the camera, “I’m playing my music so that you can’t post on YouTube.”¹⁸

¹⁴ *Id.*

¹⁵ Anti Police-Terror Project, *Cop Plays Taylor Swift to Prevent Video Sharing of Him Harassing Protesters*, YOUTUBE (July 1, 2021), <https://youtu.be/cmZmo81Cdcc> [<https://perma.cc/TQM4-5WHY>].

¹⁶ *Id.*

¹⁷ *Id.*

¹⁸ *Id.*; see also Samantha Cole, ‘WHYYYYYYY?’: Police Upset Idiot Colleague Played Taylor Swift to Trigger YouTube Filter, VICE NEWS (Aug. 10, 2021, 9:00 AM), <https://www.vice.com/en/article/4avp4m/alameda-county-police-department-taylor-swift-filming-youtube> [<https://perma.cc/293S-QD99>] (reporting on the frustration felt by the Alameda County Sheriff’s Department due

The incidents above illustrate a tactic that *Vice News* Reporter Dexter Thomas described as “copyright hacking.”¹⁹ “Copyright hacking” incidents follow the same basic pattern: a bystander, usually an activist, films a police officer performing run-of-the-mill tasks, while the officer plays a copyrighted piece of music in response to being filmed. If the bystander is livestreaming during the interaction or later uploads the footage, the copyrighted material might trigger the social media platform’s copyright filtering system, which removes or mutes the bystander’s video.

All of the “copyright hacking” incidents outlined above also had the same basic outcome: they completely backfired. Instead of those videos being removed from the internet,²⁰ the involved officers received negative media attention while the videos remained online.²¹ At the time of this writing, videos of the above incidents

to the negative media attention from the sergeant’s actions and including an email from a sergeant telling other sheriffs “[l]ets not be YouTube famous or even worse Media Famous”).

¹⁹ Thomas, *supra* note 3.

²⁰ This Note will use lowercase when referring to the internet. This choice is intentional and reflects both the consensus approach by major media organizations. See, e.g., Kristen Hare, *AP Style Alert: Don’t Capitalize internet and web Anymore*, POYNTER (Apr. 2, 2016), <https://www.poynter.org/educators-students/2016/ap-style-change-alert-dont-capitalize-internet-and-web-any-more/> [<https://perma.cc/PS3Z-CZ7K>] (discussing the AP’s announcement that the news agency would no longer capitalize the word internet). My personal belief is that the term “the internet” does not refer to a specific place, but rather to a generic infrastructure. For a more in-depth discussion about how individual Supreme Court Justices have approached this stylistic choice, see Charles Duan, *‘Internet’ or ‘internet’? The Supreme Court Weighs in*, VICE (June 22, 2017, 9:00 AM), <https://www.vice.com/en/article/pay5ek/internet-or-internet-the-supreme-court-weighs-in> [<https://perma.cc/K8C8-KE28>].

²¹ See, e.g., Julian Mark, *An Officer Played a Taylor Swift Song to Keep His Recording Off YouTube. Instead It Went Viral.*, WASH. POST (July 2, 2021, 7:40 AM), <https://www.washingtonpost.com/nation/2021/07/02/taylor-swift-california-cop/> [<https://perma.cc/5GWD-PSFY>].

are still available to view on Instagram²² and YouTube.²³ Although the most public examples of “copyright hacking” have been unsuccessful, it is impossible to know how many videos have fallen prey to this tactic due to the sheer volume of content uploaded to²⁴ and removed from²⁵ social media platforms every day. Even so, the fact that police officers around the country believe that they can use copyright as a sword to silence the exercise of free speech is alarming and deserves attention. This belief also represents a

²² Sennett Devermont (@mrcheckpoint_), INSTAGRAM (Feb. 6, 2021) <https://www.instagram.com/tv/CK9s6LUDmQd>; Sennett Devermont (@mrcheckpoint_), INSTAGRAM (Feb. 11, 2021) <https://www.instagram.com/p/CLKaLPiDwz2>.

²³ Accountability Angel, *supra* note 10; Anti Police-Terror Project, *supra* note 15; *see also* Santa Ana Audits, *Council Member arrives to an immature seasoned Corporal Officer badge#3134 #knowyourrights #1aaudits*, YOUTUBE (Apr. 5, 2022), <https://www.youtube.com/watch?v=9f-z-5HZr6w> [<https://perma.cc/3K4Q-5XR9>]; Nathan Solis, *Santa Ana Police Officers Who Blasted Disney Songs to Thwart Video Recording Are Under Investigation*, L.A. TIMES (Apr. 15, 2022), <https://www.latimes.com/california/story/2022-04-15/police-blast-disney-songs-in-attempt-to-prevent-resident-from-filming-them> [<https://perma.cc/D6LX-67X5>] (describing a recent incident posted to YouTube in which a police officer used his patrol car’s loudspeaker to blast copyrighted Disney songs, and in doing so, accidentally woke the entire neighborhood. When Santa Ana Councilmember Johnathan Ryan Hernandez asked the officer why he was playing the music, the officer “admitted he was playing music from his phone through his cruiser’s PA system, citing copyright infringement.”).

²⁴ *See, e.g.,* Susan Wojcicki, *YouTube at 15: My Personal Journey and the Road Ahead*, YOUTUBE OFFICIAL BLOG (Feb. 14, 2020), <https://blog.youtube/news-and-events/youtube-at-15-my-personal-journey/> [<https://perma.cc/4P43-BNUM>] (“500 hours of video [are] uploaded [to YouTube] every minute.”).

²⁵ *See* GOOGLE, *How Google Fights Piracy*, 30 (Nov. 2018), https://www.blog.google/documents/25/GO806_Google_FightsPiracy_eReader_final.pdf [<https://perma.cc/UQX8-JYLP>] (“In 2017, YouTube received over 2.5 million DMCA takedown requests from over 300,000 copyright claimants, requesting the removal of more than [seven] million video URLs. While the vast majority of the time we remove this content, we also find a large number of requests represent a misunderstanding of the process or sometimes even outright abuse. YouTube carefully reviewed these takedown requests and either asked for more information or rejected requests targeting more than 300,000 of those videos”).

fundamental misunderstanding among Americans of what copyright is and how platforms can enforce it.²⁶

The issue of “copyright hacking” underscores the tension between two provisions of the Constitution: the First Amendment right to free speech²⁷ and Congress’s enumerated power “[t]o promote the Progress of Science . . . by securing for limited Times, to Authors . . . the exclusive Right to their respective Writings.”²⁸ This conflict came to a head most recently in 2003, when the Supreme Court held in *Eldred v. Ashcroft* that the extension of present and future copyrights did not violate the First Amendment because copyright law already accommodates First Amendment issues.²⁹ The Court pointed to the statutory provisions distinguishing

²⁶ See JESSICA LITMAN, DIGITAL COPYRIGHT 169 (Mich. Publ’g, 2017) (predicting that, following the 1998 passage of the Digital Millennium Copyright Act, “most people will continue to ignore [copyright] law written in barely comprehensible prose that makes no sense whatsoever from their point of view . . . [because] even the most cynical of them will continue to believe that Congress intended the law to make sense, and continue about their business”). See generally Jessica Litman, *Real Copyright Reform*, 96 IOWA L. REV. 1, 33 (2010) (“The copyright law is long, complex, counterintuitive and packed with traps and pitfalls, some of which were inserted intentionally to trip unwary new entrants, hapless authors, or pesky potential competitors. . . . [T]he fact that legacy copyright rules bind ordinary people engaging in everyday transactions, but are too complicated to explain to them, is nothing for us to be proud of”).

²⁷ U.S. CONST. amend. I, cl. 2.

²⁸ U.S. CONST. art. I, § 8, cl. 8.

²⁹ See *Eldred v. Ashcroft*, 537 U.S. 186, 219 (2003); see also *Harper & Row Publishers, Inc. v. Nation Enters.*, 471 U.S. 539, 556 (1985) (“[C]opyright’s idea/expression dichotomy strike[s] a definitional balance between the First Amendment and the Copyright Act by permitting free communication of facts while still protecting an author’s expression.”) (quotations omitted) (citation omitted); see *Eldred*, 537 U.S. at 244 (Breyer, J., dissenting) (“The Copyright Clause and the First Amendment seek related objectives—the creation and dissemination of information. When working in tandem, these provisions mutually reinforce each other, the first serving as an engine of free expression, the second assuring that government throws up no obstacle to its dissemination. At the same time, a particular statute that exceeds proper Copyright Clause bounds may set Clause and Amendment at cross-purposes, thereby depriving the public of the speech-related benefits that the Founders, through both, have promised”) (quotations omitted) (citation omitted).

the eligibility of ideas from expression for copyright protection³⁰ and establishing the “fair use” defense which can be invoked by alleged infringers.³¹ In the twenty years since this decision, however, the internet has evolved into arguably the most important piece of infrastructure in American society. The internet drives our economy,³² keeps us informed,³³ and makes our lives easier.³⁴ Today’s internet is virtually unrecognizable from the internet that the *Eldred* Court contemplated.³⁵

³⁰ See 17 U.S.C. § 102(b) (“In no case does copyright protection for an original work of authorship extend to any idea . . . regardless of the form in which it is described, explained, illustrated, or embodied in such work”).

³¹ See 17 U.S.C. § 107 (“[T]he fair use of a copyrighted work . . . for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright”); see also *Campbell v. Acuff–Rose Music, Inc.*, 510 U.S. 569 (1994) (holding that a rap group’s parody of Roy Orbison’s “Oh, Pretty Woman” may have been a fair use after applying the four-factor test to determine whether the use of a work is fair).

³² See, e.g., Ruth Igielnik, *As Telework Continues for Many U.S. Workers, No Sign of Widespread ‘Zoom Fatigue’*, PEW RSCH. CTR. (May 4, 2022), <https://www.pewresearch.org/fact-tank/2022/05/04/as-telework-continues-for-many-u-s-workers-no-sign-of-widespread-zoom-fatigue/> [<https://perma.cc/H9TF-6EKU>].

³³ See, e.g., Elisa Shearer, *More Than Eight-in-Ten Americans Get News From Digital Devices*, PEW RSCH. CTR. (Jan. 12, 2021), <https://www.pewresearch.org/fact-tank/2021/01/12/more-than-eight-in-ten-americans-get-news-from-digital-devices/> [<https://perma.cc/NP7Z-SVEU>].

³⁴ See, e.g., Monica Anderson, *Payment Apps Like Venmo and Cash App Bring Convenience – and Security Concerns – to Some Users*, PEW RSCH. CTR. (Sept. 8, 2022), <https://www.pewresearch.org/fact-tank/2022/09/08/payment-apps-like-venmo-and-cash-app-bring-convenience-and-security-concerns-to-some-users/> [<https://perma.cc/4PQ6-BKEQ>] (“Roughly six-in-ten Americans who have ever used PayPal, Venmo, Zelle or Cash App (61%) say a major reason for doing so is because it makes paying for things easier”).

³⁵ To illustrate this point, in 2003, Netflix’s subscription DVD rental service had just surpassed one million members. See Press Release, Netflix Announces First Quarter 2003 Ending Subscribers of 1,052,000, Up 74% Over the Prior Year, NETFLIX INVS. (Apr. 1, 2003), <https://ir.netflix.net/investor-news-and-events/financial-releases/press-release-details/2003/Netflix-Announces-First-Quarter-2003-Ending-Subscribers-of-1052000-Up-74-Over-The-Prior-Year/default.aspx> [<https://perma.cc/2CX5-HNZ4>]. Netflix would not introduce an internet streaming option until 2007. See Ashley Rodriguez, *Ten Years Ago, Netflix Launched Streaming Video and Changed the Way We Watch Everything*,

Perhaps the clearest example of the internet's explosive growth and entanglement with everyday life is the story of YouTube. YouTube was founded in 2005, two years after the *Eldred* decision; just a year later, Google bought it for \$1.65 billion.³⁶ At the time of this acquisition, and less than a year after its public launch, 57% of adult internet users said that they watched online video; of those viewers, 27% used YouTube.³⁷ Today, 81% of *all* Americans use YouTube.³⁸ In 2012, smartphones became the most commonly owned mobile communication device among Americans.³⁹ Just four

QUARTZ (July 20, 2022), <https://qz.com/887010/netflix-nflx-launched-streaming-video-10-years-ago-and-changed-the-way-we-watch-everything/> [https://perma.cc/3G6T-ZCBY]. At the end of 2019, Netflix had approximately two million DVD rental subscribers, who accounted for about 1.2% of the company's 167.09 million paid subscribers. See Julia Stoll, *Number of Netflix Paying DVD Subscribers in the United States From 3rd Quarter 2011 to 4th Quarter 2019*, STATISTA (Jan. 13, 2021), <https://www.statista.com/statistics/250940/quarterly-number-of-netflix-dvd-subscribers-in-the-us/> [https://perma.cc/BU9L-UEKF]; Julia Stoll, *Number of Netflix Paid Subscribers Worldwide from 1st Quarter 2013 to 2nd Quarter 2022*, STATISTA (Aug. 26, 2022), <https://www.statista.com/statistics/250934/quarterly-number-of-netflix-streaming-subscribers-worldwide/> [https://perma.cc/65ZF-LGH9]. Internet streaming has become so popular that at the outset of the COVID-19 pandemic, Netflix and YouTube, along with other video service providers, voluntarily reduced the quality of their video streams in Europe in an effort to mitigate the strain being placed on the continent's broadband networks. See Julia Alexander, *Amazon and Apple Are Reducing Streaming Quality to Lessen Broadband Strain in Europe*, THE VERGE (Mar. 20, 2020, 8:39 PM), <https://www.theverge.com/2020/3/20/21188072/amazon-prime-video-reduce-stream-quality-broadband-netflix-youtube-coronavirus> [https://perma.cc/XCJ9-8NWF].

³⁶ See Andrew Ross Sorkin & Jeremy W. Peters, *Google to Acquire YouTube for \$1.65 Billion*, N.Y. TIMES (Oct. 9, 2006), <https://www.nytimes.com/2006/10/09/business/09cnd-deal.html> [https://perma.cc/84E8-8R2B].

³⁷ Mary Madden, *The Audience for Online Video*, PEW RSCH. CTR. (July 25, 2007), <https://www.pewresearch.org/internet/2007/07/25/the-audience-for-online-video/> [https://perma.cc/JX97-64AJ].

³⁸ Brooke Auxier & Monica Anderson, *Social Media Use in 2021*, PEW RSCH. CTR. (Apr. 7, 2021), <https://www.pewresearch.org/internet/2021/04/07/social-media-use-in-2021/> [https://perma.cc/977C-LTUV].

³⁹ See Reuben Fischer-Baum, *What 'Tech World' Did You Grow Up In?*, WASH. POST (Nov. 26, 2017),

years later, in 2016, 75% of Americans owned a smartphone capable of recording and uploading user-created video to social media platforms.⁴⁰

With nearly three-fourths of Americans owning smartphones capable of recording, distributing, and viewing video as soon as it is recorded, every moment has the potential to go viral.⁴¹ Some actors, like the police officers described above, have recognized the ramifications of this power, and, in turn, have tried using “copyright hacking” as an extrajudicial tool to stymie the dissemination of these videos over the internet. This Note seeks both to demystify the mechanisms and incentive structures that make “copyright hacking” possible and to explain the legal system’s failure to provide recourse for victims of successful “copyright hacks” by police officers. Because there is a dearth of litigation in this area, much of this Note’s analysis is theoretical and requires an understanding of the “why” and “how” of the copyright law. Part I of this Note surveys the modern era of copyright legislation in the United States and the Digital Millennium Copyright Act (“DMCA”), the congressional response to the birth of the internet. Part II discusses how the DMCA has failed to keep pace with the internet’s exponential growth, leading to the rise of filtering systems that can be exploited to “copyright hack” users of online platforms and ultimately suppress

<https://www.washingtonpost.com/graphics/2017/entertainment/tech-generations/> [<https://perma.cc/75QH-33N9>].

⁴⁰ *Id.*

⁴¹ See, e.g., Joe Hernandez, *Darnella Frazier, Who Filmed George Floyd’s Murder, Wins An Honorary Pulitzer*, NPR (June 11, 2021, 4:05 PM), <https://www.npr.org/2021/06/11/1005601724/darnella-frazier-teen-who-filmed-george-floyds-murder-wins-pulitzer-prize-citati> [<https://perma.cc/JX7D-HUC8>] (stating that the video of George Floyd’s murder recorded by a seventeen year old bystander “played a major role in igniting a global protest movement against police violence, and was used as evidence in the trial of Floyd’s killer.”); Joshua Fechter & Reese Oxner, *Authorities Took an Hour to Stop Uvalde Gunman, Raising Questions About Law Enforcement Response*, TEX. TRIB. (May 26, 2022), <https://www.texastribune.org/2022/05/26/uvalde-school-shooting-police-response/> [<https://perma.cc/8GYN-QLWS>] (noting that despite initial praise of law enforcement’s response to the Robb Elementary School Shooting in Uvalde, Texas, “[v]ideos have circulated on social media showing frustrated parents confronting police officers outside the school while the gunman was inside,” which led to increased scrutiny of their actions during the attack).

their speech. Part III explains how the doctrine of qualified immunity functionally precludes citizens from suing police officers who violate their First Amendment rights through “copyright hacking.” Part IV recommends two possible solutions to the issue of “copyright hacking.”

I. COPYRIGHT AND THE DMCA

The foundation of United States copyright law “is premised on the assumption that we can give authors and their publishers rights to control some ways of exploiting their works, and reserve the rest of the value of the works to the public at large.”⁴² Hence, copyright law grants the creator of an original work broadly-defined exclusive rights⁴³ and copyright protection as soon as the work is “fixed in any tangible medium of expression.”⁴⁴ For instance, the owner of a copyright in a photograph has, among others, the exclusive rights to make and sell copies of the photograph⁴⁵ and to display the photograph publicly.⁴⁶

However, as a matter of public policy, there are several statutory limitations to a copyright owner’s exclusive rights. While the copyright owner in a sound recording can prohibit a buyer from making copies available for rental, he⁴⁷ cannot control the loan, gift, or resale of those copies.⁴⁸ The use of a copyrighted work “for purposes such as criticism, comment, news reporting, teaching, . . . scholarship, or research” is not an infringement of the

⁴² LITMAN, *supra* note 26, at 7.

⁴³ See 17 U.S.C. § 106.

⁴⁴ See *id.* § 102(a); see also U.S. Copyright Office, *What is Copyright?*, <https://www.copyright.gov/what-is-copyright/> [https://perma.cc/GR23-6HXU] (last visited Nov. 28, 2022) (explaining that “[a] work is fixed when it is captured . . . in a sufficiently permanent medium such that the work can be perceived, reproduced, or communicated for more than a short time.”).

⁴⁵ 17 U.S.C. § 106(1), (3).

⁴⁶ *Id.* § 106(5).

⁴⁷ When referring to an individual copyright holder, this Note uses the pronoun “he” for the sake of simplicity.

⁴⁸ See 17 U.S.C. § 109(a)–(b). This limitation is known as the “first-sale doctrine.” See, e.g., *Kirtsaeng v. John Wiley & Sons, Inc.*, 568 U.S. 519, 524 (2013) (“Section 109(a) sets forth the “first sale” doctrine . . .”).

copyright.⁴⁹ In determining whether a use is fair, a court will weigh four factors: “the purpose and character of the use,”⁵⁰ “the nature of the copyrighted work,”⁵¹ the amount of the copyrighted work used,⁵² and “the effect of the use upon the market for . . . the copyrighted work.”⁵³

The statutory framework of copyright law has been meticulously tinkered with for over a century. Historically, Congress has passed copyright legislation by “buil[ding] on a network of negotiated compromises.”⁵⁴ When drafting copyright legislation, Congress and the Copyright Office have returned to the same strategy that produced the first Copyright Act in 1909: “meeting[] and negotiat[ing] among representatives of industries with interests in copyright.”⁵⁵ Stakeholder industries that participate in these negotiations subsequently receive favorable treatment under the new law, while “interests that [are] absent from the bargaining table [are] shortchanged in the compromises that emerge[.]”⁵⁶ Obviously, interests that do not yet exist are also absent from these negotiations.⁵⁷ This problem is a recurring one, as emergent industries such as the broadcast and film industries in the 1920s or internet service providers in the 1980s have struggled to fit into the rigid statutory structure due to the new technologies they

⁴⁹ 17 U.S.C. § 107.

⁵⁰ *Id.* § 107(1).

⁵¹ *Id.* § 107(2).

⁵² *Id.* § 107(3).

⁵³ *Id.* § 107(4).

⁵⁴ LITMAN, *supra* note 26, at 37–38.

⁵⁵ *Id.* at 24.

⁵⁶ See Jessica Litman, *Copyright Legislation and Technological Change*, 68 OR. L. REV. 275, 299 (1989) [hereinafter *Copyright Legislation and Technological Change*]. For instance, Litman notes that “[t]he Librarian of Congress’s conferences in 1905 and 1906 excluded the piano roll and talking machine interests; the [1909 Copyright Act] that emerged disadvantaged them.” *Id.*

⁵⁷ See, e.g., *id.* at 300–01 (“The industries that chafed most under the provisions of the 1909 [Copyright] Act, for example, were the motion picture and broadcast industries: the former barely begun and the latter not yet imagined at the time the Librarian of Congress called his conferences in 1906”).

employed.⁵⁸ As a result, “[c]ourts . . . struggled to apply the 1909 act’s [sic] language to facts that its drafters never envisioned” in the years following the its enactment.⁵⁹

To avoid reliance on a body of case law that assumed that judges would use their “linguistic fortuity” to apply the outmoded copyright statute to new forms of technology,⁶⁰ Congress engaged in a nearly twenty year effort to revise the 1909 Act.⁶¹ This tortured legislative process culminated in the enactment of the 1976 Copyright Act.⁶² Drafters of the 1976 Copyright Act sought to “enlarge[] the copyright pie and divide[] its pieces among conference participants so that no leftovers remained.”⁶³ To achieve this, they granted copyright owners broad, exclusive rights over their works⁶⁴ while carving out narrow exceptions at the insistence of individual stakeholders.⁶⁵ While the broad rights granted to copyright holders have succeeded in adapting to technological change, many of the narrowly-tailored exemptions quickly became

⁵⁸ See LITMAN, *supra* note 26, at 33–35. But see PETER DECHERNEY, *HOLLYWOOD’S COPYRIGHT WARS: FROM EDISON TO THE INTERNET* 44 (Colum. Univ. Press 2013) (discussing theories why “Congress chose not [to] mention film at all in the 1909 Copyright Act”).

⁵⁹ LITMAN, *supra* note 26, at 35; see also DECHERNEY, *supra* note 58, at 45–57 (exploring the outcomes of litigation between the emergent film industry and the established publishing houses as a result of the film industry’s omission from that 1909 Copyright Act).

⁶⁰ LITMAN, *supra* note 26, at 35.

⁶¹ See *Copyright Legislation and Technological Change*, *supra* note 56, at 305–11.

⁶² See *id.* at 311.

⁶³ LITMAN, *supra* note 26, at 40.

⁶⁴ *Id.* at 43 (“The revision bill spelled out five expansively defined exclusive rights: the right to reproduce or copy the work, the right to make derivative works or adapt the work, the right to distribute the work, the right to perform the work publicly, and the right to display the work publicly”).

⁶⁵ See, e.g., 17 U.S.C. § 110(3) (allowing churches to play copyrighted music without infringing); 17 U.S.C. § 110(5)(B) (allowing restaurants to play radio broadcasts for its patrons without infringing, provided “the performance is communicated by means of a total of not more than [six] loudspeakers, of which not more than [four] loudspeakers are located in any [one] room or adjoining outdoor space”).

obsolete with their rigid language and the inability of emergent stakeholders to work within them.⁶⁶

The confluence of new technology, new industries, and outdated statutory language led to a renewed push to revise the United States copyright scheme in the 1990s.⁶⁷ The meteoric adoption of a consumer internet capable of facilitating the distribution of digital media once again pitted the interests of two separate stakeholder groups directly against each other.⁶⁸ On one end were copyright holders who wanted to protect their exclusive distribution and reproduction rights and their ability to enforce them in federal court.⁶⁹ On the other were members of the nascent internet industry, both online service providers (“OSPs”)⁷⁰ and internet service providers (“ISPs”),⁷¹ who feared “potentially crippling liability for acts of infringement committed by their users as a result of the strict nature of copyright infringement liability.”⁷² OSPs in particular were right to worry; many of them hosted user-generated content—some of which was copyrighted—which made the OSPs vulnerable to suit for contributory infringement.⁷³

⁶⁶ See, e.g., Niels B. Schaumann, *Copyright Protection in the Cable Television Industry: Satellite Retransmission and the Passive Carrier Exemption*, 51 FORDHAM L. REV. 637, 665 (1983) (“The emergence of new patterns of program distribution, notably the satellite-distributed superstation, has further complicated the cable problem and . . . has seriously compromised the position which copyright holders had laboriously achieved in the . . . Copyright Act of 1976.”).

⁶⁷ U.S. COPYRIGHT OFFICE, SECTION 512 OF TITLE 17: A REPORT OF THE REGISTER OF COPYRIGHTS, 13–16 (May 2020), <https://www.copyright.gov/policy/section512/section-512-full-report.pdf> [<https://perma.cc/MN8H-UBDQ>] [hereinafter *Section 512 Report*].

⁶⁸ See LITMAN, *supra* note 26, at 103–25 (describing “the process [of passing the Digital Millennium Copyright Act] in mind-numbing detail”).

⁶⁹ *Id.* at 115.

⁷⁰ An OSP, referred to simply as a “service provider” by the statute, is “a provider of online services or network access, or the operator of facilities therefor.” 17 U.S.C. § 512(k)(1)(B).

⁷¹ ISPs are a type of OSP that “serve[] as a conduit for the automatic transmission of material at the direction of third parties.” *Section 512 Report*, *supra* note 67, at app. C.

⁷² *Section 512 Report*, *supra* note 67, at 8.

⁷³ U.S. COPYRIGHT OFFICE, SECTION 512 OF TITLE 17: RESOURCES ON ONLINE SERVICE PROVIDER SAFE HARBORS AND NOTICE-AND-TAKEDOWN

For instance, in the 1995 case of *Religious Technology Center v. Netcom*, the holders of copyrights in L. Ron Hubbard's published and unpublished works sued Dennis Erlich, a former member of the Church of Scientology and user of an online bulletin board system,⁷⁴ claiming that he had infringed their copyrights by posting portions of the copyrighted works on the bulletin board system.⁷⁵ The plaintiffs also named Netcom, the ISP whose facilities connected the bulletin board system to the internet, and Thomas Klemesrud, the operator of the bulletin board system, in their suit.⁷⁶ The district court concluded that both Klemesrud and Netcom had created copies of the infringing material to both defendants' storage devices when Erlich had posted it to the bulletin board system.⁷⁷ Although neither Netcom nor Klemesrud were directly liable for the copying caused by Erlich's infringement, the court found that they both *could* face liability for contributory infringement if they had knowledge and continued to aid in Erlich's use of their servers to post copyrighted material.⁷⁸

To established copyright owners, the outcomes of *Netcom* and similar internet copyright cases⁷⁹ represented a profitable path

SYSTEM (last visited Nov. 28, 2022), [https://www.copyright.gov/512/\[https://perma.cc/Z7X9-MK7B\]](https://www.copyright.gov/512/[https://perma.cc/Z7X9-MK7B]).

⁷⁴ Utilized before the internet was available to and widely adopted by consumers in the late 1990s, bulletin board systems were online communities that allowed users to post to message boards by connecting personal computers to remote servers through the use of telephone lines. See Scott Gilbertson, *Feb. 16, 1978: Bulletin Board Goes Electronic*, WIRED (Feb. 16, 2010, 12:00 AM), <https://www.wired.com/2010/02/0216cbbs-first-bbs-bulletin-board/> [https://perma.cc/L8C6-CA8P]. The use of telephone lines limited the speed at which users uploaded and downloaded information to the bulletin board services; as a result, much of the content posted on these bulletin board services consisted of messages and small files. See generally *id.* Online bulletin board systems can be considered an early OSP.

⁷⁵ *Religious Tech. Ctr. v. Netcom On-Line Commc'n Servs., Inc.*, 907 F. Supp. 1361, 1365–66 (N.D. Cal. 1995).

⁷⁶ *Id.* at 1366.

⁷⁷ *Id.* at 1368.

⁷⁸ *Id.* at 1372, 1375 (“The court does not find workable a theory of [direct] infringement that would hold the entire Internet liable for activities that cannot reasonably be deterred”).

⁷⁹ See, e.g., *MAI Sys. Corp. v. Peak Comput., Inc.*, 991 F.2d 511, 518–19 (9th Cir. 1993) (holding that the loading of copyrighted data into a computer's

forward. By aggressively filing copyright infringement claims against young OSPs that profited off their user's infringement, large companies that held copyrights could hamper the development of these middlemen and control the distribution of their own work over the burgeoning consumer internet marketplace.⁸⁰ Congress recognized that if the copyright law was left unaddressed, future court decisions would scare potential OSPs from entering the market with the looming threat of being held liable by copyright owners for their user's infringement.⁸¹ On the other hand, if Congress overcorrected copyright law and granted broad immunity to OSPs for its users' infringement, copyright owners would be unwilling to make their works available digitally.⁸² To find a balance that would result in passable legislation, Congress returned to the same blueprint it had used to address disputes over copyright in the past:

random access memory ("RAM") could constitute infringement within the meaning of the 1976 Copyright Act because the data stays in the RAM long enough to be perceived).

⁸⁰ For an in-depth accounting of the outcome of this strategy, see Jessica D. Litman, *Antibiotic Resistance*, 30 CARDOZO ARTS & ENT. L.J. 53, 58 (2012) ("Indiscriminate litigation against new entrants into the entertainment and information marketplace killed off a broad swathe of potential competitors and partners. The ones who were left, though, faced a less crowded field because old media had helpfully cleared it for them. The music, movie, and book publishing businesses no doubt expected to take advantage of the opening themselves, but discovered significant difficulties in doing it well").

⁸¹ See, e.g., *The Copyright Infringement Liability of Online and Internet Service Providers: Hearing on S. 1146 Before the S. Comm. on the Judiciary*, 105th Cong. 2 (1997), <https://books.google.com/books?id=RstMAZxEjzkC&pg=PP1#v=onepage&q&f=false> [<https://perma.cc/9HLQ-2V2K>] (statement of Sen. Orrin G. Hatch, Chairman, S. Comm. On the Judiciary) ("Do we want [the growth of the internet] to be retarded by a series of adverse court rulings or because content providers are reluctant to make full use of the Internet?"); see also LITMAN, *supra* note 26, at 88 ("History teaches that whenever we have discovered or enacted a copyright exception, an industry has grown up within its shelter").

⁸² *Id.*; see also LITMAN, *supra* note 26, at 83 (describing the contention that "[i]f the public wished [a thriving internet] . . . it must offer strong copyright protection as a bribe to those it hoped to persuade to create enough stuff to make an [internet] worthwhile").

let the stakeholders negotiate.⁸³ The product of these negotiations is embodied in the safe harbor provisions of the 1998 DMCA.⁸⁴

The DMCA, 17 U.S.C. § 512, builds upon the Copyright Act of 1976 and grants OSPs that host infringing content broad immunity from claims of contributory infringement as long as they meet the statute's eligibility criteria articulated in Section 512.⁸⁵ To start, an OSP seeking protection in the host safe harbor must adopt, reasonably implement, and inform users of a policy to terminate the accounts of repeat infringers.⁸⁶ Additionally, an OSP must accommodate "standard technical measures" ("STMs") used by copyright owners to identify and protect their work.⁸⁷ Next, the OSP must designate an agent to receive notification from copyright owners who believe that a specific piece of material being hosted by

⁸³ See Maayan Perel & Niva Elkin-Koren, *Accountability in Algorithmic Copyright*, 19 STAN. TECH. L. REV. 473, 484 (2016) (explaining that "[r]ights-holders pushed towards active involvement of OSPs in copyright enforcement in exchange for limited immunity from liability for copyright infringement committed by their users," leading to the inclusion of the safe harbor provisions in the Digital Millennium Copyright Act); see, e.g., LITMAN *supra* note 26, at 27–28, 43 (explaining how Congress used this same approach for the 1909 Copyright Act and the 1976 Copyright Act).

⁸⁴ 17 U.S.C. § 512; see Perel & Elkin-Koren, *supra* note 83, at 484.

⁸⁵ See 17 U.S.C. § 512(c); U.S. Copyright Office, *Copyright Law of the United States (Title 17)*, <https://www.copyright.gov/title17/> [<https://perma.cc/U3D6-M2PG>] (last visited Nov. 28, 2022) (explaining "[t]he Copyright Act of 1976 . . . provides the basic framework for the current copyright law"). Section 512 also provides safe harbors for OSPs that transmit, cache, or link to infringing content. See 17 U.S.C. § 512(a), (b), (d). However, for the purposes of this Note, this discussion is confined to the "host" safe harbor.

⁸⁶ 17 U.S.C. § 512(i)(1)(A).

⁸⁷ *Id.* § 512(i)(1)(B). In addition to identifying and protecting copyrighted work, "standard technical measures" must also be "developed pursuant to a broad consensus of copyright owners and service providers in an open, fair, voluntary, multi-industry standards process," be made "available to any person on reasonable and nondiscriminatory terms," and must not "impose substantial costs on service providers or substantial burdens on their systems or networks." *Id.* § 512(i)(2). Given both the historically acrimonious relationship between copyright holders and OSPs and the broad coalition of industries with different incentives and different demands that makes up these stakeholders, there are currently no technological measures that qualify as a "standard technical measure." See *Section 512 Report*, *supra* note 67, at 176. However, similar tools have been created by individual OSPs and are used privately. See *id.* at 66 n.352, 66–68.

the OSP is infringing.⁸⁸ OSPs are not eligible for host safe harbor protection if they have “actual knowledge” of specific infringement or are “aware of facts or circumstances from which infringing activity is apparent;” if an eligible OSP gains actual knowledge of specific infringement, it must “act[] expeditiously to remove, or disable access to, the material” in order to retain its eligibility.⁸⁹ OSPs are also ineligible for the host safe harbor if they “receive a financial benefit directly attributable to the infringing activity, in a case in which the service provider has the right and ability to control such activity.”⁹⁰

Finally, Section 512 states that in addition to the requirements described above, an OSP must employ a notice-and-takedown process.⁹¹ Notice-and-takedown works as follows: if a copyright holder has a good faith belief that an OSP is hosting specific material that infringes their copyright, the copyright holder may send a written notification to the OSPs’ designated agent.⁹² This notification must include the signature of the copyright owner or their agent;⁹³ “[i]dentification of the copyrighted work claimed to have been infringed;”⁹⁴ “[i]dentification of the material that is claimed to be infringing . . . and information reasonably sufficient to permit the service provider to locate the material;”⁹⁵ contact information for the complaining party;⁹⁶ “[a] statement that the complaining party has a good faith belief that the use of” their copyrighted material is unauthorized;⁹⁷ and a statement attesting to the accuracy of the information contained within the notice and, “under penalty of perjury, that the complaining party is authorized to act on behalf of the [copyright] owner.”⁹⁸ Upon receipt of a “notification of claimed infringement,” the OSP must “respond[]

⁸⁸ See 17 U.S.C. § 512(c)(2).

⁸⁹ *Id.* § 512(c)(1)(A).

⁹⁰ *Id.* § 512(c)(1)(B).

⁹¹ See *id.* § 512(c)(1)(C).

⁹² See *id.* § 512(c)(2).

⁹³ *Id.* § 512(c)(3)(A)(i).

⁹⁴ *Id.* § 512(c)(3)(A)(ii).

⁹⁵ *Id.* § 512(c)(3)(A)(iii).

⁹⁶ *Id.* § 512(c)(3)(A)(iv).

⁹⁷ *Id.* § 512(c)(3)(A)(v).

⁹⁸ *Id.* § 512(c)(3)(A)(vi).

expeditiously to remove, or disable access to, the material that is claimed to be infringing”⁹⁹ If the OSP complies with these host safe harbor eligibility requirements, it will not be held liable “for infringement of copyright by reason of the storage at the direction of a user of material that resides on a system or network controlled or operated by or for the service provider.”¹⁰⁰

Section 512 also grants OSPs immunity from any claim by any person based on the OSP’s “good faith disabling of access to, or removal of, material . . . claimed to be infringing . . . , regardless of whether the material or activity is ultimately determined to be infringing”¹⁰¹ as long as the OSP “takes reasonable steps promptly to notify the [user] that it has removed . . . the material”¹⁰² and facilitates the counter-notification process if initiated by the user.¹⁰³ If a user believes in good faith that their content was removed due to OSP error or due to their content falling under a copyright exception,¹⁰⁴ they may send the OSP’s designated agent a counter-notification.¹⁰⁵ Upon receipt, the agent must provide a copy of the counter-notification to the complaining party and notify that person that the OSP will “replace the removed material . . . in [ten] business days.”¹⁰⁶ Unless the complaining party files a copyright infringement action against the user, the OSP must “replace[] the removed material . . . not less than [ten], nor more than [fourteen], business days following [the] receipt of the counter notice.”¹⁰⁷

Lenz v. Universal Music Corporation illustrates some of the issues that this notice-and-takedown and counter-notification regime brings to the surface.¹⁰⁸ In February of 2007, Stephanie Lenz uploaded a twenty-nine-second video to YouTube of her children

⁹⁹ *Id.* § 512(c)(1)(C).

¹⁰⁰ *Id.* § 512(c)(1).

¹⁰¹ *Id.* § 512(g)(1).

¹⁰² *Id.* § 512(g)(2)(A).

¹⁰³ *Id.* § 512(g)(2)(B).

¹⁰⁴ *Id.* § 512(g)(3)(C).

¹⁰⁵ *Id.* § 512(g)(3). This counter-notification must include a statement that the user “consents to the jurisdiction of a federal district court” and agrees to accept service of process from the complaining party. *Id.* § 512(g)(3)(D).

¹⁰⁶ 17 U.S.C. § 512(g)(2)(B).

¹⁰⁷ *Id.* § 512(g)(2)(C).

¹⁰⁸ *Lenz v. Universal Music Corp.*, 815 F.3d 1145 (9th Cir. 2016).

dancing to the song “Let’s Go Crazy” by Prince.¹⁰⁹ At the time, Universal Music Corporation (“Universal”) was Prince’s publishing administrator, responsible for enforcing the artist’s copyright.¹¹⁰ To enforce its artists’ copyrights on YouTube, Universal assigned a legal department assistant to monitor the site manually and review any video that made “significant use of . . . [Prince’s] composition, specifically if the song was recognizable, was in a significant portion of the video, or was the focus of the video.”¹¹¹ When the assistant found Lenz’s video, he concluded that Prince’s song was the “focus of the video” because it played in the background for duration of the video and because the video was titled “‘Let’s Go Crazy’ #1.”¹¹² Universal later sent YouTube a takedown notice, containing a list of more than 200 videos (including Lenz’s) that Universal, in good faith, believed made unauthorized use of Prince’s music.¹¹³

Upon receipt of Universal’s notification and consistent with the conditions of its host safe harbor eligibility,¹¹⁴ YouTube removed Lenz’s video and notified her of the removal.¹¹⁵ Lenz responded with a counter-notification to restore her video.¹¹⁶ YouTube provided a copy of the counter-notification to Universal, who “protested the videos reinstatement,” claiming that “Lenz failed to properly acknowledge that her statement was made under penalty of perjury” and “that the video constituted infringement because” Universal had not granted Lenz a license to exploit Prince’s

¹⁰⁹ *Id.* at 1149.

¹¹⁰ *Id.*

¹¹¹ *Id.* (citations omitted). It is worth noting that in 2007, Universal was still manually monitoring YouTube for any infringements of their copyrights. *Id.* YouTube would introduce its automated Content ID copyright enforcement tool later that year in response to infringement lawsuits from media companies. See Kevin J. Delaney, *YouTube to Test Software to Ease Licensing Fights*, WALL ST. J. (June 12, 2007, 11:59 PM), <https://www.wsj.com/articles/SB118161295626932114> [<https://perma.cc/D4GZ-3LNW>].

¹¹² *Lenz*, 815 F.3d at 1149.

¹¹³ *Id.*

¹¹⁴ 17 U.S.C. § 512(c)(1)(C).

¹¹⁵ *Lenz*, 815 F.3d at 1149–50.

¹¹⁶ *Id.* at 1150.

composition.¹¹⁷ Twenty days after she had sent the initial counter-notice, Lenz, with the help of legal counsel, sent YouTube a second counter-notice.¹¹⁸ A few weeks later, YouTube reinstated the video.¹¹⁹ Shortly thereafter, Lenz sued Universal for misrepresentation under Section 512(f) of the DMCA, arguing that her use of the Prince song was obviously fair.¹²⁰

In 2013, six years after Lenz first filed her complaint, the Northern District of California denied both parties' motions for summary judgment, and both parties appealed to the Ninth Circuit.¹²¹ The issue before the court was whether the notice-and-takedown regime required Universal to consider whether Lenz's video was a fair use of a copyright before it sent a takedown notice to YouTube.¹²² Here, the Ninth Circuit held that by requiring a notice to include "a statement that the complaining party has a good faith belief that the use of the material in the manner complained of is not authorized by the copyright owner,"¹²³ the DMCA clearly "contemplates fair use as a use authorized by the law."¹²⁴ Therefore, "a copyright holder must consider the existence of fair use before sending a takedown notice under [Section] 512(c)."¹²⁵ Further, the court discussed whether Universal had a good faith belief that

¹¹⁷ *Id.*

¹¹⁸ *Id.*

¹¹⁹ *Id.*

¹²⁰ *Id.* at 1150, 1153. A claim for misrepresentation is derived from the following subsection of Section 512: "Any person who knowingly materially misrepresents under this section— (1) that material or activity is infringing, or (2) that material or activity was removed or disabled by mistake or misidentification, shall be liable for any damages, including costs and attorneys' fees, incurred by the alleged infringer, by any copyright owner or copyright owner's authorized licensee, or by a service provider, who is injured by such misrepresentation, as the result of the service provider relying upon such misrepresentation in removing or disabling access to the material or activity claimed to be infringing, or in replacing the removed material or ceasing to disable access to it." 17 U.S.C. § 512(f).

¹²¹ *Lenz*, 815 F.3d at 1150.

¹²² *Id.* at 1151.

¹²³ *Id.* (quoting 17 U.S.C. § 512(c)(3)(A)(v)).

¹²⁴ *Id.*

¹²⁵ *Id.* at 1153.

Lenz's video was not a fair use of its copyright.¹²⁶ Because the good faith belief requirement "encompasses a subjective, rather than objective, standard,"¹²⁷ the majority noted that "whether Universal's actions were sufficient to form a subjective good faith belief about the video's fair use or lack thereof" was an issue for the jury.¹²⁸ However, Judge Smith disagreed with the majority's conclusion.¹²⁹ He noted that Universal did not direct the legal assistant to consider fair use when compiling videos to include in the takedown notices; rather, the assistant was instructed merely to "spare videos that had 'a second or less of a Prince song' or where the song was 'distorted beyond reasonable recognition.'"¹³⁰ Thus, Judge Smith found that there was no disputed issue of fact since "Universal did *not* consider fair use before issuing a takedown notice."¹³¹

While the Ninth Circuit unanimously held that a copyright holder must consider whether a use is fair before sending a takedown notice to an OSP,¹³² the DMCA's notice-and-takedown regime now regulates an internet vastly larger than the one into which it was born.¹³³ To protect their distribution rights on an ever-expanding internet, copyright holders have developed content-detection technologies that identify infringing uses of their content on the internet and automatically generate notices.¹³⁴ These notice-

¹²⁶ *Id.* at 1153–54.

¹²⁷ *Rossi v. Motion Picture Ass'n of Am.*, 391 F.3d 1000, 1004 (9th Cir. 2004).

¹²⁸ *Lenz*, 815 F.3d at 1154.

¹²⁹ *Id.* at 1158 (Smith, J., concurring in part, dissenting in part).

¹³⁰ *Id.* at 1159 ("Nothing in Universal's methodology considered the purpose and character of the use, the commercial or noncommercial nature of the use, or whether the use would have a significant impact on the market for the copyrighted work.").

¹³¹ *Id.* at 1159–60 (Smith, J., concurring in part, dissenting in part).

¹³² *Id.* at 1153.

¹³³ See *Section 512 Report*, *supra* note 67, at 30–32 (noting that Internet access worldwide has increased from 3.14% in 1998 to over 50% in 2020, and that the notice-and-takedown system has been overloaded by the volume of infringement notices being sent).

¹³⁴ See YOUTUBE, *Copyright Transparency Report 3* (2021), https://storage.googleapis.com/transparencyreport/report-downloads/pdf-report-22_2021-1-1_2021-6-30_en_v1.pdf [<https://perma.cc/5PDJ-3KZ5>].

generating technologies raise serious free speech concerns.¹³⁵ Without constant human review, they are ill-equipped to distinguish between an infringing use and a fair one, making the *Lenz* good faith standard much more difficult to meet.¹³⁶ As a result, in the last three decades, the number of infringement notices copyright holders sent to OSPs increased dramatically—for instance, while Google received less than three million such notices between the DMCA’s enactment in 1998 and 2010, it received 882 million URL-based infringement notices in 2017 alone.¹³⁷ Because OSPs must expeditiously remove or block access to the subject of the notice to maintain its Section 512 safe harbor protection,¹³⁸ this skyrocketing in the volume of notices has forced OSPs to develop automated rights management solutions that allow them to work around the stringent choreography of the DMCA and directly with the largest copyright holders.

¹³⁵ See, e.g., Jonathon W. Penney, *Privacy and Legal Automation: The DMCA as a Case Study*, 22 STAN. TECH. L. REV. 412, 464–65 (2019) (finding, in a study investigating the chilling effects of DMCA notices on online speech and expression, that 70% of survey respondents were either very unlikely or somewhat unlikely to repost or re-share content targeted by a DMCA notice and that 66% of survey respondents would not challenge a DMCA notice even if they believed that the notice was wrong or inaccurate).

¹³⁶ See *The Digital Millennium Copyright Act at 22: What Is It, Why Was It Enacted, and Where Are We Now? Before the Subcomm. on Intell. Prop. of the S. Comm. on the Judiciary*, 116th Cong. 9 (2020) (testimony of Jessica Litman, Professor of Law and Information, University of Michigan) (“[Automated] solutions were and continue to be buggy. There are widespread documented instances of over-claiming, mistaken claiming, and false claiming. . . . Efforts to use computers to distinguish infringing from fair uses are, perhaps unavoidably, crude”).

¹³⁷ For instance, Google received less than three million notices for URLs hosting allegedly infringing content in the twelve years between the DMCA’s enactment in 1998 and 2010. *Section 512 Report*, *supra* note 67, at 32. In 2017 alone, the number of notices received by Google skyrocketed to approximately 882 million URLs. See GOOGLE, *supra* note 25, at 14.

¹³⁸ See 17 U.S.C. § 512(c)(1)(C).

II. OSP-CREATED COPYRIGHT FILTERING SYSTEMS WITHIN DMCA SAFE HARBORS

Lawrence Lessig, the Roy L. Furman Professor of Law and Leadership at Harvard Law School, predicted that “[c]ode can, and increasingly will, displace law as the primary defense of intellectual property in cyberspace.”¹³⁹ Today, with respect to online video hosting websites within DMCA safe harbors, this transition from legal to algorithmic enforcement of intellectual property rights has already occurred. YouTube redefined its relationship with major copyright owners by developing its automated copyright filtering system that has effectively usurped the DMCA’s notice-and-takedown regime,¹⁴⁰ enriching the company through licensing deals with large copyright holders while silencing non-infringing content.¹⁴¹

In 2007, one year after Google’s \$1.65 billion acquisition of YouTube, Viacom International (“Viacom”), a media conglomerate, sued both companies for direct and secondary copyright

¹³⁹ LAWRENCE LESSIG, CODE: VERSION 2.0 175 (2nd ed. 2006); *Lawrence Lessig*, HARVARD LAW SCHOOL, <https://hls.harvard.edu/faculty/lawrence-lessig/> [<https://perma.cc/X3JQ-966N>] (last visited Nov. 28, 2022). Lessig also argued against copyright extensions before the Supreme Court in *Eldred*. *Lawrence Lessig*, STANFORD LAW SCHOOL—THE CTR. FOR INTERNET SECURITY, <https://cyberlaw.stanford.edu/about/people/lawrence-lessig> [<https://perma.cc/2LV9-9R5L>] (last visited Nov. 28, 2022).

¹⁴⁰ See YouTube, *Copyright Transparency Report* 10, 12 (Dec. 2021), https://storage.googleapis.com/transparencyreport/report-downloads/pdf-report-22_2021-1-1_2021-6-30_en_v1.pdf [<https://perma.cc/5PDJ-3KZ5>] (noting that “[o]ver 99% of [the total 722,649,569] Content ID claims from the first half of 2021 were made through automated detection, with partners’ usage of manual options being exceedingly rare (fewer than 0.5% of total claims.)”); GOOGLE, *supra* note 25, at 24 (“Over 98% of copyright issues on YouTube are handled through Content ID, rather than the notice-and-takedown process.”).

¹⁴¹ See Cedric Manara, *Protecting What We Love About the Internet: Our Efforts to Stop Online Piracy*, GOOGLE: THE KEYWORD (Nov. 7, 2018), <https://www.blog.google/outreach-initiatives/public-policy/protecting-what-we-love-about-internet-our-efforts-stop-online-piracy/> [<https://perma.cc/9MQU-K4S3>] (noting that as of 2018, “YouTube has paid to rights holders who have monetized use of their content in other videos through Content ID” over \$3 billion).

infringement.¹⁴² In *Viacom International Inc. v. YouTube, Inc.*, Viacom “identified more than 150,000 unauthorized clips of [its] copyrighted programming on YouTube” and alleged that YouTube had profited by “actively engag[ing] in, promot[ing] and induc[ing] . . . infringement” to grow its website.¹⁴³ YouTube moved for summary judgment, arguing that because Viacom had not provided notice of the infringements identified in the complaint, it did not have specific knowledge of the infringing material and was thus protected by the DMCA’s host safe harbor.¹⁴⁴ The district court granted YouTube’s motion,¹⁴⁵ stating that the DMCA explicitly places the burden of policing infringement on the copyright owner.¹⁴⁶ However, the court noted that when Viacom “accumulated some 100,000 videos and then sent one mass take-down notice” to YouTube before the commencement of the lawsuit, YouTube expeditiously removed nearly every video; thus, YouTube’s behavior complied with the DMCA’s safe harbor standards.¹⁴⁷ To the court, this case illustrated that “the DMCA notification regime work[ed] efficiently.”¹⁴⁸

On appeal, while the Second Circuit vacated the lower court’s ruling and remanded the case for further fact-finding on specific issues, it largely agreed with the lower court’s interpretation of Section 512.¹⁴⁹ In particular, the Second Circuit stated that the statute does not condition safe harbor protection on “affirmative monitoring by an [OSP].”¹⁵⁰ Therefore, if YouTube did not have specific knowledge of the infringing content on its platform, it could

¹⁴² See *Viacom Int’l, Inc. v. YouTube, Inc.*, 718 F. Supp. 2d 514 (S.D.N.Y. 2010).

¹⁴³ Complaint for Declaratory and Injunctive Relief and Damages at 2–3, *Viacom Int’l, Inc. v. YouTube, Inc.*, 718 F. Supp. 2d 514 (S.D.N.Y. 2010) (No. 07 Civ. 2103).

¹⁴⁴ *Viacom*, 718 F. Supp. 2d at 516.

¹⁴⁵ See *id.* at 529.

¹⁴⁶ *Id.* at 523–24; see also 17 U.S.C. § 512(m)(1) (stating that a service provider’s eligibility for safe harbor protection shall not be conditioned on monitoring its service).

¹⁴⁷ *Viacom*, 718 F. Supp. 2d at 524.

¹⁴⁸ *Id.*

¹⁴⁹ *Viacom Int’l, Inc. v. YouTube, Inc.*, 676 F.3d 19, 41–42 (2d Cir. 2012).

¹⁵⁰ *Id.* at 35; see also 17 U.S.C. § 512(m)(1).

not have been “willfully blind” to the presence of such content.¹⁵¹ On remand, Viacom could not point to any specific examples of infringing content still being hosted on YouTube.¹⁵² Because the DMCA does not require an OSP to “affirmatively seek[] facts indicating infringing activity,”¹⁵³ YouTube did not have to find the infringing clips that Viacom could only identify generally.¹⁵⁴ Thus, the district court held that YouTube was not willfully blind to specific infringement¹⁵⁵ and again granted YouTube’s motion for summary judgment.¹⁵⁶ The parties settled shortly before they were scheduled to appear before the Second Circuit.¹⁵⁷ Although Viacom had sought \$1 billion in damages,¹⁵⁸ the settlement reportedly did not include any payments.¹⁵⁹ In a joint statement, Google and

¹⁵¹ *Viacom*, 676 F.3d at 35 (“Accordingly, we hold that the willful blindness doctrine may be applied, in appropriate circumstances, to demonstrate knowledge or awareness of specific instances of infringement under the DMCA”).

¹⁵² *Viacom Int’l Inc. v. YouTube, Inc.*, 940 F. Supp. 2d 110, 116–17 (S.D.N.Y. 2013).

¹⁵³ 17 U.S.C. § 512(m)(1).

¹⁵⁴ *Viacom*, 940 F. Supp. 2d at 117.

¹⁵⁵ *Id.*

¹⁵⁶ *Id.* at 123.

¹⁵⁷ Leslie Kaufman, *Viacom and YouTube Settle Suit Over Copyright Violations*, N.Y. TIMES (Mar. 18, 2014), <https://www.nytimes.com/2014/03/19/business/media/viacom-and-youtube-settle-lawsuit-over-copyright.html> [https://perma.cc/HX8R-DXLJ]; see John Silver, *Viacom and Google Settle \$1 Billion YouTube Lawsuit*, ARS TECHNICA (Mar. 18, 2014 11:54 AM), <https://arstechnica.com/tech-policy/2014/03/viacom-and-google-reach-settlement-in-long-running-youtube-lawsuit/> [https://perma.cc/FNQ9-7NRH].

¹⁵⁸ See Miguel Helft, *Judge Sides with Google in Viacom Video Suit*, N.Y. TIMES (June 23, 2010), <https://www.nytimes.com/2010/06/24/technology/24google.html> [https://perma.cc/S546-58RP]. During the seven-year life of the case, both companies revealed embarrassing information about the business practices of the other, with respect to their handling and unauthorized use of copyrighted material for the sake of growth. *Id.* (mentioning emails sent by YouTube’s founders that “suggested they were willing to overlook pirated videos on the site as they tried to increase traffic to the site and sell the company” and emails showing that agents of Viacom were “uploading copyrighted clips to YouTube even as [Viacom] was complaining about copyright infringement”).

¹⁵⁹ See Kaufman, *supra* note 157.

Viacom wrote that “[t]his settlement reflect[ed] the growing collaborative dialogue between [the] two companies on important opportunities” and that “[they] look[ed] forward to working more closely together.”¹⁶⁰

The same year that Viacom’s lawsuit began, YouTube launched the beta version of what would become its proprietary copyright filtering system: Content ID.¹⁶¹ While the DMCA does not require OSPs to monitor their platforms for infringing content,¹⁶² much to the delight of large copyright owners,¹⁶³ Content ID represents a voluntary adoption of this optional duty to monitor. When a video is uploaded to YouTube, Content ID scans it against a database of audio and visual reference files provided by participating content owners.¹⁶⁴ When an uploaded video matches a database file, YouTube notifies the copyright owner, who then has the option to “block the video that matched their content, monetize the video,” or merely “track the video to get detailed analytics, such as countries where their content is popular.”¹⁶⁵ In the event of a match, a user can dispute the Content ID claim if they believe that their video was misidentified with a database file; if the user chooses to dispute the claim, the video will remain active and unchanged until the

¹⁶⁰ Jonathan Stempel, *Google, Viacom Settle Landmark YouTube Lawsuit*, REUTERS (Mar. 18, 2014, 9:05 AM), <https://www.reuters.com/article/us-google-viacom-lawsuit/google-viacom-settle-landmark-youtube-lawsuit-idUSBREA2H11220140318> [<https://perma.cc/ZZ9R-4DDD>].

¹⁶¹ See David King, *Latest Content ID Tool for YouTube*, GOOGLE BLOG (Oct. 15, 2007), <https://googleblog.blogspot.com/2007/10/latest-content-id-tool-for-youtube.html> [<https://perma.cc/WFY8-G88F>]; Megan Geuss, *YouTube Has Paid \$1 Billion to Rights Holders via Content ID Since 2007*, ARS TECHNICA (Oct. 13, 2014, 7:53 PM), <https://arstechnica.com/tech-policy/2014/10/youtube-has-paid-1-billion-to-rights-holders-via-content-id-since-2007/> [<https://perma.cc/B26E-PRPP>].

¹⁶² See 17 U.S.C. § 512(m).

¹⁶³ See *Section 512 Report*, *supra* note 67, at 43.

¹⁶⁴ See *id.* at 42.

¹⁶⁵ *How Content ID Works*, YOUTUBE HELP, <https://support.google.com/youtube/answer/2797370> [<https://perma.cc/TUG5-CQQJ>] (last visited Nov. 28, 2022).

copyright owner responds.¹⁶⁶ At any point during this process, the copyright owner may choose to bypass the Content ID process and send YouTube's agent a formal notice-and-takedown request as mandated by the DMCA.¹⁶⁷ However, 98% of YouTube's copyright claims are handled through Content ID, while "the remaining 2% are addressed through DMCA takedown requests."¹⁶⁸

YouTube openly admits that its Content ID system is not governed by the same statute that governs the notice-and-takedown process.¹⁶⁹ However, there are some other key differences in the two systems that make Content ID more restrictive to online speech than the DMCA. On the one hand, any copyright holder can utilize the DMCA notice-and-takedown process.¹⁷⁰ While OSPs have simplified this process by hosting takedown request forms on their platforms, copyright holders still have the burden of locating the infringing content.¹⁷¹ On the other hand, only a select group of copyright holders can participate in YouTube's Content ID system.¹⁷² Therefore, the Content ID system does not treat all copyright holders equally. In addition, once a copyright holder becomes a participant, he no longer has the burden of finding potentially infringing content thanks to the Content ID algorithm that automatically notifies him of a match when the video is uploaded.¹⁷³ In theory, once notified, he could then issue a takedown

¹⁶⁶ See *Dispute Content ID Claim*, YOUTUBE HELP, <https://support.google.com/youtube/answer/2797454> [https://perma.cc/JQ37-2HGB] (last visited Nov. 28, 2022).

¹⁶⁷ See *id.*

¹⁶⁸ See GOOGLE, *supra* note 25, at 24.

¹⁶⁹ See *What Is a Copyright Claim?*, YOUTUBE HELP, <https://support.google.com/youtube/answer/7002106> [https://perma.cc/J2RB-7XVJ] (last visited Nov. 28, 2022) ("Unlike copyright removal requests, which are defined by law, Content ID is a tool created by YouTube. When Content ID finds a match, it applies a Content ID claim on the matching content").

¹⁷⁰ See 17 U.S.C. § 512(m).

¹⁷¹ *Id.*

¹⁷² See YOUTUBE HELP, *supra* note 165 ("YouTube only grants Content ID to copyright owners who meet specific criteria. To be approved, they must own exclusive rights to a substantial body of original material that is frequently uploaded by the YouTube creator community").

¹⁷³ See GOOGLE, *supra* note 25, at 24 ("Within Content ID, 98% of claims in 2017 were automated—meaning that Content ID automatically identified the

notice to remove the video from YouTube immediately. The DMCA clearly and exhaustively choreographs a notice-and-takedown regime that, while cumbersome, is a transparent process able to be disputed before a judge in federal court. This makes sense, as the statute was publicly negotiated by stakeholders before being enacted into law.¹⁷⁴ In contrast, Content ID represents the product of a different kind of bargain—one between a single OSP (YouTube) and the copyright holders with whom it chooses to work. YouTube’s dominance¹⁷⁵ and major copyright holders’ inability to monitor the entire internet for potential infringement has led those major copyright holders to believe that participating in YouTube’s Content ID system is the most realistic way to receive value for general copyright infringement.¹⁷⁶ Although YouTube educates creators and copyright holders about the basics of the Content ID system,¹⁷⁷ it

work and applied the copyright owner’s preferred action, without the need for intervention by the copyright owner”).

¹⁷⁴ See LITMAN, *supra* note 26, at 73.

¹⁷⁵ See Auxier & Anderson, *supra* note 38 (finding that 81% of Americans use YouTube).

¹⁷⁶ See Jem Aswad, *YouTube Strikes New Deals with Universal and Sony Music*, VARIETY (Dec. 19, 2017, 8:14 AM), <https://variety.com/2017/biz/news/universal-music-group-and-youtube-reach-new-global-multi-year-agreement-1202644815/> [https://perma.cc/UTM8-WFWX] (In a statement by Warner Music Group CEO Steve Cooper regarding a 2017 memo announcing the extension of Warner’s licensing deal with YouTube, Cooper stated “[w]e secured the best possible deals under very difficult circumstances. Our new deals are also shorter than usual, giving us more options in the future Nevertheless, our fight to further improve compensation and control for our songwriters and artists continues to be hindered by the leverage that ‘safe harbor’ laws provide YouTube and other user-uploaded services There’s no getting around the fact that, even if YouTube doesn’t have licenses, our music will still be available but not monetized at all”); see also *The Digital Millennium Copyright Act at 22: What Is It, Why It Was Enacted, And Where Are We Now?: Hearing Before the Subcomm. on Intell. Prop. of the S. Comm. on the Judiciary*, 116th Cong. 10 (2020), (statement of Jessica Litman, Professor of Law and Information, University of Michigan) (“[Apple, Amazon, Facebook, and Google] had become obligatory partners for content owners hoping to distribute their works online. The content industries faced a market in which they could no longer dictate terms and prices.”).

¹⁷⁷ See, e.g., YouTube Creators, *YouTube Content ID*, YOUTUBE (Sept. 28, 2010), <https://www.youtube.com/watch?v=9g2U12SsRns> [https://perma.cc/25AB-EV6Y].

has never disclosed the mechanics of its matching process. This lack of transparency limits users' understanding of why their content receives a Content ID claim and raises many questions about the ability of the Content ID algorithm to distinguish infringing from non-infringing uses, such as *de minimis* copying¹⁷⁸ or fair uses.¹⁷⁹ Additionally, limited human oversight over Content ID's decisions exacerbates these issues.¹⁸⁰

¹⁷⁸ *De minimis* copying occurs when a trivial amount of copyrighted material appears in an otherwise infringing work. See, e.g., *On Davis v. The Gap, Inc.*, 246 F.3d 152, 172 (2d Cir. 2001), as amended (May 15, 2001) ("The *de minimis* doctrine essentially provides that where unauthorized copying is sufficiently trivial, the law will not impose legal consequences") (quotations omitted) (citation omitted).

¹⁷⁹ There is a great deal of anecdotal evidence illustrating Content ID's inability to differentiate infringing and non-infringing uses. See, e.g., *How Explaining Copyright Broke the YouTube Copyright System*, N.Y.U. ENGELBERG CTR. ON INNOVATION L. & POL'Y (Mar. 4, 2020) <https://www.law.nyu.edu/centers/engelberg/news/2020-03-04-youtube-takedown> [<https://perma.cc/A7HH-PHJN>] (describing the Content ID takedown of a YouTube video of a panel about "analyz[ing] and explain[ing] songs in copyright litigation," which the NYU faculty was confident would be protected by fair use); Joseph Bottum, *The Empire Strikes Bach*, WASH. FREE BEACON (Sept. 8, 2018, 5:00 AM) <https://freebeacon.com/culture/google-youtube-algorithm-copyright/> [<https://perma.cc/8D5R-688W>] (describing an incident in which the Content ID System "almost immediately removed [a] video" of a classical pianist playing Bach because Sony owned the copyright for a specific recording); Cory Doctorow, *Youtube Nukes 7 Hours' Worth of Science Symposium Audio Due To Background Music During Lunch Break*, BOING BOING (Nov. 25, 2014, 3:00 PM) <https://boingboing.net/2014/11/25/youtube-nukes-7-hours-worth.html> [<https://perma.cc/KV2Z-8G7U>] (explaining that the recording of a seven hour conference was muted by YouTube because "our DJ played music during [the] lunch break, and YouTube allege[d] this to be a copyright violation.").

¹⁸⁰ Already limited human oversight has been reduced further by the COVID-19 pandemic. See The YouTube Team, *Protecting Our Extended Workforce and The Community*, YOUTUBE OFF. BLOG (Mar. 16, 2020) <https://blog.youtube/news-and-events/protecting-our-extended-workforce-and/> [<https://perma.cc/K596-28JU>] ("As a result of the new measures we're taking, we will temporarily start relying more on technology to help with some of the work normally done by reviewers. This means automated systems will start removing some content without human review, so we can continue to act quickly to remove violative content and protect our ecosystem").

Together, the issues described above reflect the reality that YouTube's Content ID system has effectively replaced the DMCA's notice-and-takedown regime to become de facto copyright law "governing" online videos. The obfuscation of Content ID and actual copyright law has led some police officers to attempt to silence free speech and avoid accountability for their actions, no matter how innocuous, by weaponizing these filtering systems with "copyright hacking."

III. "COPYRIGHT HACKING" AND QUALIFIED IMMUNITY

If a police officer successfully "copyright hacks" a bystander's video, the video could be removed from the social media platform to which it was uploaded. The "copyright hacking" officer would likely avoid liability because of qualified immunity's high bar. 42 U.S.C. § 1983 is arguably one of the strongest legal tools that ordinary citizens have against state government agents who overstep their authority and engage in unlawful activity.¹⁸¹ Section 1983 states that "every person who . . . subjects, or causes to be subjected, any citizen of the United States . . . to the deprivation of any rights, privileges, or immunities secured by the Constitution and laws, shall be liable to the party injured"¹⁸² Notably, the text of the statute does not include any grounds for immunity.¹⁸³ However, the Supreme Court has integrated the common law principle of judicial immunity into its jurisprudence¹⁸⁴ and has since extended this principle to provide qualified immunity to state government officials

¹⁸¹ 42 U.S.C. § 1983; see Dani Kritter, *The Overlooked Barrier to Section 1983 Claims: State Catch-All Statutes of Limitations*, CALIF. L. REV.: ONLINE (Mar. 2021), <https://www.californialawreview.org/the-overlooked-barrier-to-section-1983-claims-state-catch-all-statutes-of-limitations/> [https://perma.cc/XD7T-QQTG].

¹⁸² 42 U.S.C. § 1983.

¹⁸³ See Jay R. Schweikert, *Qualified Immunity: A Legal, Practical, and Moral Failure*, CATO INST. 6 (Sept. 14, 2020), <https://www.cato.org/sites/cato.org/files/2020-09/pa-901-update.pdf> [https://perma.cc/AK5Z-N5LV].

¹⁸⁴ *Bradley v. Fisher*, 80 U.S. 335, 347 (1871); *Forrester v. White*, 484 U.S. 219, 225–30 (1988).

who act within the scope of their roles, such as legislators,¹⁸⁵ prosecutors,¹⁸⁶ and perhaps most significantly, police officers.¹⁸⁷

In the 1967 case *Pierson v. Ray*, the Supreme Court crafted its first qualified immunity standard, holding that police officers who committed the tort of false imprisonment should be excused from liability in a Section 1983 claim on the common law defense of good faith.¹⁸⁸ Only seven years later, the Court expanded the applicability of the good-faith defense, holding that it could be used by any state executive official for “acts performed in the course of official conduct.”¹⁸⁹ In subsequent decisions, the Court determined that qualified immunity was an affirmative defense¹⁹⁰ that would be defeated only if the defendant-official “knew or reasonably should have known that the action he took within his sphere of official responsibility would violate the constitutional rights of the [plaintiff] affected, or if he took the action with the malicious intention to cause a deprivation of constitutional rights or other injury to the [plaintiff].”¹⁹¹

The Court later acknowledged that the subjective good-faith requirement of the qualified immunity defense would impede courts from “dismiss[ing] . . . insubstantial lawsuits without trial,”¹⁹² which, in turn, would lead to potentially invasive discovery and “disrupti[on] of effective government.”¹⁹³ Thus, in 1982, the Court eliminated the subjective good-faith requirement of qualified immunity and replaced it with an objective good-faith requirement, creating the framework for our modern day conception of the

¹⁸⁵ *Tenney v. Brandhove*, 341 U.S. 367, 377–79 (1951).

¹⁸⁶ *Imbler v. Pachtman*, 424 U.S. 409, 430 (1976).

¹⁸⁷ *Pierson v. Ray*, 386 U.S. 547, 555–57 (1967).

¹⁸⁸ *Id.*

¹⁸⁹ *Scheuer v. Rhodes*, 416 U.S. 232, 247–48 (1974).

¹⁹⁰ *Gomez v. Toledo*, 466 U.S. 635, 640 (1980). (“Since qualified immunity is a defense, the burden of pleading it rests with the defendant. It is for the official to claim that his conduct was justified by an objectively reasonable belief it was lawful”) (citations omitted).

¹⁹¹ *Wood v. Strickland*, 420 U.S. 308, 322 (1975), *abrogated by* *Harlow v. Fitzgerald*, 457 U.S. 800, 818 (1982).

¹⁹² *Harlow*, 457 U.S. at 814, 817.

¹⁹³ *Id.* at 819.

doctrine.¹⁹⁴ In *Harlow v. Fitzgerald*, the Court articulated a new standard for qualified immunity, holding that “government officials performing discretionary functions generally are shielded from liability for civil damages insofar as their conduct does not violate clearly established statutory or constitutional rights of which a reasonable person would have known.”¹⁹⁵ The Court also expressly stated that while the facts of *Harlow* dealt with elements of immunity available to federal officials and not to “state officials sued for constitutional violations under [Section 1983], . . . it would be ‘untenable to draw a distinction for purposes of immunity law between suits brought against state officials under [Section] 1983 and suits brought directly under the Constitution against federal officials.’”¹⁹⁶ Therefore, the qualified immunity defense is available to both federal and state government officials.

While the Supreme Court has continued to employ the *Harlow* standard’s basic contours on qualified immunity claims,¹⁹⁷ recent decisions have made it significantly more difficult for plaintiffs to overcome the “clearly established right” prong. To overcome this standard, a plaintiff must show in their pleading that an official violated their rights as enumerated by statute or by the Constitution, and that this right was clearly established at the time the alleged violation occurred.¹⁹⁸ In 2009, the Court abrogated an earlier decision that required lower courts ruling on qualified immunity claims to determine whether a plaintiff’s rights were violated before moving on to whether that right was clearly established.¹⁹⁹ The Court held in *Pearson v. Callahan* that lower courts may address either prong of the two-pronged qualified immunity analysis first “in

¹⁹⁴ *Id.* at 818.

¹⁹⁵ *Id.*

¹⁹⁶ *Id.* at 818 n.30 (quoting *Butz v. Economou*, 438 U.S. 478, 504 (1978)).

¹⁹⁷ *See, e.g., City of Escondido, Cal. v. Emmons*, 139 S. Ct. 500, 503 (2019) (“As we have explained many times: ‘Qualified immunity attached when an official’s conduct does not violate clearly established statutory or constitutional rights of which a reasonable person would have known’”) (quoting *Kisela v. Hughes*, 138 S. Ct. 1148, 1152 (2018)).

¹⁹⁸ *Harlow*, 457 U.S. at 819.

¹⁹⁹ *Saucier v. Katz*, 533 U.S. 194, 201 (2001), *abrogated by Pearson v. Callahan*, 555 U.S. 223, 236 (2009).

light of the circumstances in the particular case at hand.”²⁰⁰ In effect, this ruling gave lower courts discretion to dismiss a lawsuit against a government official as soon as they determine that the plaintiff’s right was not clearly established, without addressing whether the official’s actions constituted a violation of that right.²⁰¹ Therefore, the fate of any case in which a defendant asserts qualified immunity hinges on the threshold issue of whether the plaintiff’s rights were clearly established at the time of the alleged violation. Unfortunately for plaintiffs, a clearly established right cannot be defined “at a high level of generality”²⁰² and “must be ‘particularized’ to the facts of the case.”²⁰³ Therefore, if there is no caselaw in which the court held that there was a clearly established right and in which facts are substantially similar to those alleged by the plaintiff, a court will not hold that the right was clearly established.²⁰⁴

While the Supreme Court has previously stated that a major purpose of the First Amendment “was to protect the free discussion of governmental affairs,”²⁰⁵ it has not explicitly held that the First Amendment contains a right to record the public activity of police officers. Without guidance from the Supreme Court, federal appellate courts were left to grapple with this issue. Until recently, appellate courts unanimously found that a First Amendment right to record does exist.²⁰⁶ However, despite the overwhelming persuasive

²⁰⁰ *Pearson*, 555 U.S. at 236.

²⁰¹ *See id.* at 242 (“Because the two-step *Saucier* procedure is often, but not always, advantageous, the judges of the district courts and the court of appeals are in the best position to determine the order of decisionmaking [*sic*] that will best facilitate the fair and efficient disposition of each case.”).

²⁰² *Ashcroft v. al-Kidd*, 563 U.S. 731, 742 (2011).

²⁰³ *White v. Pauly*, 580 U.S. 73, 79 (2017) (quoting *Anderson v. Creighton*, 483 U.S. 653, 640 (1987)).

²⁰⁴ *See* Schweikert, *supra* note 183, at 7–8 (listing examples of federal appellate cases in which courts held that police officers did not violate clearly established law because the cases that plaintiffs cited had superficial factual differences). In other words, by defining the right too specifically, the right becomes useless in practice. *Id.*

²⁰⁵ *Mills v. State of Ala.*, 384 U.S. 214, 218 (1966).

²⁰⁶ However, federal appellate courts have disagreed on the scope of this right. *See Fordyce v. City of Seattle*, 55 F.3d 436, 439 (9th Cir. 1995) (holding that a police officer who assaulted the plaintiff for filming bystanders during a public demonstration may have done so to “prevent or dissuade him from

authority from other appellate courts, in March of 2021, the Tenth Circuit held that this First Amendment right was not clearly established.²⁰⁷

In *Frasier v. Evans*, Plaintiff-Appellee Levi Frasier used his tablet to record Denver police officers using force during the arrest of an uncooperative suspect in a public parking lot.²⁰⁸ Once the suspect was in custody, a police officer, Christopher Evans, approached Frasier and asked him if he had filmed the altercation; Frasier lied, telling the officer that “he took only a Snapchat photo of the arrest.”²⁰⁹ As the two spoke, the remaining officers surrounded Frasier and “repeatedly demanded” that he hand over his tablet.²¹⁰ Frasier complied; he retrieved his tablet and went with Officer Evans behind a nearby SUV.²¹¹ Once there, Officer Evans “grabbed the tablet computer out of Mr. Frasier’s hands and began to search for the video of the arrest, asking [Frasier] where it

exercising his First Amendment right to film matters of public interest”); *Smith v. City of Cumming*, 212 F.3d 1332, 1333 (11th Cir. 2000) (“[Plaintiffs] had a First Amendment right, subject to reasonable time, manner and place restrictions, to photograph or videotape police conduct”); *Glik v. Cunniffe*, 655 F.3d 78, 82 (1st Cir. 2011) (“Basic First Amendment principles, along with case law from this and other circuits, answer [whether there is a constitutionally protected right to videotape police carrying out their duties in public] unambiguously in the affirmative”); *ACLU of Ill. v. Alvarez*, 679 F.3d 583, 595 (7th Cir. 2012) (entering an injunction to block the enforcement of an Illinois eavesdropping statute and holding that it likely violated the First Amendment because it was overly broad and impermissibly restricted “audio and audiovisual recording of utterances that occur in public”); *Turner v. Lieutenant Driver*, 848 F.3d 678, 688 (5th Cir. 2017) (“We conclude that First Amendment principles, controlling authority, and persuasive precedent demonstrate that a First Amendment right to record the police does exist, subject only to reasonable time, place, and manner restrictions”); *Fields v. City of Phila.*, 862 F.3d 353, 355–56 (3d Cir. 2017) (“Every Circuit Court of Appeals to address this issue (First, Fifth, Seventh, Ninth, and Eleventh) has held that there is a First Amendment right to record police activity in public. Today we join this growing consensus”) (citations omitted).

²⁰⁷ *Frasier v. Evans*, 992 F.3d 1003, 1015 (10th Cir. 2021).

²⁰⁸ *Id.* at 1008.

²⁰⁹ *Id.* at 1010.

²¹⁰ *Id.* at 1010–11.

²¹¹ *Id.* at 1011.

was.”²¹² Despite Frasier’s protests, Officer Evans continued searching the computer for “thirty to forty-five seconds” without finding the video of the arrest.²¹³ Finally, Officer Evans handed the tablet back to Frasier and allowed him to leave the parking lot.²¹⁴ Later, Frasier could not find the video on his tablet and publicly accused Officer Evans of deleting it.²¹⁵

In 2015, one year after the incident, Frasier filed a Section 1983 claim against the police officers individually for, among other claims, violating his First Amendment right to film the public activity of the police by retaliating against him for filming the arrest in the parking lot.²¹⁶ The officer defendants asserted a qualified immunity defense and moved to dismiss Frasier’s claim, arguing that the First Amendment right to record police officers performing their official duties was not clearly established when the incident occurred in August 2014.²¹⁷ Although the district court conceded that Frasier did not have a clearly established right to film a public arrest, it denied the defendants’ motion, as the record showed that the officers had knowledge of Frasier’s right to record from training they had received from the Denver Police Department.²¹⁸

On appeal, the Tenth Circuit reversed the ruling of the district court and reinstated the officers’ qualified immunity against the retaliation claim for two reasons.²¹⁹ First, the court stated that “a defendant’s eligibility for qualified immunity is judged by an objective standard and, therefore, what the officer defendants subjectively understood or believed the law to be was irrelevant with respect to the clearly-established-law question.”²²⁰ Had the pre-*Harlow* qualified immunity standard been used, each officer’s subjective understanding of the law would be directly relevant to the

²¹² *Id.*

²¹³ *Frasier*, 992 F.3d at 1011.

²¹⁴ *Id.*

²¹⁵ *Id.*

²¹⁶ *Id.*

²¹⁷ *Id.* at 1011–12.

²¹⁸ *Id.* at 1012.

²¹⁹ *Frasier*, 992 F.3d at 1015.

²²⁰ *Id.*

issue of whether the law was clearly established.²²¹ Second, the court held that when determining what constituted clearly established law, “judicial decisions are the only valid interpretive source.”²²² By limiting the inquiry to past judicial decisions, the court ignored the fact that the officers had received training about the right of bystanders to record public police activity.²²³ Based on the actions of the police officers, such as notifying fellow officers of Frasier’s recording, crowding around him after the scuffle, and searching his tablet for the video, the record showed that the officers may have understood that they were retaliating against Frasier for recording them, even though he may have had the right to do so.²²⁴ The Tenth Circuit’s test for qualified immunity completely ignores the motivations and knowledge of the law of the officers who assert it.

Interestingly, when addressing Frasier’s argument that the First Amendment right to record was clearly established, the court confined its discussion of the right to a single footnote in the decision.²²⁵ There, the court explained that it “[does] not consider, nor opine on, whether Mr. Frasier actually had a First Amendment right to record the police performing their official duties in public spaces....[The court] exercise[d its] discretion to bypass the constitutional question of whether such right even exists.”²²⁶ Punting on this determination of whether the right exists was permissible following the Supreme Court’s decision in *Pearson*. However, by doing so, the Tenth Circuit effectively precluded future plaintiffs from using this case as precedent to show that a right was clearly defined. Without judicial precedent showing that a right is

²²¹ See, e.g., *Wood v. Strickland*, 420 U.S. 308, 322 (1975) (describing the application of the pre-Harlow qualified immunity standard).

²²² *Frasier*, 992 F.3d at 1015.

²²³ *Id.*

²²⁴ See Jay Schweikert, *Tenth Circuit Grants Qualified Immunity to Police Who Knowingly Violated the First Amendment*, CATO INSTITUTE: CATO AT LIBERTY (Apr. 12, 2021, 2:04 PM), <https://www.cato.org/blog/tenth-circuit-grants-qualified-immunity-police-who-knowingly-violated-first-amendment> [<https://perma.cc/Y9GG-3AAM>].

²²⁵ *Frasier*, 992 F.3d at 1020 n.4.

²²⁶ *Id.*

clearly defined, a plaintiff will fail in showing that it is, and police officers will avoid liability.

IV. PROPOSED SOLUTIONS TO “COPYRIGHT HACKING”

“Copyright hacking” has the potential to harm members of the public who were excluded from both the “multiparty negotiation” that led to the passage of the DMCA²²⁷ and the licensing deals that resulted in major copyright holders participating in YouTube’s Content ID program.²²⁸ Ideally, any legislative or administrative solution would ban the practice of “copyright hacking” outright. However, should Congress or the Copyright Office fail to address “copyright hacking” directly, state actors, like police officers, who abuse this tactic must be held accountable for attempting to stifle speech. On this front, a judicial solution may also be appropriate.

A. Ex-Ante Legislative and Administrative Approaches to Prevent “Copyright Hacking”

One of the many difficulties in changing the copyright scheme is that the DMCA, as passed in 1998, already represents a tenuous compromise between the two major stakeholders.²²⁹ Any attempt to tip this balance back in favor of copyright owners would be met with fierce resistance by OSPs.²³⁰ Therefore, any change to the copyright scheme both has to preserve the DMCA safe harbors and has to affect copyright owners and OSPs equally. These two goals are diametrically opposed to one another. At first glance, the most

²²⁷ LITMAN, *supra* note 26, at 124 (“There is no overarching vision of the public interest animating the [DMCA]. None.”).

²²⁸ See Aswad, *supra* note 176.

²²⁹ See LITMAN, *supra* note 26, at 37.

²³⁰ For an example of a failed attempt to do just this, see LITMAN, *supra* note 26, at 182–84 (recounting the copyright owner lobbies’ attempt to overturn the judicial construction of the DMCA’s safe harbor provision in 2011 by proposing the Stop Online Piracy Act, which would have allowed copyright owners to serve notice on credit card companies and advertising services and force them to stop doing business with websites that facilitated infringement). Opposition from OSPs like Google and Wikipedia was fierce and the bill lost support in Congress. *Id.*

logical legislative solution to “copyright hacking” would be for Congress to amend the fair use section of the 1976 Copyright Act.²³¹ Currently, the statute states that “the fair use of a copyrighted work . . . for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright,” and lists four factors that a court must weigh when determining whether a use for an unenumerated purpose is fair.²³² Were Congress to amend the fair use section to state that “any copyrighted work included in a separate work due to the purposeful actions of a third-party, government’s agent is a fair use and not an infringement of copyright,” OSPs with copyright filtering systems would have to program their algorithms to discern whether a video’s copyrighted music is present due to infringement by the user or by an third-party actor operating in bad faith. On YouTube, however, the Content ID algorithm, rather than federal judges, determines whether a use is fair. Because filtering systems are not equipped to accurately detect fair use,²³³ adding an additional clause to the fair use section of the Copyright Act would be effectively useless. Social media companies have failed at far simpler content detection tasks in the past.²³⁴

²³¹ 17 U.S.C. § 107.

²³² *Id.* These four factors are “the purpose and character of the use . . . ; the nature of the copyrighted work; the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and the effect of the use upon the potential market for or value of the copyrighted work.” *Id.*

²³³ See *supra* note 180 and accompanying text.

²³⁴ See, e.g., Alex Heath, *A Facebook Bug Led to Increased Views of Harmful Content Over Six Months*, VERGE (Mar. 31, 2022), <https://www.theverge.com/2022/3/31/23004326/facebook-news-feed-downranking-integrity-bug> [<https://perma.cc/77S2-UWPZ>] (“A group of Facebook engineers identified a ‘massive ranking failure’ that exposed as much as half of all News Feed views to potential ‘integrity risks’ over the past six months, according to an internal report on the incident”); Ryan Mac, *Facebook Apologizes After A.I. Puts ‘Primates’ Label on Video of Black Men*, N.Y. TIMES (updated Oct. 4, 2021), <https://www.nytimes.com/2021/09/03/technology/facebook-ai-race-primates.html> [<https://perma.cc/C5N8-4TGK>] (“Facebook users who recently watched a video from a British tabloid featuring Black men saw an automated prompt from the social network that asked if they would like to ‘keep seeing videos about Primates.’”); Deepa Seetharaman et al., *Facebook Says AI Will Clean Up the Platform. Its Own Engineers Have Doubts.*, WALL ST. J. (Oct. 17,

Instead, a more practical legislative solution to “copyright hacking” would be to target the copyright filtering systems themselves. While the DMCA conditions an OSP’s safe harbor eligibility on the provider’s accommodation of STMs,²³⁵ the Copyright Office has concluded that no copyright filtering system currently qualifies as an STM,²³⁶ and has sought public comment²³⁷ and hosted stakeholder discussions²³⁸ about their future development and adoption. Separately, the Copyright Office has “convene[d] a series of consultations on technical measures [that are not STMs] for identifying or protecting copyrighted works online,” such as Content ID.²³⁹ Information gathered by the Copyright Office from the public and stakeholders will be useful to determine how to move forward with copyright filtering systems generally. But in order to address the narrower issue of “copyright hacking,” the Copyright Office should exercise its regulatory authority²⁴⁰ and

2021, 9:17 AM), <https://www.wsj.com/articles/facebook-ai-enforce-rules-engineers-doubtful-artificial-intelligence-11634338184> [<https://perma.cc/636H-DK5U>] (“Facebook’s AI can’t consistently identify first-person shooting videos, racist rants and even, in one notable episode that puzzled internal researchers for weeks, the difference between cockfighting and car crashes.”); Sapna Maheshwari, *On YouTube Kids, Startling Videos Slip Past Filters*, N.Y. TIMES (Nov. 4, 2017), <https://www.nytimes.com/2017/11/04/business/media/youtube-kids-paw-patrol.html> [<https://perma.cc/ZN9C-4DH5>] (“[V]ideos that are disturbing for children[, such as ‘Claymation Spider-Man urinating on Elsa of ‘Frozen’ and ‘Nick Jr. characters in a strip club,’] slip past [YouTube Kids] filters, either by mistake or because bad actors have found ways to fool the YouTube Kids algorithms.”).

²³⁵ See 17 U.S.C. § 512(i)(1)(B).

²³⁶ See *Section 512 Report*, *supra* note 67, at 176.

²³⁷ See Standard Technical Measures and Section 512, 87 Fed. Reg. 25049, 25051 (Apr. 27, 2022).

²³⁸ See *Standard Technical Measures Discussion Event*, U.S. COPYRIGHT OFFICE, <https://www.copyright.gov/events/stm-discussion/> [<https://perma.cc/6A95-CAEJ>] (last visited Nov. 28, 2022).

²³⁹ Technical Measures: Public Consultations, 86 Fed. Reg. 72,638 (Dec. 21, 2021). See also *Technical Measures Consultations*, U.S. COPYRIGHT OFFICE, <https://www.copyright.gov/policy/technical-measures/> [<https://perma.cc/6LMU-K5XQ>] (last visited Nov. 28, 2022).

²⁴⁰ See 17 U.S.C. § 702 (“The Register of Copyrights is authorized to establish regulations not inconsistent with law for the administration of the functions and duties made the responsibility of the Register under this title.”).

require OSPs to register their proprietary copyright filtering systems to study and to ensure that the filter's code accurately reflects the law. The Copyright Office could test these filters for compliance with the standards of fair use to protect the public from a would-be "copyright hacker," police officer or otherwise.

*B. An Ex-Post Judicial Solution to Hold Police Officers
Who "Copyright Hack" Accountable*

An ex-ante solution would stop "copyright hacking" before it happens by regulating the enabling infrastructure that allows it to occur in the first place. However, should this effort meet resistance from OSPs, there must be some legal mechanism that would allow victims of "copyright hacking" to hold police officers—like the ones described at the beginning of this Note—accountable. Given the velocity with which the internet continues to expand and evolve, it seems unlikely that slow-moving litigation will result in any timely changes to the federal copyright scheme.²⁴¹ The Supreme Court could address this problem by granting certiorari to a case that would resolve the circuit split created by the Tenth Circuit in *Frasier* and explicitly holding that recording public police activity is protected speech under the First Amendment.²⁴² In doing so, the Supreme Court would clearly establish the right to record, allowing individuals bringing Section 1983 claims against police officers for "copyright hacking" to get past the "clearly established right" prong of the *Harlow* qualified immunity standard. Thus, a plaintiff would only have to show that the officer violated this right by successfully

²⁴¹ See, e.g., Eriq Gardner, *A Landmark Legal Battle Over a Toddler Dancing to Prince Song Looks to Be Ending*, HOLLYWOOD REP. (June 6, 2018, 9:14 AM), <https://www.hollywoodreporter.com/business/business-news/a-landmark-legal-battle-a-toddler-dancing-prince-song-looks-be-ending-1117660/> [<https://perma.cc/5E7B-ASDC>] (describing the *Lenz* case, which culminated in a settlement after 11 years of litigation and appeals); Kaufman, *supra* note 157 (describing the settlement between YouTube and Viacom after seven years of litigation).

²⁴² Unfortunately, *Frasier* will not be the case in which the Court holds that the recording of public police activity is protected speech under the First Amendment, as the Court denied *Frasier*'s petition for a writ of certiorari on November 1, 2021. See *Frasier v. Evans*, 992 F.3d 1003 (10th Cir. 2021), *cert. denied*, 142 S. Ct. 427 (2021).

playing music to get the plaintiff's video removed from the internet. Allowing these claims to reach the second prong without being dismissed would also force federal courts to analyze the particular facts of each case and address whether "copyright hacking" constitutes a violation of the "right to record."²⁴³

CONCLUSION

The internet continues to grow.²⁴⁴ As more users come online, OSPs and major copyright owners will continue to fight over how to protect intellectual property. It is imperative that members of the public and their elected representatives pay attention to the compromises that the OSPs and copyright owners make, as these compromises may result in more automated copyright enforcement tools like Content ID. At the very least, the Supreme Court must modernize the First Amendment to provide members of the public some protection from bad actors who exploit these copyright filters by "copyright hacking;" holding that a "right to record" exists would be a modest and necessary step.

²⁴³ Holding that the "right to record" is protected speech has never been more urgent – at the time of this writing, bills effectively criminalizing the recording of the police have been signed into law in Arizona and Florida. *See* Shreya Tewari, *Arizona's New Law Banning People from Recording Police Violates our First Amendment Rights*, ACLU (Aug. 23, 2022), <https://www.aclu.org/news/free-speech/arizonas-new-law-banning-people-from-recording-police-violates-our-first-amendment-rights> [https://perma.cc/HNN2-CFME]; Trone Dowd, *Your Right to Film the Police Is Under Attack*, VICE (Mar. 25, 2022, 10:51 AM), <https://www.vice.com/en/article/g5qn57/filming-police-legality> [https://perma.cc/V5PW-RL8T].

²⁴⁴ *See Cisco Annual Internet Report (2018–2023) White Paper*, CISCO ANN. INTERNET REP., <https://www.cisco.com/c/en/us/solutions/collateral/executive-perspectives/annual-internet-report/white-paper-c11-741490.html> [https://perma.cc/CHL9-49XG] (last visited Nov. 28, 2022) ("[By 2023,] 66% of the [global] population will be using the Internet up from 51% in 2018[.]").