BOSTON UNIVERSITY SCHOOL OF LAW
JOURNAL OF SCIENCE & TECHNOLOGY LAW

CONTENTS

ARTICLES

NOTES

BOSTON UNIVERSITY
SCHOOL OF LAW

ADMINISTRATIVE OFFICERS

ROBERT A. BROWN, B.S., M.S., PH.D., *President*
ANGELA ONWUACHI-WILLIG, B.A., J.D., M.A., M.PHIL., PH.D., *Dean; Ryan Roth Gallo & Ernest J. Gallo Professor of Law*
MAUREEN A. O'ROURKE, B.S., J.D., *Dean Emerita; Professor of Law; Michaels Faculty Research Scholar*
JULIE A. DAHLSTROM, B.S., J.D., *Associate Dean for Experiential Education; Clinical Associate Professor of Law*
GERALDINE M. MUIR, B.A., M.S., J.D., *Associate Dean of Student Affairs*
ANNA DI ROBILANT, LL.B., LL.M., PH.D., S.J.D., *Associate Dean for Academic Affairs; Professor of Law; Law Alumni Scholar*
GARY S. LAWSON, B.A., J.D., *Associate Dean for Intellectual Life; Philip S. Beck Professor of Law*
CHRISTOPHER ROBERTSON, B.A., M.A., PH.D., J.D., *Associate Dean for Graduate & International Programs; Professor of Law; Professor of Health Law, Policy & Management, Boston University School of Public Health*
JASMINE GONZALES ROSE, B.A., J.D., *Associate Dean for Equity, Justice & Engagement; Professor of Law; Class of 1960 Scholar*
RONALD E. WHEELER, B.A., M.L.I.S., J.D., *Associate Dean, Fineman & Pappas Library; Associate Professor of Law & Legal Research*
JILL A. COLLINS, B.A., J.D., *Assistant Dean for Student Affairs*
ZACH DUBIN, B.A., M.B.A., *Assistant Dean for Development & Alumni Relations*
ELLEN FRENTZEN, B.A., M.L.I.S., J.D., LL.M., *Assistant Dean for Administration*
MANDIE LEBEAU, B.A., J.D., *Assistant Dean for Career Development & Public Service*
ALISSA R.E. LEONARD, A.B., *Assistant Dean for Admissions & Financial Aid*
JYOTHI NANDAKUMAR, *Assistant Dean for Finance*
CHRISTINA RICE, B.A., LL.M., J.D., *Assistant Dean for Graduate, International & Online Programs; Lecturer*
JOANNE A. THOMAS, B.S., M.A., *Assistant Dean for Marketing, Communications & Graduate Admissions*
ADAM KRUECKEBERG, B.A., M.A., M.B.A, *Vice Dean for Administration*

EMERITI FACULTY

MICHAEL S. BARAM, B.S., LL.B., *Professor of Law Emeritus*
MARY C. CONNAUGHTON, B.A., M.S.W., J.D., *Professor of Law Emerita*
STANLEY Z. FISHER, B.A., LL.B., *Professor of Law Emeritus*
TAMAR FRANKEL, DIPLOMA, LL.M., S.J.D., *Professor of Law Emerita*
WENDY J. GORDON, B.A., J.D., *Professor of Law Emerita*
MICHAEL C. HARPER, A.B., J.D., *Professor of Law Emeritus; Barreca Labor Relations Scholar*
NEIL S. HECHT, B.A., J.D., LL.M., J.S.D., *Professor of Law Emeritus*
WENDY KAPLAN, A.B., J.D., *Clinical Professor of Law Emerita*
SUSAN P. KONIAK, B.A., J.D., *Professor of Law Emerita*
PNINA LAHAV, LL.B., LL.M., J.S.D., M.A., *Professor of Law Emerita*
DAVID B. LYONS, B.A., M.A., PH.D., *Professor of Law Emeritus, Professor of Philosophy, Boston University College & Graduate School of Arts*
PEGGY MAISEL, B.A., M.A., J.D., M.A.T., *Professor of Law Emerita*
FRANCES H. MILLER, A.B., J.D., *Professor of Law Emerita*
EVA S. NILSEN, B.A., J.D., LL.M., *Clinical Associate Professor of Law Emerita*
DAVID ROSSMAN, B.A., J.D., *Professor of Law Emeritus*
LARRY W. YACKLE, A.B., J.D., LL.M., *Professor of Law Emeritus*

FACULTY

CLAIRE BISHOP ABELY, B.A., J.D., *Senior Lecturer*
AZIZA AHMED, B.A., M.S., J.D., *Professor of Law; N. Neale Pike Scholar, Co-Director, Boston University Law Program in Reproductive Justice*
ZOHRA AHMED, B.A., J.D., *Associate Professor of Law*
SUSAN M. AKRAM, B.A., J.D., M.ST., *Clinical Professor of Law*
GEORGE J. ANNAS, A.B., J.D., M.P.H., *Professor of Law; Chairman & William Fairfield Warren Distinguished Professor of Health Law, Bioethics & Human Rights, Boston University School of Public Health; Professor of Socio-Medical Sciences, Boston University School of Medicine*
JACK M. BEERMANN, B.A., J.D., *Philip S. Beck Professor of Law; Harry Elwood Warren Scholar*
JADE BROWN, B.S., J.D., *Clinical Associate Professor of Law*
JAMES E. BESSEN, A.B., *Lecturer, Executive Director of Technology & Policy Research Initiative; Director and Founder of Research on Innovation*
CONSTANCE A. BROWNE, B.A., J.D., *Clinical Associate Professor of Law*

MARNI GOLDSTEIN CAPUTO, B.A., J.D., *Senior Lecturer*
DANIELA CARUSO, LL.B., LL.M., PH.D., *Professor of Law; Jean Monnet European Union Professor*
KENT A. COIT, A.B., M.A., PH.D., J.D., *Director, Transactional Law Program; Professor of the Practice of Law*
MADISON CONDON, B.S., M.A., J.D., *Associate Professor of Law*
LAURA E. D'AMATO, B.A., J.D., *Director of Lawyering; Senior Lecturer*
STEVEN DEAN, B.A., J.D., *Professor of Law; Paul Siskind Research Scholar*
STACEY L. DOGAN, B.S., J.D., *Professor of Law; Law Alumni Scholar*
JONATHAN FEINGOLD, B.A., J.D., *Associate Professor of Law*
ALAN L. FELD, B.A., J.D., *Professor of Law; Maurice Poch Faculty Research Scholar*
JAMES E. FLEMING, A.B., A.M., J.D., PH.D., *The Honorable Paul J. Liacos Professor of Law*
LISA FREUDENHEIM, B.A., J.D., *Associate Professor of Law*
CAITLIN GLASS, B.A., J.D., *Visiting Lecturer and Clinical Instructor*
WOODROW HARTZOG, B.A., J.D., LL.M., PH.D., *Professor of Law; Class of 1960 Scholar*
SCOTT HIRST, B.COMM., LL.B., LL.M., S.J.D., *Associate Professor of Law*
NICOLE HUBERFELD, B.A., J.D., *Professor of Law; Professor of Health Law, Ethics & Human Rights, Boston University School of Public Health*
ILANA HURWITZ, B.A., LL.B., J.D., LL.M., *Professor of Law*
KEITH N. HYLTON, B.A., J.D., PH.D., *William Fairfield Warren Distinguished Professor; Professor of Law*
CODY JACOBS, B.A., J.D., LL.M, *Lecturer*
SEAN J. KEALY, A.B., M.G.A., J.D., *Clinical Associate Professor of Law*
STEVEN ARRIGG KOH, A.B., M.PHIL., J.D., *Associate Professor of Law; Gordon Butler Scholar in International Law*
GERALD F. LEONARD, A.B., PH.D., J.D., *Professor of Law; Law Alumni Scholar*
ARI LIPSITZ, B.F.A, J.D., *Lecturer and Clinical Instructor, BU/MIT Student Innovations Law Clinic*
KAREN PITA LOOR, B.S., J.D., *Clinical Professor of Law; Michaels Faculty Research Scholar*
KATHLEEN LUZ, B.A., J.D., *Senior Lecturer*
TRACEY MACLIN, B.A., J.D., *Professor of Law; Joseph Lipsitt Faculty Research Scholar*
NAOMI M. MANN, B.A., J.D., *Clinical Associate Professor of Law; Executive Director, Civil Litigation & Justice Program*
WENDY K. MARINER, B.A., J.D., LL.M., M.P.H., *Professor of Law; Edward R. Utley Professor of Health Law, Bioethics & Human Rights, Boston University School of Public Health; Professor of Medicine, Boston University School of Medicine*
STEPHEN G. MARKS, B.A., M.A., J.D., PH.D., *Professor of Law; Class of 1960 Scholar*
LINDA C. MCCLAIN, B.A., A.M., J.D., LL.M., *Robert Kent Professor of Law; Professor in the Women's, Gender & Sexuality Studies Program, Boston University College of Arts & Sciences*
JENNIFER TAYLOR MCCLOSKEY, B.A., J.D., *Director, Advocacy Program; Lecturer*
LIZ MCCUSKEY, B.A., J.D., *Professor of Health Law, Policy & Management*
MADELINE H. METH, B.A., J.D., *Clinical Associate Professor*
MICHAEL J. MEURER, S.B., S.B., J.D., PH.D., *Professor of Law; Abraham & Lillian Benton Scholar*
NANCY J. MOORE, B.A., J.D., *Professor of Law; Nancy E. Barton Scholar*
MARIA O'BRIEN, A.B., J.D., *Professor of Law; Paul Siskind Scholar*
NGOZI OKIDEGBE, B.A., B.C.L., LL.B., LL.M., *Moorman-Simon Interdisciplinary Career Development Associate Professor of Law; Assistant Professor of Computing & Data*
KEVIN OUTTERSON, B.S., J.D., LL.M., *Professor of Law; Austin B. Fletcher Professor of Law; Executive Director, CARB-X*
WILLIAM W. PARK, B.A., J.D., M.A., *Professor of Law; R. Gordon Butler Scholar in International Law*
PORTIA PEDRO, B.A., J.D., PH.D., *Associate Professor of Law*
DANIELLE PELFREY DURYEA, B.A., M.A., J.D., LL.M., *Director, Compliance Policy Clinic; Clinical Instructor; Lecturer*
ANGELO PETRIGH, B.A., J.D., *Clinical Associate Professor*
BENJAMIN DAVID PYLE, B.A., M.A.E., J.D., PH.D., *Associate Professor of Law*
JARROD F. REICH, B.A., J.D., *Senior Lecturer*
CHRISTOPHER ROBERTSON, B.A., M.A., PH.D., J.D., *Associate Dean for Strategic Initiatives; Professor of Law*
VICTORIA SAHANI, A.B., J.D., *Associate Provost for Community & Inclusion; Professor of Law*
DAVID J. SEIPP, A.B., B.A., LL.B., J.D., *Professor of Law; Law Alumni Scholar*
ANDREW SELLARS, B.S., J.D., *Director, Technology Law Clinic; Clinical Associate Professor of Law*
SARAH R. SHERMAN-STOKES, B.A., J.D., *Associate Director, Immigrants' Rights & Human Trafficking Clinic; Clinical Associate Professor of Law*
JED HANDELSMEN SHUGERMAN, B.A., J.D., PH.D., *Professor of Law; Joseph Lipsitt Scholar*
KATHARINE B. SILBAUGH, B.A., J.D., *Professor of Law; Law Alumni Scholar*
JESSICA SILBEY, B.A., J.D., PH.D., *Professor of Law; Yanakakis Faculty Research Scholar*
THEODORE S. SIMS, A.B., J.D., PH.D., *Professor of Law*
ROBERT D. SLOANE, B.A., J.D., *Professor of Law; R. Gordon Butler Scholar in International Law*
PAUL SWEENEY, *Director of the Transactional Law Program*
MAYA STEINITZ, LL.B., LL.M., J.S.D., *Professor of Law; R. Gordon Butler Scholar in International Law*
JOHN D. SULLIVAN, B.A., M.B.A., A.M., PH.D., *Associate Professor & Chair of Administrative Sciences at MET*
ROBERT L. TSAI, B.A., J.D., *Professor of Law; Law Alumni Scholar*
FREDERICK TUNG, A.B., J.D., *Professor of Law; Howard Zhang Faculty Research Scholar*

MICHAEL ULRICH, B.S., J.D., M.P.H., *Assistant Professor of Health Law, Ethics & Humans Rights, Health Law Policy & Management, Boston University School of Public Health*
RORY VAN LOO, B.A., J.D., PH.D., *Professor of Law; Michaels Faculty Research Scholar*
GIGI HODO WALKER, B.A., ME.D., J.D., *Senior Lecturer*
DAVID I. WALKER, B.E., J.D., *Professor of Law; Maurice Poch Faculty Research Scholar*
JAY D. WEXLER, B.A., M.A., J.D., *Professor of Law; Michaels Faculty Research Scholar*
DAVID H. WEBBER, B.A., J.D., *Professor of Law; Paul M. Siskind Scholar*
KATHRYN ZEILER, B.S., M.S., M.S., J.D., PH.D., *Professor of Law; Nancy E. Barton Scholar*

BOSTON UNIVERSITY SCHOOL OF LAW
JOURNAL OF SCIENCE & TECHNOLOGY LAW

VOLUME 30 **2023 – 2024**

EDITORIAL BOARD

GENERAL INFORMATION

The Boston University Journal of Science & Technology Law publishes two issues annually. The Journal also distributes its articles, notes, legal updates, and other published subject matter on LEXIS®-NEXIS® and WESTLAW®. Articles are available on the Journal's web page, found at: https://www.bu.edu/jostl/archives/.

Publication of the Journal is solely the responsibility of its membership, consisting of second- and third-year students at the Boston University School of Law. An Editorial Board consisting of third year members coordinates the Journal's activities. Please cite to this volume of the Journal of Science & Technology Law as 28 B.U. J. SCI. & TECH. L. 1 (2022).

Articles and other information are available on the Journal's website: https://www.bu.edu/jostl/.

CORRESPONDENCE

Address all correspondence regarding subscriptions, address changes, claims for non-receipt, single copies, advertising, and permission to reprint to Journal of Science & Technology Law, Administrative Editor, Boston University School of Law, 765 Commonwealth Avenue, Boston, Massachusetts 02215. Telephone: 617-353-8368. Facsimile: 617-353-8369. E-mail: jostl@bu.edu.

SUBSCRIPTIONS

Annual subscriptions are $50 for domestic subscribers and $55 for international subscribers. Please allow two weeks for delivery. Payment may be made by check, or international money order. Domestic claims for non-receipt of issues should be made within 90 days of the month of publication; overseas claims should be made within 180 days. Thereafter, the regular back-issue rate ($25 per issue (domestic), $27.50 (international)) will be charged for replacement. Overseas delivery is not guaranteed.

BACK ISSUES

Back issues may be ordered directly from William S. Hein & Co., Inc., 1285 Main Street, Buffalo, New York 14209-1987. Orders may also be placed by calling Hein at (800) 828-7571, via fax at (716) 883-8100, or email to order@wshein.com. Back issues can also be found in electronic format for all your research needs on HeinOnline at http://heinonline.org/.

SUBMISSIONS

The Editorial Board for the Journal of Science & Technology Law invites the submission of unsolicited manuscripts. Submissions may include previously unpublished articles, essays, case notes, or comments concerning any aspect of the relationship between science, technology, and the law. If any part of a manuscript has been previously published, the author should so indicate. In addition, the author should include their credentials, including full name, degrees earned, academic or professional affiliations, and citations to all previously published legal articles. Please send manuscripts for consideration to the Managing Editors via the Expresso website at http://law.bepress.com/expresso/. Correspondence to the Journal of Science & Technology Law may be addressed to jostl@bu.edu.

FORMAT AND CITATIONS

Manuscripts should be double-spaced with one-inch margins. We regret that submissions cannot be returned. Authors should retain an exact copy of any material submitted. Electronic documents should be submitted in Microsoft Word® format. All citations should conform to The Bluebook: A Uniform System of Citation (21st ed. 2020).

COPYRIGHTED MATERIAL

If material contains any copyrighted table, chart, graph, illustration, photograph, or more than eight lines of text, the author must obtain written permission from the copyright holder for use of the material. A photocopy of such written permission should accompany the submission.

CONFLICT OF INTEREST

Authors should disclose at the time of submission any financial, consulting, or other arrangement they may have with a company or organization whose products or interests figure prominently in the submitted manuscript. This information will be held in confidence while the paper is under review and will not influence the editorial decision. If such a paper is accepted for publication, the editor will discuss with the author(s) the way such information will be disclosed to the reader.

ARTICLE

PRIVACY'S ALGORITHMIC TURN

MARÍA P. ANGEL*

ABSTRACT

As algorithms have taken over contemporary society, a portion of American privacy law scholars has gradually transformed information privacy into a post-algorithmic concept. Besides enabling individuals to protect their autonomy and attain certain collective benefits, these scholars now expect information privacy to act as the government's tool to protect society against data extraction and its consequent power asymmetries. This Article presents evidence of this transformation—here referred to as "privacy's algorithmic turn"—, identifying its two main features: (1) a change in what is usually considered privacy harms, and (2) a transformation of the tools proposed to protect privacy. Additionally, the Article explores some possible drivers and implications of this new development. Time will tell if privacy's algorithmic turn was worthwhile. For now, acknowledging its existence gives American privacy law scholars the opportunity to reflect on their journey and the future directions they want the field to pursue.

CONTENTS

* Ph.D. in Law Candidate at the University of Washington School of Law. Support for this research came from the Tech Policy Lab at the University of Washington, where the author works as a Research Assistant. The author would like to thank the attendees of the Privacy Research Group ("PRG") at the NYU Information Law Institute and the 2023 Privacy Law Scholars Conference ("PLSC") for their insightful comments on earlier versions of this article; as well as Ryan Calo and Megan Finn for their judicious feedback and comments.

INTRODUCTION

In 2003 Paul M. Schwartz and William Michael Treanor published an article titled *The New Privacy*. By the beginning of the 21st century—the authors suggest—theoretical work both within and outside the American legal academy pointed to the development of a "new privacy," designed to protect autonomy and centered primarily around the Fair Information Practices ("FIPs").[1]

It has been twenty years since Schwartz and Treanor described this phenomenon. In these past two decades, massive sociotechnical change has taken place, the Privacy Law Scholars Conference ("PLSC") was born in the United States, and American privacy law scholars have written extensively about emerging information technologies. In the context of the transition to artificial intelligence ("AI") and algorithmic decision-making systems, a large portion of scholars presenting articles at PLSC have begun to consider new privacy harms. For example, there is now a growing recognition that privacy harms include issues such as algorithmic discrimination (unfairness), online manipulation, and procedural injustices perpetuated by automated decision-making. Accordingly, scholars have gradually begun to reject the FIPs as ineffective or inadequate tools. In their place, they are now calling for more holistic approaches that include, among other tools, substantive rules and prohibitions rather than simply procedural requirements.

The time has come to describe this new development in American privacy law scholarship. This Article aims to meet this goal. Building on the concept of

[1] Paul Schwartz & William Michael Treanor, *The New Privacy*, 101 MICH. L. REV. 2163, 2164 (2003).

"algorithmic turn" proposed by Lilian Edwards and Michael Veale,[2] Ifeoma Ajunwa,[3] and Woodrow Hartzog,[4] and inspired by the "computational turn" described by Mireille Hildebrandt and Katja De Vries,[5] it presents evidence of an emerging transformation of the concept of information privacy in a considerable portion of American privacy law scholarship presented at PLSC.

PLSC "is *the premier gathering* of privacy scholars, researchers, and practitioners in the world."[6] It is a paper workshop conference that has been taking place in the United States since 2008, annually assembling a wide array of scholars and practitioners who engage in scholarship "in privacy, broadly defined."[7] According to its charter, "[a]t PLSC's core is work related to privacy law, including work in the humanities and social sciences, computer and data science, and other fields."[8] Julie Cohen, Priscilla Regan, Paul Schwartz, and Daniel Solove—who Schwartz and Treanor mention as part of the "new privacy"[9]—would become active members (or even co-founders, as was the case of Daniel Solove) of this community, joined by several other established and emerging privacy scholars.

In order to advance this project, I conducted document analysis of the papers workshopped at PLSC between 2008 and 2020 that ended up being published up to 2022[10] or are available online as drafts.[11] Likewise, when necessary, I have included additional articles and, in some few cases, books that, although not part of the initial sample, were also authored by the authors presenting at PLSC. These additional materials provide a more comprehensive picture of the regulatory approaches and theoretical stances of these scholars.[12]

---

[2] Lilian Edwards & Michael Veale, *Slave to the Algorithm? Why a 'Right to an Explanation' Is Probably Not the Remedy You Are Looking For*, 16 DUKE L. & TECH. REV. 18, 24 (2017).

[3] Ifeoma Ajunwa, *The Paradox of Automation as Anti-Bias Intervention*, 41 CARDOZO L. REV. 1671, 1683 (2020).

[4] Woodrow Hartzog, *What is Privacy? That's the Wrong Question*, 88 U. CHI. L. REV. 1677, 1681 (2021).

[5] Mireille Hildebrandt & Katja De Vries, *Privacy, Due Process and the Computational Turn at a Glance*, *in* PRIVACY, DUE PROCESS AND THE COMPUTATIONAL TURN (Mireille Hildebrandt & Katja De Vries eds., 2013).

[6] PRIV. L. SCHOLARS CONF. (emphasis added), https://privacyscholars.org/ [https://perma.cc/KKU2-F2JA].

[7] *PLSC Charter*, PRIV. L. SCHOLARS CONF., https://privacyscholars.org/about-us/plsc-charter/ [https://perma.cc/QTZ9-9XWK].

[8] *Id*.

[9] Schwartz & Treanor, *supra* note 1, at 2177.

[10] Either as an article or a book chapter.

[11] For example, when they are accessible on SSRN. However, I excluded drafts with a clear "do not cite" restriction.

[12] This Article is part of a larger research project on the Intellectual History of American Privacy Law Scholarship. As part of this project, I also conducted oral history interviews with a purposely drawn representative sample of fifteen American privacy law scholars.

For this research, I was especially interested in analyzing PLSC articles focused on information privacy in—mostly—commercial contexts. Therefore, I largely avoided studying papers on the Fifth Amendment, the Fourth Amendment, government surveillance, intellectual property, the right to publicity, and decisional privacy. To conduct the analysis, I took a Grounded Theory approach and drew on the methodological framework of Intellectual History. In particular, I used the discursive contextual approach proposed by David A. Hollinger[13] to trace the algorithmic turn in the PLSC community's discourse about information privacy.

As will be seen, the two main features that characterize this turn are: (1) a change in what is usually considered privacy harms, and consequently, (2) a transformation of the tools proposed to protect privacy. As algorithms have taken over contemporary society, a considerable group of American privacy law scholars have gradually transformed information privacy into a post-algorithmic concept. Besides enabling individuals to protect their autonomy and attain certain collective benefits,[14] these scholars now expect information privacy to act as the government's tool to protect society against data extraction and its consequent power asymmetries.

This Article also explores some possible sociotechnical drivers and implications of the turn. Reasons can range from the simple appreciation of privacy law as a useful shorthand tool at hand in the algorithmic age, to a radical change in American legal scholars' techno-legal imaginaries. Halfway down this spectrum, other possible causes include American scholars' efforts to play catch-up to European data protection regulations, a win-win strategic movement to find cognizable harms and increase privacy's moral significance, and novel dimensions of data that algorithms have made particularly salient, calling for a concept reformulation. Implications, in turn, include a potential threat to information privacy's instrumental efficacy (in favor of its symbolic value), the emergence of a new privacy paradigm, and an open window for impact on American public policy about privacy.

This Article, however, focuses exclusively on the data collected through the analysis of documents. Future research will take into account the information obtained from the interviews.

[13] *See* DAVID A. HOLLINGER, IN THE AMERICAN PROVINCE: STUDIES IN THE HISTORY AND HISTORIOGRAPHY OF IDEAS (1985). To gain a deeper understanding of this methodological framework and how it was used in this research project, *see* María P. Angel, Privacy's Algorithmic Turn: An Intellectual History (2024) (Ph.D. dissertation, University of Washington).

[14] As Schwartz and Treanor aptly describe the participants of the "new privacy" "reject[ed] privacy as an individual right of control." Instead, these authors argued that privacy is a kind of social good. Schwarz & Treanor, *supra* note 1, at 2179. In that sense, around the 2000's, a big chunk of American privacy law scholars saw privacy not simply as an individual right, but as a social value and a necessary precondition for community. They considered that autonomy generates concrete collective benefits such as the rule of civility (Robert Post), democracy (Paul Schwartz and Ruth Gavison), civil society, innovation, and creativity (Julie Cohen), or intellectual activities and a free society (Neil Richards). *See generally id.*

The community of scholars that has developed over the years around PLSC is not necessarily defined[15] and may not be representative of the full community of privacy law scholars in the United States. Therefore, this article does not intend to generalize its findings to American privacy law scholarship as a whole. Nevertheless, given the significance of this conference in the evolution of the field, recognizing this algorithmic turn seems worthwhile. Likewise, the fact that this transformation is described here as a "turn," which semantically refers to a change of direction when moving, does not mean that it has been radical. As will be seen, it was more of a gradual, progressive, and in many cases imperceptible change of approach and priorities—which seems to be still unfolding.

The Article proceeds as follows. Part I traces the algorithmic turn in contemporary society. Against this contextual backdrop, Part II describes privacy's algorithmic turn in the scholarship of a considerable portion of the PLSC community. It explores its main features as well as its outliers. Finally, Part III inquires as to the possible sociotechnical drivers and implications of this transformation in the conception of information privacy held by a significant group of American privacy law scholars.

I. THE ALGORITHMIC TURN IN CONTEMPORARY SOCIETY

Over the last few years, several privacy law scholars around the world have called attention to the influence algorithms have had on contemporary society. As early as 2013, Mireille Hildebrandt and Katja De Vries employed the concept of "computational turn" to refer to this dynamic.[16] While proposing three different notions of the concept, the societal-phenomenon one is characterized as "an umbrella term to describe the recent avalanche of governmentalities . . . which act through machine learning and data mining techniques. These computational governmentalities blossom in both the private and public sector."[17]

Building on this definition, in 2017 Lilian Edwards and Michael Veale employed the term "algorithmic turn" to refer to "the use of technologies that do not model broad or abstract phenomena such as the climate, the economy or urban traffic, but model varied entities—usually people, groups or firms."[18] Similarly, in 2020 Ifeoma Ajunwa proposed this expression to signal "the profusion of algorithmic decision-making in our daily lives, even in the absence of established regulatory or ethical frameworks to guide the deployment of those algorithms."[19]

---

[15] For different reasons, some scholars who used to attend PLSC have stopped attending. Similarly, although until 2020 participation to the conference was by invitation only, it has recently moved to an open format where not only is the call for papers open to all, but people can attend/register without an invitation. Therefore, as time passes, PLSC has become bigger and its borders harder to determine.

[16] *See* Hildebrandt & De Vries, *supra* note 5.

[17] *Id*. at 14-15.

[18] Edwards & Veale, *supra* note 2, at 24.

[19] Ajunwa, *supra* note 3, at 1683-84.

In this Article, I contend that the scholarship of a significant portion of American privacy law scholars has undergone its own algorithmic turn. This claim, however, needs to be substantiated by describing first what the algorithmic turn—as originally proposed by others—entails.

As Professors Edwards, Veale, and Ajunwa have aptly highlighted, we are currently facing the ubiquity of algorithmic technologies. We are now "in a society that increasingly functions thanks to algorithms."[20] And even more, we find ourselves amid what Ed Finn describes as the *age of the algorithm*: "the era dominated by the figure of the algorithm as an ontological structure for understanding the universe."[21] Whether we believe in it or not, we are all driven by the idea (also known as the *effective computability argument*) that any "problem—whether it is agriculture or square root extraction—can be solved by following the steps of the method,"[22] meaning, by an algorithm.

To be clear, algorithms are not new. Defined as "a set of rules that precisely define a sequence of operations,"[23] they have been in use since around 1600 BC, when the first-known algorithm was developed in ancient Babylon.[24] However, it was by being coupled with electronic and general purpose computers in the 1940s that algorithms came to show their potential.[25] The fact that we can program a computer to execute an algorithm means that the rules or steps that the algorithm is composed of will be followed a lot faster. "An algorithm gains power on a computer because it can be executed there in a fraction of the time it would take us to perform the same steps, *but they are still the same steps*."[26]

Computers were just the first factor in a row. Just as Gordon Moore accurately predicted in 1965, the number of transistors in a processor has been doubling about every two years. Accordingly, we went "from about 2,000 transistors in a processor in 1971 (the Intel 4004) to more than 19 billion in 2017 (the 32-core AMD Epyc)."[27] In addition, around 2010 most of us were here to witness the big data revolution.[28] And as time passes, "hardware engineers are designing better

[20] LOURIDAS, ALGORITHMS xv (2020).

[21] ED FINN, WHAT ALGORITHMS WANT: IMAGINATION IN THE AGE OF COMPUTING 21 (2017).

[22] *Id*. at 53.

[23] HAROLD S. STONE, INTRODUCTION TO COMPUTER ORGANIZATION AND DATA STRUCTURE xx (1971). Similarly, Louridas defines them as "a set of steps that you can follow with pen and paper." *See* LOURIDAS, *supra* note 20, at 5.

[24] DONALD KNUTH, THE ART OF COMPUTER PROGRAMMING 318 (2d ed. 1981).

[25] *See* LOURIDAS, *supra* note 20.

[26] *Id*. at 23 (emphasis in original).

[27] *Id*. at 36-37.

[28] With the web came the development of browsers (X Mosaic, Netscape Navigator, Internet Explorer, etc.), software applications that allowed people to navigate the web. And with them, the first wave of dot-com companies began to emerge in domains such as search (e.g., Yahoo!, Excite, Lycos, Infoseek, Altavista), ecommerce (e.g., Amazon, eBay), and media, with digital advertising as their revenue engine. In the years after the dot-com bubble burst (2000), additional companies such as Google, Apple, Netflix, PayPal, and Facebook—which

and better chips to run more and more neural computations faster while using less computer power."[29]

As should come as no surprise to anyone today, algorithms are part of the "building blocks"[30] of the popular AI systems we hear about so often today. As Gary Marcus and Ernest Davis point out, "[m]uch of th[e] recent success in AI has been driven largely by two factors: first, advances in hardware, which allow for more memory and faster computation, often by exploiting many machines working in parallel; second, big data, ..."[31] Furthermore—Marcus and Davis add—a type of machine learning algorithm known as *deep learning*[32] has turned into a key player in this success. According to these authors,

> Deep learning has been at the center of practically every advance in AI in the last several years, from DeepMind's superhuman Go and chess player AlphaZero to Google's recent tool for conversation and speech synthesis, Google Duplex. In each case, big data plus deep learning plus faster hardware has been a winning formula.[33]

Thanks to these different factors, we are now witnessing an explosion of investment, research, development, commercialization, and use of AI and algorithmic decision-making systems in every corner of society. All of this is apparently supported by a common belief about algorithms: "They're faster than us, they're cheaper than us, and, when things work as they should, they make far fewer mistakes than we do."[34]

In this Part, I offer a brief description of the world we find ourselves in today in relation to algorithms, both in our day-to-day and in regulatory spaces. Hopefully, this broader panorama will allow us to have a better understanding of the contextual background against which a considerable portion of American privacy law scholarship ended up having its own algorithmic turn.

---

had been launched or regained force while the bubble was growing—would take over the Internet, leading us into the big data revolution. *See* BRIAN MCCULLOUGH, HOW THE INTERNET HAPPENED (2018).

[29] LOURIDAS, *supra* note 20 at 229-30.

[30] DEF. SCI. & TECH. LAB'Y, MINISTRY OF DEF., BUILDING BLOCKS FOR ARTIFICIAL INTELLIGENCE AND AUTONOMY (2020).

[31] GARY MARCUS & ERNEST DAVIS, REBOOTING AI: BUILDING ARTIFICIAL INTELLIGENCE WE CAN TRUST 10 (2019).

[32] Deep learning algorithms rely on two key ideas: hierarchical pattern recognition and learning. They are used to train four or more layers in a neural network. Their "forte is working with millions or billions of data points, gradually landing on a set of neural network weights that will capture the relations between those examples." *Id*. at 56.

[33] *Id*. at 10.

[34] CHRISTOPHER STEINER, AUTOMATE THIS: HOW ALGORITHMS TOOK OVER MARKETS, OUR JOBS, AND THE WORLD 6 (2013).

A. Our day-to-day life

Today, social media platforms, such as Facebook, Twitter, and TikTok, use algorithms to run their recommendation engines, shaping our perceived reality.[35] Algorithms are also used by the owners of these platforms to moderate content, as well as to deliver ads for commercial products and employment, housing, and credit opportunities.[36]

And despite being the most commonly known users of algorithms, social media platforms are far from being the only ones. Ride sharing companies like Uber and Lyft implement dynamic pricing algorithms to determine the price we end up paying for a ride.[37] Insurance companies employ algorithms containing dozens of variables to run their risk models and charge us premiums.[38] Banks, fintech start-ups, and digital mortgage platforms alike use algorithms to predict how well we, as prospect lenders, will perform on a loan and to maximize profit.[39] Similarly, the tenant screening industry offers algorithms that conduct background checks of prospective tenants based on criminal, eviction, and credit histories,[40] or recommend rents of open apartments to landlords.[41] Recruiting companies even use algorithms to review job applications.[42]

[35] *See* Olivia Little & Abbie Richards, *TikTok's Algorithm Leads Users From Transphobic Videos to Far-Right Rabbit Holes*, MEDIA MATTERS FOR AM. (Oct. 5, 2021, 9:03 AM), https://www.mediamatters.org/tiktok/tiktoks-algorithm-leads-users-transphobic-videos-far-right-rabbit-holes [https://perma.cc/99CT-3J4P].

[36] *See* Kate Cox, *New Google Rule Bans Discriminatory Targeting for House Ads,* ARS TECHNICA (June 12, 2020, 12:26 PM), https://arstechnica.com/tech-policy/2020/06/new-google-rule-bans-discriminatory-targeting-for-housing-ads/ [https://perma.cc/3KAY-EE3E].

[37] *See* Kyle Wiggers, *Researchers Find Racial Discrimination in "Dynamic Pricing" Algorithms Used By Lyft, Uber and Others*, VENTUREBEAT (June 12, 2020, 7:30 AM), https://venturebeat.com/ai/researchers-find-racial-discrimination-in-dynamic-pricing-algorithms-used-by-uber-lyft-and-others/ [https://perma.cc/PKW3-XC89].

[38] *See* Maddy Varner & Adam Sankin, *Suckers List: How Allstate's Secret Auto Insurance Algorithm Squeezes Big Spenders,* MARKUP (Feb. 25, 2020, 5:00 AM), https://themarkup.org/allstates-algorithm/2020/02/25/car-insurance-suckers-list [https://perma.cc/TS36-VNRW].

[39] *See* Jennifer Miller, *Is an Algorithm Less Racist Than a Loan Officer,* N.Y. TIMES (Sept. 18, 2020), https://www.nytimes.com/2020/09/18/business/digital-mortgages.html [https://perma.cc/2JMA-B582].

[40] *See* Lauren Kirchner & Matthew Goldstein, *Access Denied: Faulty Automated Background Checks Freeze Out Renters,* MARKUP (May 28, 2020, 5:00), https://themarkup.org/locked-out/2020/05/28/access-denied-faulty-automated-background-checks-freeze-out-renters [https://perma.cc/E7US-8ZSY].

[41] *See* Heather Vogell, *Rent Going Up? One Company's Algorithm Could Be Why*, PROPUBLICA (Oct. 15, 2022, 5:00 AM), https://www.propublica.org/article/yieldstar-rent-increase-realpage-rent [https://perma.cc/3JPU-TM8G].

[42] Hilke Schellman, *Finding It Hard to Get a New Job? Robot Recruiters Might Be to Blame*, GUARDIAN (May 11, 2020, 4:30 PM), https://www.theguardian.com/us-

At a societal level, algorithms can be found in healthcare, education, and the workplace, to name just a few scenarios.[43] The healthcare system continually uses algorithms to make decisions about care, such as kidney allocation and C-section administration.[44] The US largest electronic health record vendor, EPIC, developed an algorithm to predict length of hospital stay, who may become seriously ill, and who may fail to show up for medical appointments.[45] According to STAT News, "[a]rtificial intelligence (AI) is being used in health care to flag abnormalities in head CT scans, cull actionable information from electronic health records, and help patients understand their symptoms."[46]

Similarly, if we take a look at education, we easily find that schools employ admissions screening tools powered by algorithms.[47] They also use these tools to scan student emails and flag words that could indicate potential problems.[48] Schools have even used algorithms to assign "predicted" grades to students.[49] And when it comes to universities, algorithms have also been deployed to

news/2022/may/11/artitifical-intelligence-job-applications-screen-robot-recruiters [https://perma.cc/E3HE-PNQX].

[43] LYDIA X. BROWN, RIDHI SHETTY, MATTHEW U. SCHERER & ANDREW CRAWFORD, CTR. FOR DEMOCRACY & TECH., ABLEISM AND DISABILITY DISCRIMINATION IN NEW SURVEILLANCE TECHNOLOGIES 5 (2022), https://cdt.org/wp-content/uploads/2022/05/2022-05-23-CDT-Ableism-and-Disability-Discrimination-in-New-Surveillance-Technologies-report-final-redu.pdf [https://perma.cc/XH8W-ESVL].

[44] Sharon Begley, *Racial Bias Skews Algorithms Widely Used to Guide Care from Heart Surgery to Birth, Study Finds*, STAT (June 17, 2020), https://www.statnews.com/2020/06/17/racial-bias-skews-algorithms-widely-used-to-guide-patient-care/ [https://perma.cc/A2BF-WQF4]; *see also* Tom Simonite, *Lawmakers Demand Scrutiny of Racial Bias in Health Algorithms*, WIRED (Sept. 24, 2020, 10:00 AM), https://www.wired.com/story/lawmakers-demand-scrutiny-racial-bias-health-algorithms/ [https://perma.cc/GH49-TU8E].

[45] Casey Ross, *Epic's AI Algorithms, Shielded from Scrutiny by a Corporate Firewall, Are Delivering Inaccurate Information on Seriously Ill Patients*, STAT (July 26, 2021), https://www.statnews.com/2021/07/26/epic-hospital-algorithms-sepsis-investigation/ [https://perma.cc/F93W-EPTW].

[46] Saurabh Jha, *Can You Sue an Algorithm for Malpractice? It Depends*, STAT (Mar. 9, 2020), https://www.statnews.com/2020/03/09/can-you-sue-artificial-intelligence-algorithm-for-malpractice/ [https://perma.cc/G3WF-H6Z5].

[47] Colin Lecher & Maddy Varner, *NYC's School Algorithms Cement Segregation. This Data Shows How*, CITY (May 26, 2021, 8:00 AM), https://www.thecity.nyc/2021/5/26/22453952/nyc-high-school-algorithms-segregation [https://perma.cc/2NNG-9WRD].

[48] Mark Keierleber, *A Boy Wrote About His Suicide Attempt. He Didn't Realize His School's Gaggle Software Was Watching*, GUARDIAN (Oct. 12, 2021, 7:15), https://www.theguardian.com/education/2021/oct/12/school-surveillance-dragnet-suicide-attempt-healing [https://perma.cc/F8GN-XM39].

[49] Meredith Broussard, *When Algorithms Give Real Students Imaginary Grades*, N.Y. TIMES (Sept. 8, 2020), https://www.nytimes.com/2020/09/08/opinion/international-baccalaureate-algorithm-grades.html [https://perma.cc/4894-JEDL].

predict, for example, how likely a student is to drop out of school if she remains within her selected major.[50] Likewise, they have been implemented to predict the probability of the admissions committee of a Ph.D. program approving an applicant.[51] And, in the wake of remote learning, colleges and universities have turned to algorithmic proctoring tools to monitor students during tests.[52]

Algorithms are also increasingly integrated into the workplaces and labor processes (so-called "algorithmic management").[53] Gig work companies, for instance, use opaque algorithms for rating employees, scheduling shifts, and governing their pay models.[54] Likewise, algorithms play a key role in tracking workers' productivity,[55] predicting drivers' safety,[56] and optimizing delivery routes.[57] Similarly, other companies use algorithmic systems to score stores and logistic warehouses to determine risk of employees unionizing.[58] And other sectors and occupations have not escaped from this trend either. Against the

[50] Todd Feathers, *Major Universities Are Using Race as a "High Impact Predictor" of Student Success*, MARKUP (Mar. 2, 2021, 8:00), https://themarkup.org/machine-learning/2021/03/02/major-universities-are-using-race-as-a-high-impact-predictor-of-student-success [https://perma.cc/2RY4-BGX5].

[51] Lilah Burke, *The Death and Life of an Admissions Algorithm*, INSIDE HIGHER ED (Dec. 13, 2020), https://www.insidehighered.com/admissions/article/2020/12/14/u-texas-will-stop-using-controversial-algorithm-evaluate-phd [https://perma.cc/N9BN-QJL3].

[52] Shea Swauger, *Software That Monitors Students During Tests Perpetuates Inequality And Violates Their Privacy*, MIT TECH. REV. (Aug. 7, 2020), https://www.technologyreview.com/2020/08/07/1006132/software-algorithms-proctoring-online-tests-ai-ethics/ [https://perma.cc/6JYB-LRW7].

[53] AIHA NGUYEN, DATA & SOC'Y, THE CONSTANT BOSS: WORK UNDER DIGITAL SURVEILLANCE (2021), https://datasociety.net/wp-content/uploads/2021/05/The_Constant_Boss.pdf [https://perma.cc/S663-LKS3].

[54] Bryan Menegus, *'Every Single Person Is Losing Money': Shipt is the Latest Gig Platform to Screw Its Workers*, GIZMODO (Feb. 12, 2020), https://gizmodo.com/targets-shipt-pay-model-change-cuts-worker-pay-shipter-1841620656 [https://perma.cc/HG3Z-LC9Q].

[55] Luis F. Leon, *Regulating Amazon's Warehouse Algorithms Is About More Than Injuries*, NEW REPUBLIC (Sept. 8, 2021), https://newrepublic.com/article/163588/amazon-warehouse-algorithms-injuries-california-bill [https://perma.cc/8SHR-9DTH].

[56] Belle Lin, *Uber Patents Reveal Experiments With Predictive Algorithms To Identify Risky Drivers*, INTERCEPT (Oct. 30, 2021, 8:00 AM), https://theintercept.com/2021/10/30/uber-patent-driver-risk-algorithms/ [https://perma.cc/5M3U-V86Q]; *see also* KAREN LEVY, DATA DRIVEN: TRUCKERS, TECHNOLOGY, AND THE NEW WORKPLACE SURVEILLANCE (2022).

[57] Lauren K. Gurley, *Amazon's Cost Saving Routing Algorithm Makes Drivers Walk into Traffic*, VICE (June 2, 2021, 10:33 AM), https://www.vice.com/en/article/5db95k/amazons-cost-saving-routing-algorithm-makes-drivers-walk-into-traffic [https://perma.cc/7QUR-SSXG].

[58] *Amazon-Owned Whole Foods Is Quietly Tracking Its Employees Heat Map Tool That Ranks Which Stores Are Most at Risk of Unionizing*, BUSINESS INSIDER, https://www.businessinsider.com/whole-foods-tracks-unionization-risk-with-heat-map-2020-1 [https://perma.cc/DX22-HJ5C].

framework of the Covid-19 pandemic, reports show how lesser-known "little tech" companies have also developed software to monitor office workers for productivity (especially when working from home), health (e.g., temperature-checking), and safety (e.g., whether workers are keeping two meters apart).[59]

The criminal justice system has long relied on risk assessment instruments ("RAI") to predict which convicts pose a flight risk or a threat to society and to make decisions about bail.[60] Despite massive criticism to algorithmic systems such as the Correctional Offender Management Profiling for Alternative Sanctions ("COMPAS"),[61] RAIs are still used around the US "in a hail-Mary effort to fix their overburdened jails and prisons."[62]

The administrative state is not exempt either from the effects of this algorithmic revolution.[63] Time and again, government agencies deploy automated decision-making systems powered by algorithms. At the state level, it is well known that states implemented algorithmic tools (also known as "care-rationing algorithms") to allocate scarce resources during the COVID-19 pandemic.[64] Likewise, both local and state governments use algorithms to flag welfare fraud,[65] predict child abuse,[66] decide foster care placement,[67] or to identify those

[59] Sarah O'Connor, *Never Mind Big Tech – 'Little Tech' Can Be Dangerous at Work Too*, FIN. TIMES (Feb. 22, 2022), https://www.ft.com/content/147bce5d-511c-4862-b820-2d85b736a5f6 [https://perma.cc/X57D-43U3].

[60] Alex Chohlas-Wood, *Understanding Risk Assessment in Instruments in Criminal Justice*, BROOKINGS (June 19, 2020), https://www.brookings.edu/research/understanding-risk-assessment-instruments-in-criminal-justice/ [https://perma.cc/7KSB-MYLN].

[61] Julia Angwin, Jeff Larson, Surya Mattu & Lauren Kirchner, *Machine Bias*, PROPUBLICA (May 23, 2016), https://www.propublica.org/article/machine-bias-risk-assessments-in-criminal-sentencing [https://perma.cc/J6L6-L8PL].

[62] Karen Hao, *AI Is Sending People To Jail — And Getting It Wrong*, MIT TECH. REV. (Jan. 21, 2019), https://www.technologyreview.com/2019/01/21/137783/algorithms-criminal-justice-ai/ [https://perma.cc/6GFL-HXYA].

[63] *See* Ryan Calo & Danielle K. Citron, *The Automated Administrative State: A Crisis of Legitimacy*, 70 EMORY L.J. 797, 800-02 (2021).

[64] Pria Anand, *Algorithms of Inequality*, APPEAL (Apr. 17, 2020), https://theappeal.org/politicalreport/algorithms-of-inequality-covid-ration-care/ [https://perma.cc/PZ6G-66UN].

[65] Sarah Marsh, *Councils Scrapping Use of Algorithms in Benefit and Welfare Decisions*, GUARDIAN (Aug. 24, 2020, 7:48 AM), https://www.theguardian.com/society/2020/aug/24/councils-scrapping-algorithms-benefit-welfare-decisions-concerns-bias [https://perma.cc/UF3M-D86R].

[66] Kim Strong, *Can a Computer Program Save More Children from Abuse and Neglect*. YORK DAILY REC. (June 24, 2021, 12:15 PM), https://www.ydr.com/story/news/2021/06/24/allegheny-countys-child-welfare-algorithm-hoped-save-children/5318550001/ [https://perma.cc/P4HG-WS36].

[67] Jeremey Loudenback, *The Foster Care System Turns to Big Data: Promising or Profiling?*, IMPRINT (Feb. 1, 2022, 2:48 PM), https://imprintnews.org/child-welfare-2/the-foster-care-system-turns-to-big-data-promising-or-profiling/62359 [https://perma.cc/JA3P-BETB].

experiencing homelessness who are "vulnerable enough" to qualify for housing.[68] A 2022 report from the Electronic Privacy Information Center ("EPIC") includes a comprehensive list of critical governmental decisions that the D.C. government has outsourced to automated decision-making ("ADM") systems.[69]

When it comes to law enforcement agencies, in 2020 the US Government Accountability Office ("GAO") reported how:

> Federal law enforcement agencies [GAO] reviewed primarily use probabilistic genotyping, latent print, and face recognition algorithms to help assess whether or not evidence collected in a criminal investigation may have originated from an individual. To a more limited extent, agencies also use algorithms to compare iris images, speech, and handwriting.[70]

Similarly, many of the surveillance technologies used by law enforcement agencies have algorithmic components. For instance, they use predictive policing software to predict the locations of and people involved in future crime.[71] They also arrest suspects based on matches from facial recognition algorithms.[72] Law enforcement also uses algorithmic social media monitoring tools to detect migration movements,[73] mass shootings, traffic accidents, natural disasters, protests, etc.[74] And the list goes on.

B. Regulatory spaces

This overwhelming avalanche of algorithms has invariably attracted the attention of regulatory actors. Although at a slower pace than technological

---

[68] Caitlin Thompson, *Who's Homeless Enough for Housing? In San Francisco, an Algorithm Decides*, CODA MEDIA (Sept. 21, 2021), https://www.codastory.com/authoritarian-tech/san-francisco-homeless-algorithm/ [https://perma.cc/T2NY-DZQL].

[69] THOMAS MCBRIEN, BEN WINTERS, ENID ZHOU & VIRGINIA EUBANKS, ELEC. PRIV. INFO. CTR., SCREENED & SCORED IN THE DISTRICT OF COLUMBIA (2022), https://epic.org/wp-content/uploads/2022/11/EPIC-Screened-in-DC-Report.pdf [https://perma.cc/KH2D-FXQZ].

[70] U.S. GOV'T ACCOUNTABILITY OFF., GAO-20-479SP, FORENSIC TECHNOLOGY, ALGORITHMS USED IN FEDERAL LAW 5 (2020).

[71] Kate Robertson, Cynthia Khoo, & Yolanda Song, *To Surveil and Predict: A Human Rights Analysis of Algorithmic Policing in Canada*, CITIZEN LAB (Sept. 1, 2020), https://citizenlab.ca/2020/09/to-surveil-and-predict-a-human-rights-analysis-of-algorithmic-policing-in-canada/ [https://perma.cc/2T6Z-SEQ7].

[72] Kashmir Hill, *Wrongfully Accused by an* Algorithm, N.Y. TIMES (June 24, 2020), https://www.nytimes.com/2020/06/24/technology/facial-recognition-arrest.html [https://perma.cc/ZWK9-XDAN].

[73] Julia Ainsley, *Biden Admin to Build Intelligence-Gathering Cell to Track Groups of Migrants Headed* North, NBC NEWS (Oct. 18, 2021, 4:30 AM), https://www.nbcnews.com/politics/immigration/biden-admin-build-intelligence-gathering-cell-track-groups-migrants-headed-n1281578 [https://perma.cc/86DP-D6AM].

[74] Matt Stroud, *Banjo's Surveillance Systems Grind to a Halt After CEO's KKK Past Revealed*, MEDIUM (Apr. 29, 2020), https://onezero.medium.com/states-ditch-surveillance-firm-banjo-after-ceos-kkk-past-is-revealed-acebaefea17f [https://perma.cc/D25Y-9JCM].

advancements, the legal and policy communities have slowly begun to recognize the outsized impact of algorithm-driven decision-making. Public awareness of computational algorithms' risks has grown, as have lawsuits challenging algorithmic decision-making in public benefits.[75]

Consequently, in the last eight years work by policymakers, civil society, and even the industry has sought to make algorithmic systems more accountable. First, the General Data Protection Regulation (GDPR) was adopted by the European Parliament in April 2016. Although a data protection law, the GDPR's Article 22 extended the right not to be subject to a decision based solely on automated processing provided in Article 15 of the 1995 Data Protection Directive,[76] to include the data subject's rights to obtain human intervention on the part of the controller, to express her point of view, and to contest the decision. Aside from these rights, Recital 71 of the GDPR also mentioned the right to receive an explanation of the decision reached following such an assessment.

However, as time passed, it became evident that algorithmic decision-making processes not only suffered from due process flaws. Rather, plenty other rights and values were also being jeopardized by these systems. For example, it became more and more clear that algorithms' ability to amplify biases against historically marginalized groups was not being addressed by Article 22 of the GDPR.

As a result, a wave of soft law on algorithms began to arise all around the world. As the Berkman Klein Center for Internet & Society aptly documented in 2020, "[t]he rapid spread of artificial intelligence (AI) systems has precipitated a rise in ethical and human rights-based frameworks intended to guide the

[75] LYDIA X. BROWN, MICHELLE RICHARDSON, RIDHI SHETTY, ANDREW CRAWFORD & TIMOTHY HOAGLAND, CTR. FOR DEMOCRACY & TECH., CHALLENGING THE USE OF ALGORITHM-DRIVEN DECISION-MAKING IN BENEFITS DETERMINATIONS (2020), https://cdt.org/wp-content/uploads/2020/10/2020-10-21-Challenging-the-Use-of-Algorithm-driven-Decision-making-in-Benefits-Determinations-Affecting-People-with-Disabilities.pdf [https://perma.cc/7PVA-V3Y3].

[76] "Article 15 Automated individual decisions.

1. Member States shall grant the right to every person not to be subject to a decision which produces legal effects concerning him or significantly affects him and which is based solely on automated processing of data intended to evaluate certain personal aspects relating to him, such as his performance at work, creditworthiness, reliability, conduct, etc.

2. Subject to the other Articles of this Directive, Member States shall provide that a person may be subjected to a decision of the kind referred to in paragraph 1 if that decision:

(a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his legitimate interests, such as arrangements allowing him to put his point of view; or

(b) is authorized by a law which also lays down measures to safeguard the data subject's legitimate interests." Council Directive 95/46, art. 15, 1995 O.J. (L 281) 43 (EC).

development and use of these technologies."[77] Authored by governments and intergovernmental organizations, companies, professional associations, advocacy groups, and multi-stakeholder initiatives, these AI principles initiatives looked to offer guidelines on the following eight themes—also referred to as "the 'normative core' of a principle-based approach to AI ethics and governance": privacy, accountability, safety and security, transparency and explainability, fairness and non-discrimination, human control of technology, professional responsibility, and promotion of human values.[78]

In the case of the United States government, this soft-law approach has included, among other initiatives, the 2016 document *Preparing for the Future of AI*, issued by the U.S. National Science and Technology Council; the 2019 *Guidance for Regulation of Artificial Intelligence Applications* proposed by the White House's Office of Science and Technology Policy; the National Institute of Standards and Technology's (NIST) 2019 document titled *U.S. LEADERSHIP IN AI: A Plan for Federal Engagement in Developing Technical Standards and Related Tools*; the U.S. Department of Defense's *Ethical Principles for Artificial Intelligence*, adopted in February 24, 2020; and the NIST's 2022 special publication *Towards a Standard for Identifying and Managing Bias in Artificial Intelligence*. In October of 2022, the White House's Office of Science and Technology Policy published the *Blueprint for an AI Bill of Rights*, which looks to "provide guidance whenever automated systems can meaningfully impact the public's rights, opportunities, or access to critical needs."[79] And in January 2023, NIST released the *AI Risk Management Framework* (*AI RMF 1.0*), which was developed in collaboration with the private and public sectors, and looks to mitigate risk, while cultivating trust in AI technologies and promoting AI innovation.[80]

In recent years, binding law has also begun to play a more significant role. When it comes to the use of algorithms by the public sector, there has been an initial wave of algorithmic accountability policies all around the world. As

[77] Jessica Fjeld, *Principled Artificial Intelligence: Mapping Consensus In Ethical And Rights-Based Approaches to Principles For AI*, BERKMAN KLEIN CTR. (Jan. 15, 2020), https://cyber.harvard.edu/publication/2020/principled-ai [https://perma.cc/6MBX-XCC4].

[78] JESSICA FELD, NELE ACHTEN, HANNAH HILLIGLOSS, ADAM NAGY, & MADHULIKA SRIKUMAR, BERKMAN KLEIN CTR. FOR INTERNET & SOC'Y, PRINCIPLED ARTIFICIAL INTELLIGENCE: MAPPING CONSENSUS IN ETHICAL AND RIGHTS-BASED APPROACHES TO PRINCIPLES FOR AI 4-5 (2020), https://dash.harvard.edu/bitstream/handle/1/42160420/HLS%20White%20Paper%20Final_v3.pdf [https://perma.cc/P6X4-SKT2].

[79] *Blueprint for an AI Bill of Rights*. WHITE HOUSE https://www.whitehouse.gov/ostp/ai-bill-of-rights/ [https://perma.cc/A7R4-B2X2]; *see also* Alex Engler, Suresh Venkatasubramanian & Justin Hendrix, *Unpacking the Blueprint for an AI Bill of* Rights, TECH. POL'Y PRESS: THE SUNDAY SHOW (Oct. 11, 2022), https://techpolicy.press/unpacking-the-blueprint-for-an-ai-bill-of-rights/ [https://perma.cc/MMU7-VHYK].

[80] *AI Risk Management* Framework, NIST: INFO. TECH. LAB'Y, https://www.nist.gov/itl/ai-risk-management-framework [https://perma.cc/3EY9-HWWA]. While this article was being edited, several other soft-law documents were published by US government agencies.

reported by the Ada Lovelace Institute ("Ada"), AI Now Institute ("AI Now"), and Open Government Partnership ("OGP") in a study published in 2021, besides non-binding principles and guidelines, governments have also sought to achieve algorithmic accountability in the public sector by use of the following binding policy mechanisms: (i) prohibitions and moratoria; (ii) transparency mechanisms such as public registries of algorithmic systems and requirements for source-code transparency; (iii) impact assessments; (iv) audits and regulatory inspections; (v) external/independent oversight bodies; (vi) rights to hearing and appeal; and (vii) procurement conditions.[81]

That is the case, for example, of the bans on governmental use of facial recognition passed in King County (Washington), Portland (Oregon), the state of Maine, and over a dozen other cities around the country;[82] the bans on law enforcement use of facial recognition in Vermont and Virginia;[83] the bans on the use of predictive policing in Bellingham (Washington), Santa Cruz (California), and Oakland (California);[84] and Canada's 2019 Directive on Automated Decision-Making, which requires an Algorithmic Impact Assessment (AIA) to determine the impact level of a system.[85] Similarly, jurisdictions such as New York City (New York),[86] Pittsburgh (Pennsylvania),[87] Vermont,[88] Washington state,[89] and Colorado[90] have established automated decision systems task

[81] ADA LOVELACE INST., AI NOW INST. & OPEN GOV'T. P'SHIP., ALGORITHMIC ACCOUNTABILITY FOR THE PUBLIC SECTOR 3 (2021), https://www.opengovpartnership.org/documents/algorithmic-accountability-public-sector/ [https://perma.cc/TZJ5-NK2K].

[82] Interactive Map, *Ban Facial Recognition*, FIGHT FOR THE FUTURE, https://www.banfacialrecognition.com/map/ [https://perma.cc/2YWZ-9E24].

[83] *Id*.

[84] OFF. OF THE CHIEF INFO. OFFICER, AUTOMATED DECISION-MAKING SYSTEMS WORKGROUP REPORT 29 (2021), https://app.leg.wa.gov/ReportsToTheLegislature/Home/GetPDF?fileName=Automated%20Decision%20Systems%20Workgroup%20Report_a1946676-3de2-4a8e-929d-b4b8a689a49d.pdf [https://perma.cc/S2EZ-EX5P].

[85] Directive on Automated Decision-Making § 6.1 (2019) (Can.), https://www.tbs-sct.canada.ca/pol/doc-eng.aspx?id=32592 [https://perma.cc/R49T-3EB4].

[86] N.Y.C. AUTOMATED DECISION SYS. TASK FORCE, NEW YORK CITY AUTOMATED DECISION SYSTEM TASK FORCE REPORT (2019), https://www.nyc.gov/assets/adstaskforce/downloads/pdf/ADS-Report-11192019.pdf [https://perma.cc/Z363-SCLN].

[87] PITTSBURGH TASK FORCE ON PUB. ALGORITHMS, REPORT OF THE PITTSBURGH TASK FORCE ON PUBLIC ALGORITHMS (2022), https://www.cyber.pitt.edu/sites/default/files/pittsburgh_task_force_on_public_algorithms_report.pdf [https://perma.cc/VFD8-EYUN].

[88] ARTIFICAL INTELLIGENCE TASK FORCE, FINAL REPORT (2020), https://outside.vermont.gov/agency/ACCD/ACCD_Web_Docs/ED/MajorInitiatves/ArtificialIntelligenceTaskForce/FinalReport.pdf [https://perma.cc/989S-ZBK4].

[89] AUTOMATED DECISION-MAKING SYSTEMS WORKGROUP REPORT, *supra* note 84. I personally served as a research expert member in the workgroup.

[90] S.B. 22-113, 74th Gen. Assemb., Reg. Sess. (Colo. 2022) (final report not yet published).

forces/workgroups to provide recommendations on the governance of algorithms used by public agencies.

In other countries, there have also been more ambitious attempts to generally regulate AI. On April 21, 2021, the European Union introduced the Artificial Intelligence Act ("AI Act"),[91]which was finally approved by the European Parliament on March 13, 2024.[92] On March 1, 2022, China's Internet Information Service Algorithmic Recommendation Management Provisions came into effect.[93] These provisions look to "create comprehensive rules on the widespread use of algorithms online, ranging from search filters, personalized recommendations, information sharing services, user rights and more."[94] In Canada, the Canadian Parliament introduced the Artificial Intelligence and Data Act ("AIDA") on June of 2022, as part of the Digital Charter Implementation Act.[95] And on March of 2023, the United Kingdom's Secretary of State for Science, Innovation and Technology presented to Parliament a white paper titled *AI Regulation: A Pro-Innovation Approach*, which details the UK's plans "to support innovation while providing a framework to ensure risks are identified and addressed."[96]

In the United States, Congress, the Federal Trade Commission ("FTC"), and the White House have also shown a persistent interest in regulating algorithms

[91] *See Proposal for a Regulation of the European Parliament and of the Council Laying Down Harmonized Rules on Artificial Intelligence (Artificial Intelligence Act) and Amending Certain Union Legislative Acts*, COM (2021) 206 final (Apr. 21, 2021).

[92] *See Artificial Intelligence Act: MEPs Adopt Landmark Law*, EUROPEAN PARLIAMENT (Mar. 13, 2024), https://www.europarl.europa.eu/news/en/press-room/20240308IPR19015/artificial-intelligence-act-meps-adopt-landmark-law [https://perma.cc/L6PL-KFHH].

[93] Roger Creemers, Graham Webster & Helen Toner, *Translation: Internet Information Service Algorithmic Recommendation Management Provisions – Effective March 1, 2022*, DIGICHINA (Jan. 10 2022), https://digichina.stanford.edu/work/translation-internet-information-service-algorithmic-recommendation-management-provisions-effective-march-1-2022/ [https://perma.cc/UPK9-JUJW].

[94] Samuel Adams, *China's Draft Algorithm Regulations: A First for Consumer Privacy*, IAPP (Oct. 13, 2021), https://iapp.org/news/a/chinas-draft-algorithm-regulations-a-first-for-consumer-privacy/ [https://perma.cc/6B89-A4HM].

[95] *See* Bill C-27, Digital Charter Implementation Act, 2022, 44th Parliament, 1st Session (Can.) Recently, a companion document was also published. *The Artificial Intelligence and Data Act (AIDA) – Companion document, GOV'T OF CAN.* (Mar. 13, 2023) https://ised-isde.canada.ca/site/innovation-better-canada/en/artificial-intelligence-and-data-act-aida-companion-document [https://perma.cc/WD3H-TDR5].

[96] DEP'T FOR SCI. INNOVATION & TECH., A PRO-INNOVATION APPROACH TO AI REGULATION 2 (2023), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/1146542/a_pro-innovation_approach_to_AI_regulation.pdf [https://perma.cc/RDQ4-HC9P].

and AI. Both in 2019[97] and in 2022,[98] Congresswoman Yvette D. Clarke attempted to pass the Algorithmic Accountability Act. In addition, the draft of the American Data Privacy and Protection Act ("ADPPA") discussed in the 117th legislative session of Congress contains a provision (Section 207(c)(1)) that requires data holders to conduct *impact assessments* of algorithms used solely or in part "to collect, process, or transfer covered data" "in a manner that poses a consequential risk of harm to an individual or group of individuals;" likewise, Section 207(c)(2) requires covered entities to conduct *algorithm design evaluations* prior to deploying the covered algorithm in interstate commerce, to reduce the risk of the potential harms identified under the impact assessments.[99] In April 2023, in turn, U.S. Senate Majority Leader Charles E. Schumer launched a high-level framework that outlined a new regulatory regime for artificial intelligence, which he expected to refine in conjunction with several stakeholders.[100] Similarly, in September 2023 the chair and ranking member of the Judiciary Subcommittee on Privacy, Technology, & the Law, Senators Richard Blumenthal and Josh Hawley, released a bipartisan framework outlining specific principles for future AI-focused legislative initiatives.[101]

In the last few years, the FTC has also explored several different avenues to rein in algorithms. In 2016 it issued a report[102] "which advised companies using big data analytics and machine learning to reduce the opportunity for bias."[103] In November 2018, the FTC held a two-day hearing on "The Competition and Consumer Protection Issues of Algorithms, Artificial Intelligence, and Predictive Analytics."[104] Likewise, in a number of settlement orders issued since 2019,

[97] Algorithmic Accountability Act of 2019, H.R. 2231, 116th Cong. (2019).

[98] Algorithmic Accountability Act of 2022, H.R. 6580, 117th Cong. (2022).

[99] American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).

[100] *Schumer Launches Major Effort To Get Ahead Of Artificial* Intelligence, SENATE DEMOCRATS (Apr. 13, 2023), https://www.democrats.senate.gov/newsroom/press-releases/schumer-launches-major-effort-to-get-ahead-of-artificial-intelligence [https://perma.cc/H9FB-8M2Y].

[101] *Blumenthal & Hawley Announce Bipartisan Framework on Artificial Intelligence Legislation*, RICHARD BLUMENTHAL (Sept. 8, 2023), https://www.blumenthal.senate.gov/newsroom/press/release/blumenthal-and-hawley-announce-bipartisan-framework-on-artificial-intelligence-legislation [https://perma.cc/XP6J-CJGS].

[102] FED TRADE COMM'N, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? (2016), https://www.ftc.gov/system/files/documents/reports/big-data-tool-inclusion-or-exclusion-understanding-issues/160106big-data-rpt.pdf [https://perma.cc/JRX2-48Z9].

[103] Andrew Smith, *Using Artificial Intelligence and Algorithms*, FED. TRADE COMM'N: BUS. BLOG (Apr. 8 2020), https://www.ftc.gov/business-guidance/blog/2020/04/using-artificial-intelligence-and-algorithms [https://perma.cc/9TGF-MKNL].

[104] *FTC Hearings on Competition and Consumer Protection in the 21st Century Continue with Examination of Algorithms, Artificial Intelligence, and Predictive Analytics*, FED. TRADE COMM'N: MEDIA ADVISORY (Nov. 9, 2018), https://www.ftc.gov/news-events/news/press-releases/2018/11/ftc-hearings-competition-consumer-protection-21st-century-continue-examination-algorithms-artificial [https://perma.cc/24CF-DD5R].

the FTC has required the destruction of algorithms built with data gathered deceptively or illegally (remedy commonly known as "algorithmic disgorgement").[105] In April 2020, Andrew Smith, Director of the FTC Bureau of Consumer Protection, issued business guidance for using artificial intelligence and algorithms.[106]

Furthermore, in August 2022, the FTC announced a Commercial Surveillance and Data Security Rulemaking.[107] Issued under the Commission's Section 5 authority to regulate and prohibit unfair and deceptive practices, the Advance Notice of Proposed Rulemaking requested public comment on, among others, a large number of questions related to Automated Decision-Making Systems, with a particular focus on algorithmic error, algorithmic discrimination, and unaccountable algorithmic decision-making.[108] In April 2023, the FTC and three other federal agencies[109] issued a joint statement pledging to uphold "America's commitment to the core principles of fairness, equality, and justice"[110] as emerging automated systems, including those sometimes marketed as AI become increasingly common in our daily lives. And in May of that same year, FTC Chair Lina M. Khan made a clear statement in a New York Times op-ed: "The F.T.C. is well equipped with legal jurisdiction to handle the issues brought to the fore by the rapidly developing A.I. sector, including collusion, monopolization, mergers, price discrimination and unfair methods of competition."[111]

Finally, since 2019 the White House issued three Executive Orders ("EO") affecting both the use of AI in the Federal Government and its use and development in the private sector: (i) EO 13859 *Maintaining American Leadership in Artificial Intelligence*; (ii) EO 13960 *Promoting the Use of Trustworthy*

[105] *See* Joshua A. Goland, *Algorithmic Disgorgement: Destruction of Artificial Intelligence Models as the FTC's Newest Enforcement Tool for Bad Data*, 29 RICH. J.L. & TECH. 1, 2 (2023); *see also* Rebecca K. Slaughter with Janice Kopec & Mohamad Batal, *Algorithms and Economic Justice: A Taxonomy of Harms and a Path Forward for the Federal Trade Commission*, 23 YALE J.L. & TECH. 1, 39 (2021). *But see* Tiffany C. Li, *Algorithmic Destruction*, 75 SMU L. REV. 479, 498 (2022).

[106] Smith, *supra* note 103.

[107] *Commercial Surveillance and Data Security Rulemaking*, FED. TRADE COMM'N (Aug. 11, 2022), *https*://www.ftc.gov/legal-library/browse/federal-register-notices/commercial-surveillance-data-security-rulemaking [https://perma.cc/QRQ8-JKU3].

[108] Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273 (proposed August 22, 2022) (to be codified at 16 CFR).

[109] The Consumer Financial Protection Bureau, the Justice Department's Civil Rights Division, and the Equal Employment Opportunity Commission.

[110] Rohit Chopra, Kristen Clarke, Charlotte A. Burrows & Lina Khan, *Joint Statement on Enforcement Efforts Against Discrimination and Bias in Automated* Systems, U.S. EQUAL EMP. OPPORTUNITY COMM'N, https://www.eeoc.gov/joint-statement-enforcement-efforts-against-discrimination-and-bias-automated-systems [https://perma.cc/VDC4-NRQQ].

[111] Lina Khan, *Lina M. Khan: We Must Regulate A.I. Here's How,* N.Y. TIMES (May 3, 2023), https://www.nytimes.com/2023/05/03/opinion/ai-lina-khan-ftc-technology.html [https://perma.cc/T3SK-WRBQ].

Artificial Intelligence in the Federal Government; and (iii) EO 14110 *Safe, Secure, and Trustworthy Development and Use of Artificial Intelligence*. The latter, issued by President Joe Bidden on October 30th, 2023, is considered to be one of the most important actions taken by any government in the world in terms of AI safety to date.[112]

Given this ubiquity of algorithmic technologies and talk in society and regulatory environments, it is not surprising that algorithms have also taken over a considerable portion of privacy law scholarship. It is interesting to investigate, though, how this has occurred. This, the subject to which I turn next.

II. THE ALGORITHMIC TURN IN AMERICAN PRIVACY LAW SCHOLARSHIP

As members of the PLSC community have followed—and personally experienced—the algorithmic turn in contemporary society, their scholarship has been inescapably affected. During the course of the evolution and permeation of information technologies, scholars have written extensively about them. And, in the context of the transition to AI and algorithmic decision-making systems, a large portion of these scholars has begun to consider not only new types of privacy harms, but also novel tools to address them.

As Deirdre Mulligan, Colin Koopman, and Nick Doty would adequately anticipate in 2016,

> [S]cholars and practitioners have advanced alternative conceptions of privacy that address the new risks of data science, machine learning and other technological innovations. Scholars have argued for privacy concepts and approaches that unburden the individual by attending to the contextual norms of spheres of social life, address risks posed by ancillary data and attend to the emerging semantics of machine learning. Professionals have developed new concepts, such as 'trust' and 'meeting expectations', and contrast concepts such as 'creepiness', in an effort to address the shifting privacy concerns of customers and citizens.[113]

As a result of these different efforts, what we can see today is that a substantial number of scholars have gradually transformed information privacy into a post-algorithmic concept. Besides enabling individuals to protect themselves from harms to their individual autonomy and to certain collective values such as democracy or innovation,[114] information privacy is now expected by many to serve as a government tool to protect society from data extraction and its consequent power imbalances.

---

[112] *See* Shiona McCallum & Zoe Kleinman, *US Announces 'Strongest Global Action Yet' on AI Safety*, BBC (Oct. 30, 2023), https://www.bbc.com/news/technology-67261284 [https://perma.cc/Z4FU-TFPY].

[113] Deirdre Mulligan, Colin Koopman & Nick Doty, *Privacy Is an Essentially Contested Concept: A Multi-Dimensional Analytic for Mapping Privacy*, 374 PHIL. TRANSACTIONS ROYAL SOC'Y. 1, 2 (2016).

[114] *See* Schwartz, *supra* note 1.

This Part delves deeper into the main two features of privacy's algorithmic turn. In order to provide a balanced analysis, it also identifies some of the outliers of this turn.

A. Features

In 2021 Woodrow Hartzog used the term "algorithmic turn" in relation to privacy scholarship, to describe how privacy scholars have lately addressed "discussions of how privacy issues impact marginalized and vulnerable populations."[115] I agree with this reading. The phenomenon I describe here, however, goes much further than Hartzog's conception. As we will see in this Section, the two main features that characterize privacy's algorithmic turn in American privacy law scholarship are: (1) a change in what is usually considered privacy harms, and consequently, (2) a transformation of the tools proposed to protect privacy.

1. Novel information privacy harms

In the last ten years, a number of American privacy law scholars have more and more focused on and called attention to data-driven harms such as

[115] Hartzog, *supra* note 4, at 1681.

algorithmic discrimination (unfairness),[116] online manipulation,[117] procedural injustices,[118] and subordination.[119] More importantly, these scholars have either identified them as privacy harms or suggested privacy tools to address them.

[116] *See e.g.*, Omer Tene & Jules Polonetsky, *Privacy in the Age of Big Data: A Time for Big Decisions,* 64 STAN. L. REV. ONLINE 63 (2012) (discrimination, exclusion); Neil Richards, *Four Privacy Myths*, *in* A WORLD WITHOUT PRIVACY: WHAT LAW CAN AND SHOULD DO? (Austin Sarat ed., 2015) (sorting); Julie E. Cohen, *Turning Privacy Inside Out*, 20 THEOR. INQ. L. 1 (2019) (racially disparate results / racial or socioeconomic segmentation) [hereinafter Cohen, *Turning Privacy Inside Out*]; Sandra Wachter & Brent Mittelstadt, *A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI*, 2019 COLUMB. BUS. L. REV. 1 (2019); Aaron Fluitt, Aloni Cohen, Micah Altman, Kobbi Nissim, Salome Viljoen & Alexandra Wood, *Data Protection's Composition Problem*, 5 EUR. DATA PROT. L. REV. 285 (2019) (virtual group redlining); SCOTT SKINNER-THOMPSON, PRIVACY AT THE MARGINS (2020) (discrimination and marginalization based on identities); Solon Barocas & Karen Levy, *Privacy Dependencies*, 95 WASH. L. REV. 555 (2020); Dennis D. Hirsch, *From Individual Control to Social Protection: New Paradigms for Privacy Law in the Age of Predictive Analytics*, 79 MD. L. REV. 439 (2020) (harmful bias); Ari E. Waldman, *The New Privacy Law*, 55 UC DAVIS L. REV. ONLINE 19 (2021) [hereinafter Waldman, *The New Privacy Law*]; Ari E. Waldman, *Privacy, Practice, and Performance*, 110 CALIF. L. REV. 1221 (2021) [hereinafter Waldman, *Privacy, Practice, and Performance*] (structural asymmetries and discriminatory harms); Neil M. Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. 961 (2021) [hereinafter Richards & Hartzog, *Duty of Loyalty*]; Danielle K. Citron & Daniel J. Solove, *Privacy Harms*, 102 B.U. L. REV. 793 (2022); Daniel J. Solove, *The Limitations of Privacy Rights*, 98 NOTRE DAME L. REV. 975 (2023) [hereinafter Solove, *The Limitations of Privacy Rights*]; Anita L. Allen, *Dismantling the "Black Opticon": Privacy, Race Equity, and Online Data-Protection Reform*, 2022 YALE L.J.F. (2022) [hereinafter Allen, *Black Opticon*] (racial discrimination); ANITA L. ALLEN, *Privacy, Critical Definition and Racial Justice*, *in* THE OXFORD HANDBOOK OF APPLIED PHILOSOPHY OF LANGUAGE (Luvell Anderson & Ernie Lepore eds., forthcoming 2024) (racial discrimination). It is important to note that discrimination had started to be highlighted by some privacy law scholars even before and around the time "the new privacy" was described by Schwartz and Treavor. However, its mentions—and its algorithmic component—have significantly increased in the last several years. *See e.g*, Paul Schwartz, *Beyond Lessig's Code for Internet Privacy: Cyberspace Filters, Privacy Control, and Fair Information Practices*, 2000 WIS. L. REV. 743 (2000) [hereinafter Schwartz, *Beyond Lessig's Code*]; Michael Froomkin, *The Death of Privacy*, 52 STAN. L. REV. 1461 (2000); Joel R. Reidenberg, *Privacy Wrongs in Search of Remedies,* 54 HASTINGS L.J. 877 (2002-2003) (information redlining practices and stereotyping individuals); Tal Z. Zarsky, *"Mine Your Own Business!": Making the Case for the Implications of the Data Mining of Personal Information in the Forum of Public Opinion*, 5 YALE J.L. & TECH. 1 (2003) [hereinafter Zarsky, *"Mine Your Own Business!"*]; Tal Z. Zarsky, *Thinking Outside the Box: Considering Transparency, Anonymity, and Pseudonymity as Overall Solutions to the Problems of Information Privacy in the Internet Society*, 58 U. MIAMI L. REV. 991 (2004) [hereinafter Zarsky, *Considering Transparency, Anonymity, and Pseudonymity*] (price discrimination).

[117] *See e.g.*, Cohen, *Turning Privacy Inside Out*, *supra* note 116; Wachter & Mittelstadt, *supra* note 116; Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687 (2020) [hereinafter Hartzog & Richards, *Privacy's Constitutional Moment*] (human susceptibility to manipulation); Hirsch, *supra* note

These harms seem distant to what Anita Allen once coined as the "paradigmatic forms of privacy," namely: seclusion, solitude, confidentiality, secrecy, and anonymity.[120] Likewise, they don't seem to be covered either by the six conceptions of privacy that Daniel Solove identified in 2002 when tracking how a

116; Waldman, *The New Privacy Law*, *supra* note 116 (attendant behavior manipulation); Neil Richards & Woodrow Hartzog, *A Relational Turn for Data Protection?*, 4 EUR. DATA PROT. L. REV. 1 (2020) [hereinafter Richards & Hartzog, *A Relational Turn*] (manipulate us against our interests); Richards & Hartzog, *Duty of Loyalty*, *supra* note 116 (nudging, manipulation); Woodrow Hartzog & Neil Richards, *The Surprising Virtues of Data Loyalty*, 71 EMORY L.J. 985 (2022) [hereinafter Hartzog & Richards, *Data Loyalty*] (nudging, influence, coercion); Citron & Solove, *supra* note 116. Although not necessarily "algorithmic" in nature, manipulation had also been mentioned by some privacy law scholars even before and around the time the "new privacy" was described by Schwartz and Treavor. However, as it happens in the case of discrimination, its mentions have significantly increased in the last several years. *See e.g*, Paul Schwartz, *Privacy and Democracy in Cyberspace*, 52 VANDERBILT L. REV. 1609 (1999) [hereinafter Schwartz, *Privacy and Democracy*]; Schwartz, *Beyond Lessig's Code, supra* note 116; Julie E. Cohen, *Examined Lives: Informational Privacy and the Subject as Object*, 52 STAN. L. REV. 1373 (2000) [hereinafter Cohen, *Examined Lives*] (behavior modification and threats to free will); Reidenberg, *supra* note 116 (large scale manipulative practices); Zarsky, *Considering Transparency, Anonymity, and Pseudonymity*, *supra* note 116; Zarsky, *"Mine Your Own Business!," supra* note 116 (manipulation [the autonomy trap]).

[118] *See e.g.,* Jerry Berman & Deirdre Mulligan, *Privacy in the Digital Age: Work in Progress*, 23 NOVA L. REV. 549 (1999) (lack of fairness); Daniel J. Solove, *Conceptualizing Privacy*, 90 CAL. L. REV. 1087 (2002) [hereinafter Solove, *Conceptualizing Privacy*] (scant knowledge of how the information is processed and used); Daniel J. Solove, "*I've Got Nothing to Hide" and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745 (2007) [hereinafter Solove, *Misunderstandings of Privacy*] (lack of transparency and accountability); Kate Crawford & Jason Schultz, Big Data and Due Process: Toward a Framework to Redress Predictive Privacy Harms, 55 Boston College L. Rev. 93 (2014); Seda Gürses & Joris van Hoboken, *Privacy After the Agile Turn*, *in* THE CAMBRIDGE HANDBOOK OF CONSUMER PRIVACY 579 (Evan Selinger et al. eds., 2018) (privacy literature has focused on algorithms and its problems of accountability, fairness, autonomy, and due process); Hartzog & Richards, *Privacy's Constitutional Moment*, *supra* note 117, at 1758 ("Data-driven companies also threaten peoples' due process rights as algorithms make decisions about people's health, finances, jobs, ability to travel, and other essential life activities. Citron has argued for a 'technological due process' that is ensured in these systems. The modern discourse around this topic has centered around algorithmic fairness, transparency, and accountability. Any approach to data privacy that does not incorporate algorithmic accountability will be incomplete."); Hirsch, *supra* note 116 (procedural unfairness).

[119] *See e.g.,* Mary Anne Franks, *Democratic Surveillance*, 30 Harvard J. L. & Tech. 425, 429 (2017) ("multiple forms of subordination"); Hartzog & Richards, *Privacy's Constitutional Moment*, *supra* note 117 (oppression and abuse); Waldman, *The New Privacy Law*, *supra* note 116 (subordination, put marginalized populations at unique risk); Waldman, *Privacy, Practice, and Performance*, *supra* note 116 (subordination, power asymmetries); Solove, *The Limitations of Privacy Rights*, *supra* note 116 (subordination of minority groups and the poor).

[120] Anita L. Allen, *Coercing Privacy*, 40 WM. & MARY L. REV. 723, 756 (1999).

wide array of actors—including scholars—had chosen to theorize about privacy (the right to be left alone, intimacy, limited access to the self, secrecy, control over personal information, and personhood).[121]

In spite of their diverse natures, these novel harms tend to share the following three characteristics: (i) they are *objective*, (ii) they derive from the actual *processing* of data, and (iii) they are *architectural*.

In 2011, Ryan Calo proposed that the privacy harm is comprised of two distinct but interrelated categories: a subjective and an objective.[122] While the subjective category encompasses "unwelcome mental states such as anxiety or embarrassment that accompany the belief of an individual (or group) that he is being watched or monitored,"[123] *objective* harm refers to "negative, external actions justified by reference to personal information."[124] Similarly, Ignacio Cofone uses the term "consequential harms" to refer to the latter category of harms. According to Cofone, these are "[h]arms that are enabled by a loss of privacy;" "they are harms that are external to privacy interests but occur as a consequence of privacy violations."[125]

Although subjective privacy harms have been continually acknowledged in the privacy law scholarship here reviewed,[126] privacy scholars' attention has more and more focused on material harms, which happen outside of the data subjects' subjectivities and as a downstream consequence or negative externality of a loss of privacy.[127] Thus, instead of discussing the psychological or dignitary

[121] Solove, *Conceptualizing Privacy*, *supra* note 118, at 1092.

[122] *See* Ryan Calo, *The Boundaries of Privacy Harm*, 86 IND. L.J. 1131 (2011) [hereinafter Calo, *Boundaries of Privacy Harm*]; *see also* Ryan Calo, *Digital Market Manipulation*, 82 GEO. WASH. L. REV. 995, 1028-1029 (2014) ("The first category is subjective in that it is internal to the person experiencing the harm. In this context, subjective privacy harm is the perception of unwanted observation, in other words the unwelcome mental states such as anxiety or embarrassment that accompany the belief of an individual (or group) that he is being watched or monitored. The second element is objective in the sense of involving external forces being brought to bear against a person or group because of information about them. Thus, this category is the unanticipated or coerced use of personal information in a way that disadvantages the individual.").

[123] Calo, *Boundaries of Privacy Harm*, *supra* note 122, at 1028.

[124] Calo, *Boundaries of Privacy Harm*, *supra* note 122, at 1133.

[125] Ignacio Cofone, *Privacy Standing*, 2022 U. ILL. L. REV. 1367, 1396 (2022). As will be seen later when we talk about the critics of the algorithmic turn, consequential harms fall outside of what Cofone has defined as privacy harm.

[126] *See e.g.,* Citron & Solove, *supra* note 116; s*ee also* Eloise Gratton, *If Personal Information Is Privacy's Gatekeeper, Then Risk of Harm is the Key: A Proposed Method for Determining What Counts as Personal Information*, 24 ALB. L.J. SCI. & TECH. 105 (2013); Roger Allan Ford & W. Nicholson Price II, *Privacy and Accountability in Black-Box Medicine*, 23 MICH. TELECOM. & TECH. L. REV. 1 (2016).

[127] *See e.g.,* James P. Nehf, *Recognizing the Societal Value in Information Privacy*, 78 WASH. L. REV. 1 (2003); Zarsky, *Considering Transparency, Anonymity, and Pseudonymity*,

effects of privacy violations, such as inhibition, self-censorship, embarrassment, or the constant fear of being surveilled, several American privacy law scholars have lately been more interested in the tangible consequences of those violations.

Among these tangible consequences, those resulting from the actual *processing* of data have garnered particular attention.[128] *Processing* normally implies the application of algorithms and other data analysis techniques—hence the algorithmic nature of the turn. In that sense, the harms these American privacy law scholars have lately cared about usually stem from the deployment of AI, machine learning, and other types of data-driven decision-making systems.

Finally, the types of harms this group of privacy law scholars mostly care about also tend to be described as *architectural*. These harms are fundamentally related to what, in 2006, Daniel Solove would describe as "architectural privacy problems." In Solove's words,

> There is another, more modern kind of privacy problem that does not readily fit with this dignitary understanding of harm. These problems are more structural in nature. I refer to them as "architectural" problems. They involve less the overt insult or reputational harm to a person and more the creation of risk that a person might be harmed in the future. They are akin, in many ways, to environmental harms or pollution. In the taxonomy, two kinds of architectural issues emerge most often. First is the enhancement of the risk that a harm will occur. … Second, *a particular activity can upset the balance of social or institutional power in undesirable ways*. A particular individual may not be harmed directly, but this balance of power can affect that person's life.[129]

As time passes, an increasing number of scholars are focusing on this second type of architectural harm. Rather than affecting individual data subjects, architectural harms have an impact on the distribution of power in society. In that sense, they are usually considered population-level harms, generating structural, systemic, widely distributed, and larger societal problems.[130] These harms can be pervasive, affecting entire groups or segments of populations.

---

supra note 116 at 994; Gratton, *supra* note 126 at 106-07; SKINNER-THOMPSON, *supra* note 116 at 3.

[128] *See e.g.,* Reidenberg, *supra* note 116; Wendy Seltzer, *Privacy, Option Value, and Feedback* (draft submitted to TPRC) (2012); Mulligan et al., *supra* note 113; Hartzog & Richards, *Privacy's Constitutional Moment*, *supra* note 117, at 1758.

[129] Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 487 (2006) (emphasis added).

[130] *See e.g.,* Haiyan Jia & Heng Xu, *Measuring Individuals' Concerns Over Collective Privacy on Social Networking Sites*, 10 CYBERPSYCHOLOGY: J. PSYCHOSOCIAL RSCH. ON CYBERSPACE 1 (2016); Fluitt et al., *supra* note 116; Waldman, *The New Privacy Law*, *supra* note 116; Waldman, *Privacy, Practice, and Performance*, *supra* note 116; Julie E. Cohen, *How (Not) to Write a Privacy Law*, KNIGHT FIRST AMENDMENT INST. (Mar. 23, 2021)

2. A transformation of the privacy tools proposed

Before PLSC, many of the scholars that would become regular participants of the conference published articles arguing for the FIPs' codification, either through statutes or through technology.[131] [132] The latter, inspired by Joel Reidenberg and Lawrence Lessig's well-known ideas about the rule-making power of technology.[133]

https://knightcolumbia.org/content/how-not-to-write-a-privacy-law [https://perma.cc/7ERH-3PYP]; Solove, *The Limitations of Privacy Rights*, *supra* note 116.

[131] *See e.g.,* Allen, *supra* note 120; Berman & Mulligan, *supra* note 118; Joel R. Reidenberg, *Restoring Americans' Privacy in Electronic Commerce Symposium - The Legal and Policy Framework for Global Electronic Commerce: A Progress Report,* 14 BERKELEY TECH. L.J. 771 (1999); Schwartz, *Privacy and Democracy*, *supra* note 117; Beth Givens, *Privacy Expectations in a High Tech World*, 16 SANTA CLARA HIGH TECH. L.J. 347 (2000); Cohen, *Examined Lives*, *supra* note 117; Froomkin, *supra* note 116; Marc Rotenberg, *Fair Information Practices and the Architecture of Privacy (What Larry Doesn't Get),* 2001 STAN. TECH. L. REV. 1 (2001); Daniel J. Solove, *Privacy and Power: Computer Databases and Metaphors for Information Privacy*, 53 STAN. L. REV. 1393 (2001); Steven Hetcher, *Changing the Social Meaning of Privacy in Cyberspace*, 15 HARV. J.L. & TECH. 149 (2001); Reidenberg, *supra* note 116; Nehf, *supra* note 127; Mary J. Culnan & Robert J. Bies, *Consumer Privacy: Balancing Economic and Justice Considerations*, 59 J. SOC. ISSUES 323 (2003); Schwartz & Treanor, *supra* note 1; Robert Gellman, *A Better Way to Approach Privacy Policy in the United States: Establish a Non-Regulatory Privacy Protection Board*, 54 HASTINGS L.J. 1183 (2003); K. A. Taipale, *Technology, Security and Privacy: The Fear of Frankenstein, the Mythology of Privacy and the Lessons of King Ludd*, YALE J.L. & TECH. (2004-2005); Daniel J. Solove & Chris Jay Hoofnagle, *A Model Regime of Privacy Protection*, 2006 U. ILL. L. REV. 357 (2006); Gaia Bernstein, *The Paradoxes of Technological Diffusion: Genetic Discrimination and Internet Privacy*, 39 CONN. L. REV. 241 (2006); Harry Surden, *Structural Rights in Privacy*, 60 SMU L. REV. 1605 (2007).

[132] Notably, other general trends of the epoch were: (i) a consensus about the necessity of a privacy agency/commission; and (ii) although much less popular, claims for a market/contractual solution (which would allow the market to define the price of personal information) or for maintaining the self-regulation approach (which had been prevalent in the early 1990s). *See e.g.,* Allen, *supra* note 120; Berman & Mulligan, *supra* note 118; Reidenberg, *supra* note 131; Schwartz, *Privacy and Democracy*, *supra* note 117; Rotenberg, *supra* note 131; Shaun B. Spencer, *Reasonable Expectations and the Erosion of Privacy*, 39 SAN DIEGO L. REV. 843 (2002); Joann M. Wakana, *The Future of Online Privacy: A Proposal for International Legislation*, 26 LOY. L.A. INT'L & COMPAR. L. REV. 151 (2003); Gellman, *supra* note 131 (calls for a privacy authority); Steven A. Bibas, Student Competition Winner, *A Contractual Approach to Data Privacy*, 17 HARV. J.L. PUB. POL'Y 591 (1994); Lawrence Lessig, *The Architecture of Privacy*, 1 VAND. J. ENT. L. PRAC. 56 (1999); Schwartz, *Beyond Lessig's Code*, *supra* note 116; Rodney A. Smolla, *Accounting for the Slow Growth of American Privacy Law*, 27 NOVA L. REV. 289 (2002); Paul M. Schwartz, *Property, Privacy, and Personal Data*, 117 HARV. L. REV. 2056 (2004) (for market solutions).

[133] Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules through Technology*, 76 TEX. L. REV. 553 (1998); Reidenberg, *supra* note 131; Lessig, *supra* note 132.

Since around 2010, however, several privacy law scholars participating in PLSC have increasingly begun to recognize the limitations of the FIPs (and the individual privacy rights they offer) in the face of algorithms and the aforementioned novel privacy harms.[134] This acknowledgement, however, has gone through two different phases. During Phase I, scholars grappled with options to either modify the FIPs or complement them. Phase II, which began just recently, has seen a complete rejection of individual rights and a shift to substantive top-down rules.

In spite of other valid classifications, modifications or complements to the FIPs proposed during Phase I could be broadly classified as follows: (i) modified FIPs; (ii) new privacy laws; and (iii) other areas of law.

A first group of scholars initially pursued the mission of proposing certain adaptations for the FIPs, while still preserving them as a valid tool. For example, in 2012 Omer Tene and Jules Polonetsky proposed using a risk matrix to balance the FIPs against additional societal values, such as public health, national security and law enforcement, environmental protection, and economic efficiency.[135] Likewise, in 2013 Eloise Gratton proposed a new interpretation of the concept of *personal information*, while Neil Richards proposed to extend the category of *sensitive data* (known as one of the elements of the global consensus on the key fair information practices) to include reader records.[136] Similarly, there were proposals from Joseph Turow, Chris Jay Hoofnagle, Deirdre K. Mulligan, Nathaniel Good, and Jens Grossklags,[137] Solove,[138] as well as others, to modify *privacy notices*. And in regard to *consent*, which is central to the application of the FIPs, several scholars grappled with the opt-in/ opt-out dichotomy.[139] In

[134] *See e.g.,* Helen Nissenbaum, *Respecting Context to Protect Privacy: Why Meaning Matters*, 24 SCI ENG'G ETHICS 831 (2018); Hartzog & Richards, *Privacy's Constitutional Moment*, *supra* note 117, at 1758; Waldman, *The New Privacy Law*, *supra* note 116; Richards & Hartzog, *A Relational Turn*, *supra* note 117; Allen, *Black Opticon*, *supra* note 116.

[135] Tene & Polonetsky, *supra* note 116.

[136] Gratton, *supra* note 126; Neil Richards, *The Perils of Social Reading*, 101 GEO. L. REV. 689 (2013).

[137] Joseph Turow, Chris Jay Hoofnagle, Deirdre K. Mulligan, Nathaniel Good & Jens Grossklags, *The Federal Trade Commission and Consumer Privacy in the Coming Decade*, 3 I/S: J. L. & POL'Y FOR INFO. SOC'Y 723 (2007-08).

[138] Solove, *The Limitations of Privacy Rights*, *supra* note 116.

[139] *See e.g.*, Mark MacCarthy, *New Directions in Privacy: Disclosure, Unfairness and Externalities*, 6 I/S: Journal of Law and Policy for the Information Society 426 (2011); Omer Tene & Jules Polonetsky, *To Track or "Do Not Track": Advancing Transparency and Individual Control in Online Behavioral Advertising*, 13 Minnesota Journal of Law, Science & Technology 281 (2012); Omer Tene & Jules Polonetsky, *Privacy in the Age of Big Data: A Time for Big Decisions*, 64 Stanford Technology Law Review Online 63 (2012); Richard Warner & Robert H. Sloan, *Behavioral Advertising: From One-Sided Chicken to Informational Norms*, 15 SSRN Journal 49 (2012); Neil Richards, *The Perils of Social Reading*, 101 THE GEORGETOWN LAW JOURNAL 689 (2013); Lauren E. Willis, *Why Not Privacy by*

turn, Solove has recently argued that instead of abandoning the figure of consent, we should strive for a murky consent, one that "embraces the fact that consent in privacy is largely a set of fictions and is at best highly dubious."[140]

A second group of scholars went further, proposing the formulation of new laws that would complement the individual rights already protected by the FIPs, with additional rights and/or tools specifically designed to tackle the novel risks of the digital age. For instance, Sandra Wachter and Brent Mittelstadt proposed reforming data protection laws to include a *right to reasonable inferences*.[141] In the same vein, in 2019, Aaron Fluitt, Aloni Cohen, Micah Altman, Kobbi Nissim, Salome Viljoen, and Alexandra Wood proposed to design regulations to explicitly tackle "the accumulation of privacy risk or harm across a sequence of decisions related to the use of data," a phenomenon they coined as the *composition effects*.[142] Similarly, in 2020, Solon Barocas and Karen Levy called for technologies, policies, and laws that address the mechanisms that create *dependencies*, understood as "the many ways that our privacy depends on the decisions and disclosures of other people."[143]

There is also a group of scholars who have recurred to other areas of law—different from privacy law—to address the newly labeled privacy harms. Drawing on fiduciary and corporate law, Neil Richards and Woodrow Hartzog[144] have built on earlier proposals[145] to suggest a duty of loyalty for personal information. Hartzog himself has also recommended the extension of contract doctrine to

Default?, 29 Berkeley Technology Law Journal 61 (2014); Ira Rubinstein, *Voter Privacy in the Age of Big Data*, 5 Wisconsin Law Review 861 (2014).

[140] Daniel Solove, *Murky Consent: An Approach to the Fictions of Consent in Privacy Law*, 104 B.U. L. REV. (forthcoming 2024).

[141] Wachter & Mittelstadt, *supra* note 116.

[142] Fluitt et al., *supra* note 116.

[143] Barocas & Levy, *supra* note 116, at 555.

[144] Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123 (2007); Neil M. Richards, *Intellectual Privacy*, 87 Tex. L. Rev. 387, 389 (2008) [hereinafter Richards, *Intellectual Privacy*]; Richards, *supra* note 136; Hartzog & Richards, *Privacy's Constitutional Moment*, *supra* note 117, at 1758; Richards & Hartzog, *A Relational Turn*, *supra* note 117; Richards & Hartzog, *Duty of Loyalty*, *supra* note 116; Hartzog & Richards, *Data Loyalty*, *supra* note 117.

[145] *See e.g.*, Michael Harvey, *Confidentiality: A Measured Response to The Failure of Privacy*, 140 U. PENN. L. REV. 2385, 2392 (1992); Randall P. Bezanson, *The Right to Privacy Revisited: Privacy, News, and Social Change, 1890-1990*, 80 CAL. L. REV. 1133, 1133 (1992); Bibas, *supra* note 132, at 592; Richard S. Murphy, *Property Rights in Personal Information: An Economic Defense of Privacy*, 84 GEO. L.J. 2381 (1996); DANIEL SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 9-10 (Jack M. Balkin & Beth Simone Novek eds., 2004); Jerry Kang, Katie Shilton, Deborah Estrin, Jeff Burke & Mark Hansen, *Self-Surveillance Privacy*, 97 IOWA L. REV. 809 (2012); Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1186 (2016); ARI WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE (2018); Jack M. Balkin, *The Fiduciary Model of Privacy*, 134 HARV. L. REV. F 11 (2020).

website design.[146] Several others have proposed intellectual property (IP) law frameworks to address the insufficiencies in privacy law. For example, Paul Ohm has proposed using trademark law to meet the notice deficiencies of privacy law.[147] Similarly, in order to balance the inequities in bargaining power between a consumer and a large corporation, Rachel Wilka proposed incorporating patent law's Reasonable and Non-Discriminatory (RAND) commitments.[148] Finally, plenty of other scholars have kept going back to the origins of privacy law in America, proposing different types of reform for privacy tort law: a reunified common law of torts,[149] a reform to provide meaningful protection for all—including marginalized people,[150] and the strengthening of trust-based torts,[151] among other proposals.

However, several scholars have slowly entered into a second phase, which Margot Kaminski has aptly described as "*regulatory* data privacy law."[152] This new approach implies a complete move away from the FIPs and an adoption of centralized, often *ex ante* democratic governance. Among other manifestations,[153] it argues for substantive, top-down rules for data uses that can effectively "defend people against algorithmic threats."[154]

Since the early 2000's, some scholars, like Mark A. Lemley and Michael Froomkin, had already endorsed some government regulation of data use by data collectors.[155] However, explicit calls to replace procedural requirements with substantive rules have significantly increased in the last few years. For example, since 2020 Hartzog and Richards have repeatedly proposed prohibiting more data practices outright.[156] According to these authors, "[t]he substantive shift we call for will require lawmakers to revisit some basic assumptions about when data collection and processing is desirable and entertains bolder obligations,

[146] *See e.g.*, Woodrow Hartzog, *Website Design as Contract*, 60 AM. U. L. REV. 1635 (2011).

[147] Paul Ohm, *Branding Privacy*, 97 MINN. L. REV. 907 (2013).

[148] Rachel Wilka, *Privacy Commitments*, 93 WASH. L. REV. ONLINE 63 (2018).

[149] Lior Jacob Strahilevitz, *Reunifying Privacy Law*, 98 CALIF. L. REV. 2007 (2010).

[150] SKINNER-THOMPSON, *supra* note 116.

[151] Hartzog & Richards, *Privacy's Constitutional Moment*, *supra* note 117, at 1696.

[152] Margot E. Kaminski, *The Case for Data Privacy Rights (Or, Please, A Little Optimism)*, 97 NOTRE DAME L. REV. REFLECTION 385, 396 (2022).

[153] For example, as part of this *ex ante* governance approach, in 2019 Rory Van Loo proposed ex ante regulatory monitoring of algorithms for privacy and other algorithmic harms. *See* Rory Van Loo, *The Missing Regulatory State: Monitoring Businesses in an Age of Surveillance*, 72 Vanderbilt L. Rev. 1563, 1604 (2019).

[154] Hirsch, *supra* note 116, at 439.

[155] Mark A. Lemley, Comments, *Private Property*, 52 STAN. L. REV. 1545, 1554 (2000); Froomkin, *supra* note 116, at 1524-25.

[156] *See* Hartzog & Richards, *Privacy's Constitutional Moment*, *supra* note 117, at 1696; Richards & Hartzog, *A Relational Turn*, *supra* note 117, at 4; Richards & Hartzog, *Duty of Loyalty*, *supra* note 116; Hartzog & Richards, *Data Loyalty*, *supra* note 117, at 1023.

such as outright bans and moratoria on certain technologies and practices."[157] Similarly, Dennis D. Hirsch has recently stated that "if privacy law is to offer meaningful protection, it must shift from a liberalist focus on individual control, to a social protection model in which public authorities set substantive standards that defend people against algorithmic threats."[158] In other words, it must transition to a model "that empowers public officials to make choices about which predictive analytics practices are safe for individuals and consistent with social values and which are not."[159]

Similar calls have been also heard from Kenneth A. Bamberger and Ariel Evan Mayse. Inspired by Jewish law, these authors suggest that "debates over national and state privacy legislation should focus on categorical rules and prohibitions—both architectural and behavioral—as the mechanisms for protecting privacy."[160] Likewise, Julie Cohen has explicitly encouraged policy-makers to consider privacy bills—like Senator Sherrod Brown's Data Accountability and Transparency Act (DATA Act)—that forbid certain operations from using personal data and prohibit various forms of data-driven discrimination.[161]

To be clear, many scholars in this latter group have been much more ambitious than this, even going so far as to propose a "third way,"[162] "a 'third wave' for Privacy Law,"[163] or a "Post-Modern Privacy."[164] The third way proposed by Hartzog and Richards, for instance, is a comprehensive alternative "that both moves beyond notice and choice and addresses the power dynamics ignored by GDPR-style data protection regimes."[165] In that sense, besides prohibiting certain data practices outright, it includes measures in the following four regulatory landscapes: corporate structure and business incentives, power disparities within relationships, data collection and processing risks, and data externalities.[166] Similarly, Ari Waldman's proposal for a 'third wave' for Privacy Law would leverage alternatives proposed by colleagues such as Danielle Citron, Kristin Johnson, Neil Richards, Woodrow Hartzog, and Julie Cohen, who have talked about civil rights laws, fiduciary duties of care and loyalty, and the regulation of data extractive business models.

In a way, these proposals are holistic approaches that, besides establishing permissible and unacceptable uses of data by means of the law, aim to effectively upset traditional structures of power. Like Professor of Philosophy Gordon Hull,

---

[157] Hartzog & Richards, *Privacy's Constitutional Moment*, *supra* note 116, at 1696-97.

[158] Hirsch, *supra* note 116, at 439.

[159] *Id*. at 462.

[160] Kenneth A. Bamberger & Ariel Evan Mayse, *Pre-Modern Insights for Post-Modern Privacy: Jewish Law Lessons for the Big Data Age*, 36 J.L. & REL. 495, 499 (2021).

[161] Cohen, *supra* note 130.

[162] Hartzog & Richards, *Privacy's Constitutional Moment*, *supra* note 117, at 1694.

[163] Waldman, *The New Privacy Law*, *supra* note 116, at 40.

[164] Bamberger & Mayse, *supra* note 160, at 526.

[165] Hartzog & Richards, *Privacy's Constitutional Moment*, *supra* note 117, at 1696.

[166] *Id*.

many of them consider that, rather than continuing to push forward notice-and-consent and similar theories, "it might make more sense to pursue a second approach: protect the data subject by attacking the power asymmetries that make the subject position a vulnerable one in the first place."[167]

B. Outliers

Evidently, the transformation of the concept of information privacy described here cannot be identified in every piece of scholarship reviewed for this study. As with all trends, the algorithmic turn has not been free of outliers.

Most scholars who can be situated away or detached from the main trend fall into just two categories—critics and outliers *per se*. Although sometimes overlooked, a silent dispute appears to exist between those American privacy law scholars on board of the turn and some who have noticed it and have tried to resist it. The first group of scholars–the critics–have explicitly resisted the turn, opposing either the labeling of the aforementioned new harms as privacy harms, the recurring to privacy law to address them, or the abandonment of the FIPs.

The second group of scholars—the outliers *per se*—, in contrast, have not explicitly stated their position against the algorithmic turn. However, whatever the reason, they seem to have deliberately chosen to avoid using the concept of privacy or privacy law itself to label and address the consequences of the use of algorithmic decision-making systems and artificial intelligence.

An early member of the first group is Daniel J. Steinbock. In 2005 Steinbock published a paper discussing the use of data matching and data mining in law enforcement and civil and administrative determinations such as air passenger screening. According to Steinbock, "[w]hen data manipulation alone produces *tangible consequences* for affected individuals, *the issue is more than one of privacy*."[168] This is rather, he would argue, a discussion about "the due process effects of using data matching and mining to identify persons against whom official action is taken,"[169] which relates to the applicability of either the Due Process Clause or the Fourth Amendment.

Ignacio Cofone has *generally* rejected the inclusion of tangible consequences of the use of personal information ("consequential harms" as he calls them) as part of the privacy harms.[170] According to Cofone, consequential harms

> fall outside what I have defined as privacy harm because they do not attack a privacy interest. Rather, they affect other important interests, such as

[167] Gordon Hull, *The Death of the Data Subject*, 00 Law, Culture and the Humanities 1, 21 (2021).

[168] Daniel J. Steinbock, *Data Matching, Data Mining, and Due Process*, 40 GA. L. REV. 1, 7 (2005).

[169] *Id*.

[170] However, it is important to note that, in his 2019 article *Antidiscriminatory Privacy*, Cofone claimed that discrimination can also be considered an information problem requiring antidiscriminatory privacy rules. *See* Ignacio N. Cofone, *Antidiscriminatory Privacy*, 72 SMU L. Rev. 139 (2019).

> financial or reputational. They are, thus, nonprivacy harms that pertain to privacy law because they also accrue due to the collection, use, or dissemination of personal information. While recent scholarly work persuasively groups them together as privacy harms so as to explain to courts the importance of recognizing them, I believe the distinction can better provide redress while navigating constitutional harm requirements.[171]

Ryan Calo could be said to be another example of a critic. Unlike Steinbock and Cofone, Calo allows some forms of objective/consequential harms to be considered privacy harms.[172] However, he has resisted considering "architectural harms" as privacy harms. "There is no question," Calo argues, "that such architectural harms are important. They are not, however, best thought of as privacy harms. Rather, architectural harms are distinct harms—harms to societal cohesion and trust—that happen to be composed of privacy harms, and often not exclusively."[173] In his view, although important, the loss of values such as civic, artistic, and technological innovation per se is not a privacy harm, but rather a distinct problem to which the loss of privacy may have contributed.

A more recent example of explicit resistance to the algorithmic turn comes from Natali Helberguer. In 2016, while exploring the use of big data and algorithms in the news media, she posed that "when the media profile and target the user to offer more personally relevant services, *not only privacy concerns are at stake*, but broader societal concerns about diversity, information access and the democratic role of the media."[174] She therefore argues that the profiling and targeting of media users and, more generally, the algorithmic making of news should be considered from the sector-specific perspective of media law and policy.

Likewise, in 2017, Pauline T. Kim rejected the use of privacy law to address what she termed as classification bias in the workplace.[175] According to Kim, "privacy protections typically focus on individual harms rather than addressing the group-based disadvantages that are the principal concern of antidiscrimination law."[176] Instead, she proposed rethinking antidiscrimination doctrine (particularly the disparate impact doctrine), so that it can adequately respond to the unique challenges raised by data-driven forms of discrimination.

Salomé Viljoen has also openly expressed the limitations of privacy law to address the harms that stem from the digital economy, mainly arising in ML-

---

[171] Cofone, *supra* note 125, at 1396.

[172] Calo, *Boundaries of Privacy Harm*, *supra* note 122, at 1331.

[173] *Id*. at 1158.

[174] Natali Helberger, *News Readers' Privacy and Fair Algorithmic Media Practices: Lessons to be Learned From Media Law and Theory*, IvIR 1, 2 (2016).

[175] She defines it as "a term that describes the use of classification schemes, such as data algorithms, to sort or score workers in ways that worsen inequality or disadvantage along the lines of race, sex, or other protected characteristics." *See* Pauline T. Kim, *Data-Driven Discrimination at Work*, 58 WM. & MARY L. REV. 857, 857 (2017).

[176] *Id*. at 868.

and AI- based systems.[177] She emphasizes the challenges in addressing "social informational harms"—such as social and economic inequality—, which she defines as "harms that third-party individuals may incur when information about a data subject is collected, processed, or used."[178] In Viljoen's words,

> Privacy and data-governance law have traditionally governed forms of private interpersonal exchange in order to secure the benefits of data-subject dignity or autonomy. Yet as data collection and use become key productive activities (i.e., economic activities that define the contemporary economy as an information economy), new kinds of information-based harm arise.[179]

According to Viljoen, these kinds of harms "will require [instead] democratizing data social relations: moving from individual data-subject rights to more democratic institutions of data governance."[180]

Interestingly, at first glance Viljoen's argument seems to showcase both features of the algorithmic turn: it highlights social and economic inequality as an architectural harm that stems from "the social process this data flow enacts, not the conditions under which it was collected"[181] and proposes a holistic approach as an alternative to the individual data-subject rights. However, she seems to deliberately detach those harms and proposed tools from privacy, moving instead towards a broader theory of data governance.

Lastly, Margot Kaminski has explicitly resisted the second feature of the algorithmic turn (and implicitly done so with regards to the first feature, as will be seen in a moment), namely, the rejection of individual privacy rights. In her essay *The Case for Data Privacy Rights (Or 'Please, a Little Optimism')*, Kaminski makes the case for why individual data privacy rights are necessary.[182] She invites algorithmic turners to think about the practical inconveniences of giving up individual procedural rights just as U.S. states have begun enacting comprehensive data privacy laws. "Lose the FIPs," she claims, "and we lose the thread that has tied the data privacy project together. We lose, in short, what motivates many to call for data privacy law."[183]

In contrast, the group of outliers *per se* is composed of other privacy law scholars who usually address the aforementioned new harms (e.g., discrimination, algorithmic classification, procedural injustices) without bringing privacy into the conversation. One clear example can be seen in Andrew D. Selbst's scholarship. In *Big Data's Disparate Impact,* an article presented along with Solon Barocas at PLSC 2014 and later published in 2016, Selbst and Barocas

[177] Salomé Viljoen, *A Relational Theory for Data Governance*, 131 YALE L.J. 573, 611 (2021).

[178] *Id*. at 586.

[179] *Id*. at 580.

[180] *Id*. at 573.

[181] *Id*. at 615.

[182] Kaminski, *supra* note 152.

[183] *Id*. *at* 388.

address the discriminatory effects of data mining without referencing privacy.[184] Similarly, in a 2021 article, Selbst clearly labels discrimination (also known as fairness in computer science), arbitrary decision-making (generated by the lack of transparency and explainability inherent in black box algorithms), and physical injury (such as those caused by autonomous vehicles and medical devices) as "algorithmic harms."[185] To tackle them, he proposes the use of Algorithmic Impact Assessments (AIA), which despite not directly addressing the harms, can serve as a regime of documentation and knowledge production to better understand their dynamics.[186]

Similarly, Sonia K. Katyal has preferred to refer to discrimination, due process violations, and privacy loss itself as "civil rights concerns."[187] To respond to them, she discusses a variety of tools outside of privacy law, that look to eliminate the opacity of AI and stem from private industry rather than from the government. Among these tools, the codes of conduct, Human Impact Statements in AI, and whistleblower protection are particularly noteworthy.

Finally, Margot Kaminski has recently adopted a similar approach.[188] In a paper where she examines and compares proposed and enacted AI risk regulation regimes, Kaminski uses the term "AI harms" to refer to, among other harms, discrimination and bias. In several instances she compares these harms to privacy harms themselves, therefore making it clear that they are different sets of harms.[189] At one point she even seems to include the privacy harms as part of the AI harms, as in a genus and species relationship.[190]

Why have some scholars adopted the turn, while others have resisted to or just ignored it? And with regard to those who have embraced the turn, why have they done it now? And, maybe more importantly, what are the possible implications of this transformation? My attention will now be turned to these questions.

---

[184] Solon Barocas & Andrew D. Selbst, *Big Data's Disparate Impact*, 104 CAL. L. REV. 671 (2016).

[185] Andrew D. Selbst, *An Institutional View of Algorithmic Impact Assessments*, 35 HARVARD J.L. & TECH. 117, 125 (2021).

[186] *Id*.

[187] Sonia K. Katyal, *Private Accountability in the Age of Artificial Intelligence*, 66 UCLA L. REV. 54, 56-60 (2019).

[188] Margot Kaminski, *Regulating the Risks of AI*, 103 B.U. L. REV. 1347 (2023).

[189] *See id*. For example, within the body of the article she states: "AI harms, *like privacy harms* and public health harms, may be latent in nature—that is, not yet vested. AI harms, *like privacy harms*, are arguably externalities that companies do not yet have an incentive to internalize." *Id*. at 1366 (emphasis added). Likewise, in footnote 92 she points out: "Similar arguments have been made in the data privacy context, analogizing privacy harms to environmental harms." *Id*. at 1368.

[190] *See id*. "Some of the harms caused by AI—physical crashes, incorrect doses of medicine, clearly erroneous decisions—may be more readily quantifiable. Many, however, are not. For example, the development and use of AI systems can cause privacy harms." *Id*. at 1409.

III. POSSIBLE DRIVERS AND IMPLICATIONS OF THIS SOCIOTECHNICAL PHENOMENON

Like contemporary society's algorithmic turn, privacy's algorithmic turn is a sociotechnical phenomenon. As such, both are the result of the complex and two-way relationship between the social and the technical.[191] More specifically, the origin and development of privacy's algorithmic turn in a significant portion of the PLSC scholarship are probably related to what has been taking place in society, technology, the legal system, and in the legal scholars' minds themselves. In the same way, the turn will probably have foreseeable effects on all these different domains.

In this Part, I explore the possible reasons and implications of this algorithmic turn. As will be seen, the transformation here described reflects and reproduces some of the ways in which the social, the technological, the legal, and the cognitive interact and become entangled.

A. Possible Drivers

The easiest way to explain the emergence and development of privacy's algorithmic turn in the scholarship of a significant group of privacy law scholars is to employ a similar argument to the one privacy scholar Neil Richards once used: in the absence of a better term, information privacy is a shorthand to address and talk about Americans' anxiety about novel data-driven harms.[192] Yet, as a sociotechnical phenomenon, privacy's algorithmic turn is much more complex.

This Section aims to explore some of the legal, social, technological, and cognitive conditions that may have contributed to this described shift in information privacy's boundaries. To be sure, the following are not the only possible drivers of the algorithmic turn here described. It is almost certain that many of the internal developments at PLSC,[193] as well as practical reasons[194] may have also greatly impacted the pool of papers and ideas that have been presented and

[191] For a better understanding of sociotechnical phenomena and the questions that can be asked around them, see Danah Boyd, Understanding Socio-Technical Phenomena in a Web2.0 Era, Remarks at the MSR New England Lab Opening (Sept. 22, 2008) (transcript available at https://perma.cc/E3KL-X6M9).

[192] Richards, *Four Privacy Myths*, *supra* note 116, at 59.

[193] E.g., changing from invitation only to an open format in 2021, the transition from open to blind review of papers, a renewed Program and Planning Committee (PPC), a new Chair, or the fact that its current Charter explicitly states that "[t]he PLSC. . . encourages submitted papers that engage with issues of systemic and/or structural bias and inequality." PRIV. L. SCHOLARS CONF., *supra* note 7.

[194] E.g., increased resources devoted by philanthropic foundations to support AI research. Kay Dervishi, *Foundations Seek to Advance AI for Good — And Also Protect the World from Its Threats,* ABC NEWS (Aug. 11, 2023), https://apnews.com/article/ethical-ai-foundations-philanthropy-6021ffd4ca62c7b7064af0e524878307 [https://perma.cc/47L8-S6BK]. Thanks to Elana Zeide for raising this possible driver.

discussed at PLSC year after year. However, rather than identifying with certainty one viable explanation, I intend to use the following list of possible drivers to dig deeper into additional characteristics that make this algorithmic turn novel and worth noting.

1. Americans playing catch up to data protection regulations (the "legal" driver)

One possible explanation of the algorithmic turn is that the American privacy law scholars involved in it are just playing catch-up to data protection as practiced in Europe and elsewhere around the world.[195] As the story goes, American scholars have long recognized the limitations of the American approach to privacy when it comes to commercial surveillance.[196] As a result, the algorithmic turn is simply an effort to broaden the concept of privacy, in order to encompass what in other jurisdictions has already been recognized as the right to data protection.[197]

As Meg Jones and Margot Kaminski clearly point out,

> Data protection arguably has a different scope than privacy—in some ways broader and in some ways narrower. Data protection is limited to covering personal data (versus, say, preventing an intrusion into the home), but follows that data outside of context more traditionally understood to be private. Data protection law, too, often refers to other complementary fundamental rights besides privacy, such as the right to nondiscrimination.[198]

The fact that the post-algorithmic right to privacy—emerging from the algorithmic turn—is expected to protect us against data-driven harms such as algorithmic discrimination, gives some hints of an American move towards a right to data protection. As Eloïse Gratton has aptly stated, "the ultimate purpose [behind the adoption of data protection laws] *was in fact broader than protecting privacy* and . . .. *it was the protection of individuals against the risk of harm,*

[195] This could be said to be partly related to the "Brussels Effect." *See* ANU BRADFORD, THE BRUSSELS EFFECT: HOW THE EUROPEAN UNION RULES THE WORLD (2020).

[196] In an oversimplified manner, this approach involves a sectoral style and a weaponization of the Section 5 of the Federal Trade Commission Act (FTC Act) (15 USC 45), which prohibits "unfair or deceptive acts or practices in or affecting commerce." 15 U.S.C. § 45(a)(1).

[197] In the European Union (EU), for example, the Right to Privacy was included since 1950 in Article 8 the European Convention for the Protection of Human Rights and Fundamental Freedoms (ECHR). However, in 2000 the Right to Data Protection emerged as a fundamental and independent right, being established in Article 8 of the Charter of Fundamental Rights of the European Union, the only EU-specific catalogue of fundamental rights recognized by EU law. The Charter became binding on EU Member States with the entry into force of the Treaty of Lisbon in December 2009. Consequently, in 2018 the General Data Protection Regulation (GDPR) went into effect, focusing on "all fundamental rights and freedoms of natural persons and in particular their *right to the protection of personal data*."

[198] Meg Leta Jones & Margot E. Kaminski, *An American's Guide to the GDPR*, 98 DENV. L. REV. 93, 100-01 (2021).

which may take place upon organizations collecting, using and disclosing their personal information."[199] Thus, by aiming to tackle data-related harms *in general*, both the right to data protection and the post-algorithmic right to privacy end up encompassing interests additional to those of privacy, such as equality and due process.

But the streak of similarities comes to a halt when it comes to the tools proposed to address those harms. Data protection laws around the world have tended to put in place what Margot Kaminski has appropriately described as a "binary system of governance:" a combination of individual rights—mainly stemming from the implementation of the FIPs—and systemic accountability mechanisms, such as Data Protection Impact Assessments (DPIAs), ex ante technical requirements, audits, and certification schemes.[200]

However, this is not exactly what we see reflected in the scholarship of the participants of the algorithmic turn. Instead of promoting the implementation of more procedural requirements, participants of the turn appear to be moving away from FIPs and from any type of voluntary accountability mechanism. In contrast, they are time and again calling for what many European scholars highlight as one of the main characteristics of privacy (in contrast to data protection): the making of normative choices and the establishment of prohibition rules.[201] Thus, while data protection trends tend to lay out the legal conditions and procedures through which data can be processed, algorithmic turners push for the formulation of more substantive rules that set normative limits to the processing of data.

Likewise, due to their emphasis on individual rights, data protection regulations do not respond to the architectural, structural, and systemic harms that the participants of the algorithmic turn are mainly focused on. As Lilian Edwards and Michael Veale point out, "a focus on data protection remedies makes an individual's rights approach inevitable. Data protection is a paradigm based on human rights which means it does not contemplate, as discussed above, remedies for groups."[202] Similarly, Elettra Bietti has also pointed out how the European regulation

> remains nonetheless grounded in procedural and neoliberal paradigms: the primacy of individual rights, individual choices, and self-determination. Data protection's 'dignitarian' focus on individual rights, choice, and control does not capture the most salient aspects of data in platform

[199] Gratton, *supra* note 126, at 141.

[200] Margot E. Kaminski, *Binary Governance: Lessons from the GDPR's Approach to Algorithmic Accountability*, 92 SOUTHERN CALIF. L. REV. 1529, 1540 (2019).

[201] *See e.g.*, Paul De Hert & Serge Gutwirth, *Privacy, Data Protection and Law Enforcement: Opacity Of the Individual and Transparency of Power*, *in* PRIVACY AND THE CRIMINAL LAW (E. Claes, A. Duff & S. Gutwirth eds., 2006).

[202] Edwards & Veale, *supra* note 2, at 74.

> ecosystems. Data is relational and collectively constructed in ways that individual consent or self-determination guarantees cannot alone address.[203]

Thus, while the right to privacy that results from the algorithmic turn shares some characteristics with the right to data protection protected in Europe and elsewhere around the world, it goes further. In particular, the tools that scholars adhering to the turn propose to protect privacy are different from what we see put in place by data protection laws around the world. Similarly, the harms they want privacy to address are, although related (all data-driven), of a different nature.

2. A win-win strategic movement (the "social" driver)

A second possible explanation of the algorithmic turn may be related to a strategic choice of the American privacy law scholars that are part of it. For years, privacy scholars have denounced how difficult it is for claimants of a privacy harm to be heard in an American court and receive relief.[204] "Through harm requirements," Danielle Keats Citron and Daniel Solove claim, "courts have made the enforcement of privacy laws difficult and, at times, impossible."[205] Thus, by adding further requirements, mandating proof of harm even for statutes that include statutory damages, and adopting narrow conceptions of cognizable harm, courts have set a very high threshold for privacy harm.

To cope with this frustration, American privacy law scholars have adopted different strategies. Of course, there have been innumerable attempts to help courts understand privacy harms.[206] However, scholars have also recurred to what late Joel R. Reindenberg used to call "tertiary claims."[207] According to Reindenberg, "[t]he lack of fundamental statutory protection forces government actors to find tertiary rights for the assertion of privacy claims."[208] Similarly, the lack of an enforceable right has forced privacy scholars to rely on tertiary rights to protect privacy values. Thus, as government officials resort to trade practice

---

[203] Elettra Bietti, *A Genealogy of Digital Platform Regulation*, 7 GEO. L. TECH. REV. 1, 47 (2023).

[204] *See e.g.,* Jacqueline D. Lipton, *Mapping Online Privacy*, 104 NW. U.L. REV. 477, 508 (2010) ("Delineating remediable harms has been a challenge for law and policy makers since the early days of the Internet."); Ryan Calo, *Privacy Harm Exceptionalism*, 12 COLO. TECH. L.J. 361, 361-63 (2014) [hereinafter Calo, *Privacy Harm Exceptionalism*]; Daniel J. Solove & Danielle Keats Citron, *Risk and Anxiety: A Theory of Data-Breach Harms*, 96 TEX. L. REV. 737, 739 (2018); Ignacio N. Cofone & Adriana Z. Robertson, *Privacy Harms*, 69 HASTINGS L.J. 1039, 1041 (2018); Lauren H. Scholz, *Privacy Remedies*, 94 IND. L.J. 653 (2019; Citron & Solove, *supra* note 116; Cofone, *supra* note 125.

[205] Citron & Solove, *supra* note 116, at 800.

[206] *See e.g.,* Calo, *Privacy Harm Exceptionalism*, *supra* note 204; *see also* Solove & Citron, *supra* note 204, at 737-38; Citron & Solove, *supra* note 116; Cofone & Robertson, *supra* note 204.

[207] Reidenberg, *supra* note 116, at 885.

[208] *Id*.

legislation (the FTC's "unfair and deceptive trade practice" jurisdiction) to safeguard privacy, scholars propose creative connections between privacy and sounder rights that have stronger protections and can stand up to countervailing values.

This is the case, for example, of the multiple connections that have been emphasized in American scholarship between privacy and the right to freedom of speech, which unlike the former, has explicit protection in the U.S. Constitution.[209] Neil Richards, for instance, proposes the concept of intellectual privacy and locates it within First Amendment theory. As Richards himself explains:

> Information relating to intellectual activity is increasingly being created, tracked, and maintained by government and private entities. Such information practices have conventionally been thought of as raising privacy concerns, *but privacy has frequently failed to stand up to the countervailing interests that have been arrayed against it*. Intellectual privacy, I would suggest, represents a more helpful way of looking at these problems because it illuminates the First Amendment values at stake. Understanding these problems in this way allows us to appreciate their true importance to our constitutional culture and *to think more creatively about possible solutions*.[210]

Similarly, Scott Skinner-Thompson suggests the concept of performative privacy, grounding it too in the First Amendment doctrine. According to him,

> [B]y demonstrating that demands for public privacy are often (but not always) imbued with expression, this Article's concept of performative privacy *helps establish that public privacy is grounded in the First Amendment's speech protections and that existing jurisprudence provides doctrinal support for a right to performative privacy in public*.[211]

In this sense, highlighting the importance of privacy values for the protection and exercise of other stronger rights has been a recurrent strategy of privacy scholars to increase the chances of legal protection.

Considering this old approach, privacy's algorithmic turn could be seen as a novel strategy to ensure the protection of privacy. How would this new strategy work? By broadening the range of harms that are considered a privacy harm, participants of the algorithmic turn would strengthen privacy in two ways: First, by allowing privacy to have more cognizable harms with seemingly better possibilities to be recognized in court; and second, by increasing its moral significance.

Objective/consequential harms, like the ones the participants of the algorithmic turn focus on, are said to be more cognizable and easier to apply as a basis

---

[209] While the right to freedom of speech is explicitly protected by the First Amendment, the source of the federal constitution's right to privacy has been said to be found in the penumbras of the Bill of Rights. *See Griswold v. Connecticut*, 381 U.S. 479, 484 (1965).

[210] Richards, *Intellectual Privacy*, *supra* note 144, at 427 (emphasis added).

[211] Scott Skinner-Thompson, *Performative Privacy*, 50 U.C. DAVIS L. REV. 1673, 1677 (2017) (emphasis added).

for substantial legal responses. As Tal Zarsky has recently argued, traditional theories justifying the protection of privacy rights, which link the protection of privacy to the promotion of control, access, intimacy, or autonomy, are weak in part because they are highly abstract and lack concrete harms. In contrast, harms like online manipulation are much easier to conceptualize and grasp. "The manipulation justification provides for promoting an intuitive reason for data protection or other appropriate regulatory steps, given an identifiable and concrete issue."[212]

Likewise, he states, recurring to manipulation helps us to sidestep doctrinal pitfalls that privacy law currently comes up against, such as the presence of apparent consent and the need to determine whether Personal Identifiable Information (PII) or merely anonymous data was used in the process that generated the manipulation. As Zarsky points out, "[w]hen regulation will in fact strive to protect individuals from such manipulations, the fact that the personal data facilitating the process was collected willfully does not necessarily matter. The manipulative actions are still normatively wrong and therefore should be positively prohibited."[213] Similarly, "[s]hifting the focus towards the manipulative aspects of the firms' actions will potentially enable effective regulation of these targeting entities and practices regardless of their anonymization attempts."[214]

Zarsky is not alone in this claim. Similarly, Shaun B. Spencer has also stated that, "given the stark nature of the threat that online manipulation poses, adding online manipulation to the list of potential data harms may increase support for comprehensive data protection legislation."[215] For both Zarsky and Spencer, the addition of more objective harms into the privacy umbrella strengthens privacy by making more concrete what privacy's absence would represent.

Besides, the expansion of the umbrella of privacy harms could also contribute to increase the "moral significance of privacy."[216] The addition of harms such as algorithmic discrimination into the privacy umbrella has turned privacy into a temporal shelter for values that find protection in no other corner of the legal system. Margaret Hu, for example, recommends relying on privacy theories as a temporal measure, at least until the current equal protection framework evolves enough to encompass the disparate-impact harms of "Algorithmic Jim Crow" regimes.[217] Relatedly, Skinner-Thompson proposes using the right to privacy to provisionally protect marginalized communities. According to him, "privacy can serve as a liminal or transitional right until such communities gain both

[212] Tal Z. Zarsky, *Privacy and Manipulation in the Digital Age*, 20 THEOR. INQ. L. 157, 164 (2019).

[213] *Id*. at 166.

[214] *Id*. at 167.

[215] Shaun B. Spencer, *The Problem of Online Manipulation*, 3 U. ILL. L. REV. 959, 1005 (2020).

[216] DANIELLE K. CITRON, THE FIGHT FOR PRIVACY. PROTECTING DIGNITY, IDENTITY AND LOVE IN OUR DIGITAL AGE xvii (2022).

[217] Margaret Hu, *Algorithmic Jim Crow*, 86 FORDHAM L. REV. 633 (2017).

formal antidiscrimination protections and lived equality."[218] In this way, equality values can take advantage of the momentum that privacy has gained lately in the legislative arena, while privacy itself gains moral importance, and with it, new allies and advocates who support its fight.

3. Salient dimensions of data (the "technical" driver)

Another possible explanation of privacy's algorithmic turn stems from the datafication context. Most participants of the algorithmic turn seem to agree on the necessity for information privacy to evolve to address two dimensions of data that algorithms have made particularly *salient*.[219]

The first dimension is the relational character of data.[220] Besides individual data, people's privacy decisions are made over *interrelated* data (data that can be used to infer data about others).[221] My behavioral characteristics are *interrelated* data, because analyzed under the right algorithms, they can be used to make inferences about other people classified in my same market segments (e.g., women, Latinas, lawyers, etc.). Therefore, whenever I choose to share any of this information, I am not only deciding over my data but the data of others. In the same way, misuse of my data can not only cause individual but also collective, structural, and systemic harms.

This relational dimension, sometimes referred to as or included in the expressions "negative privacy externalities,"[222] "networked privacy,"[223] "privacy

[218] SKINNER-THOMPSON, *supra* note 116, at 181.

[219] I use the term "salient" here deliberately. In doing so, I adhere to Jack Balkin's rejection of the term "novel." According to Balkin,

[i]n studying the Internet, to ask 'What is genuinely new here?' is to ask the wrong question. If we assume that a technological development is important to law only if it creates something utterly new, and we can find analogues in the past—as we always can—we are likely to conclude that because the development is not new, it changes nothing important. That is the wrong way to think about technological change and public policy, and in particular, it is the wrong way to think about the Internet and digital technologies. *Instead of focusing on novelty, we should focus on salience*. What elements of the social world does a new technology make particularly salient that went relatively unnoticed before? What features of human activity or of the human condition does a technological change foreground, emphasize, or problematize?

Jack M. Balkin, *Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society*, 79 N.Y.U. L. REV. 1, 2 (2004).

[220] This characteristic should be distinguished from the social value of privacy, which has been highlighted by American privacy law scholars since the time of the "new privacy." *See supra* note 14.

[221] Solove, *The Limitations of Privacy Rights*, *supra* note 116.

[222] Mark MacCarthy, *New Directions in Privacy: Disclosure, Unfairness and Externalities*, 6 J. Law Policy Inf. Soc. 426 (2011).

[223] Alice E. Marwick & Danah Boyd, *Networked Privacy: How Teenagers Negotiate Context in Social Media*, 16 NEW MEDIA & SOC'Y 1051 (2014).

dependencies,"[224] or "data's relationality,"[225] has driven some scholars to question the usefulness of the individual privacy rights and remedies endorsed by the "new privacy." At least—participants of the algorithmic turn claim—it makes evident their limitations in an information economy where more and more data is *interrelated*, and where, therefore, our privacy, and related rights and values not only depend on our exercise of those rights but on the decisions and disclosures of other people.

The second dimension of data, increasingly highlighted by PLSC scholars in the last few years, relates to data exploitation's capacity to fuel massive power asymmetries. "Information is power"[226]—Neil Richards and several others would say—and power is currently concentrated in the hands of a few tech companies who weaponize data and data-driven algorithms to influence and manipulate us. Even more, different scandals have made evident that data can be a tool of discrimination, oppression, and subordination, "whether it is exploited to train totalitarian facial recognition models, surveil protestors, incarcerate people, or subjugate vulnerable populations."[227] As time passes, it becomes increasingly apparent that privacy "is [really] about how power is distributed and wielded."[228]

To be clear, references to power asymmetries in privacy law scholarship are not new. As Neil Richards pointed out in his 2006 article,[229] since the late 90's and early 2000's, members of the "new privacy," such as Julie Cohen,[230] Paul Schwartz,[231] and Daniel Solove,[232] have been repeatedly claiming that the collection and use of personal information conceal power relationships and allow for the emergence of new structures of power over individuals.

However, two things appear to have changed: the number of scholars talking about power asymmetries, as well as the approach taken to address them. In recent years, claims about the exacerbation of power asymmetries have become widely shared by most members of the PLSC community. Among others, one possible explanation may have to do with the increasing importance of Political Economy in traditional privacy law scholarship.[233] As time passes and

[224] Barocas & Levy, *supra* note 116.

[225] Viljoen, *supra* note 177.

[226] NEIL RICHARDS, WHY PRIVACY MATTERS 3 (2021).

[227] Waldman, *Privacy, Pratice, and Performance*, *supra* note 116, at 1264.

[228] Hartzog & Richards, *Privacy's Constitutional Moment*, *supra* note 117, at 1695.

[229] *See* Neil Richards, *The Information Privacy Law Project*, 94 GEO. L.J. 1087, 1102-1103 (2006).

[230] *See e.g.*, Julie Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981-1039 (1996); Cohen, *Examined Lives*, *supra* note 117; Cohen, *Turning Privacy Inside Out*, *supra* note 116, at 1.

[231] *See e.g.,* Schwartz, *Beyond Lessig's Code*, *supra* note 116.

[232] *See e.g.,* Solove, *supra* note 131; Solove, *Conceptualizing Privacy*, *supra* note 118; SOLOVE, *supra* note 145; Solove, *supra* note 129.

[233] To be clear, this is not a new topic in fields like Communication or Political Science. *See e.g.*, THE POLITICAL ECONOMY OF INFORMATION (Vincent Mosco & Janet Wasko eds.,

interdisciplinarity grows in the privacy field and in the PLSC community in particular, more and more privacy law scholars integrate Political Economy into their areas of expertise.[234] Thanks to the methods and the particular focus of this field, in recent years the distribution of resources and power has become an increasingly dominant theme in the scholarship of privacy law scholars studying the digital economy.

Moreover, the approach taken to address these asymmetries of power appears to have changed as well. Unlike in the late 1990s and early 2000s, when most privacy law scholars suggested empowering consumers through privacy rights as the most popular way to balance power relationships, many of the current proposals showcased in Part II.A.2 seek to balance these power relationships by taking power *away* from corporations.

4. New techno-legal imaginaries (the "cognitive" driver)

In 2006, Jack Balkin and Reva Siegel proposed the notion of "imagined regulatory scenes" to describe "a set of background understandings about the paradigmatic cases, practices, and areas of social life to which [legal principles] (…) properly apply."[235] Building on this concept, in 2022 Margot Kaminski argued that

> technology (or really, the social use of technology) can alter the imagined setting around which policy conversations take place —what Jack Balkin and Reva Siegal call the "imagined regulatory scene." Sociotechnical change can alter the imagined regulatory scene's architecture, upsetting a policy balance and undermining a particular regulation or regime's goals.[236]

Drawing on Kaminski's interpretative framework, one could say that the two aforementioned salient dimensions of data—its relational character and its capacity to fuel massive power asymmetries—are altering the architecture of the imagined regulatory scene to which information privacy law used to apply. As a result, they have undermined *the goals of the regime*, here referred to as the "techno-legal imaginaries."

I define "techno-legal imaginaries" as the visions of a given legal community—in this case, legal scholars—about the desirable futures that could be

1988); OSCAR H. GANDY, JR., THE PANOPTIC SORT: A POLITICAL ECONOMY OF PERSONAL INFORMATION (1993); COLIN J. BENNETT, THE PRIVACY ADVOCATES: RESISTING THE SPREAD OF SURVEILLANCE (2008). Despite this, many American privacy law scholars had until recently overlooked its significance in their own intellectual pursuits.

[234] Thank you to Sebastian Benthall for bringing this idea to my attention, both at the 4th Symposium on Applications of Contextual Integrity and in the Privacy Research Group at the NYU Information Law Institute.

[235] Jack M. Balkin & Eva B. Siegel, *Principles, Practices, And Social Movements*, 154 U. PENN. L. REV. 927, 928 (2006).

[236] Margot E. Kaminski, *Technological "Disruption" of the Law's Imagined Scene: Some Lessons from Lex Informatica*, 36 BERKELEY TECH. L.J. 883, 883 (2022).

achieved through the regulation of technoscientific innovation. Techno-legal imaginaries have the power to shape how sociotechnical legal problems are imagined and shaped and how they are answered in different legal communities. In that sense, their change may be another possible explanation of the algorithmic turn.

When Samuel Warren and Lous Brandeis proposed the right to privacy in 1890, they envisioned a future where individuals enjoy sanctuary spaces "beyond which neither government nor private power can push."[237] When the "new privacy" described by Schwartz and Treanor came around, scholars seemed to have a different perspective about the desirable future they ambitioned privacy would take them to. Faced with the modern bureaucratic state, these scholars wanted privacy to further the development of autonomous individuals who could contribute to innovation and democracy. [238] In that sense, they envisioned autonomous individuals and a creative and democratic society.

Today, privacy's algorithmic turn signals how several American privacy law scholars now have more ambitious expectations of what information privacy should do for individuals (and society as a whole). From an instrument for individual autonomy (and consequent collective benefits), information privacy is gradually turning into a tool for social justice. Thus, besides fostering informational self-determination, innovation, and democracy, information privacy is now also expected to help the government to protect citizens (and vulnerable populations, in particular) against data extraction and its consequent power asymmetries.

For example, when suggesting the "third way" they talk about, Hartzog and Richards refer to "a more nimble, layered, and inclusive approach that protects personal data but *also looks beyond it to account for things that data protection often fails to consider: power, relationships, abusive practices, and data externalities*."[239] Relatedly, when Ari Waldman proposes a 'third wave' for privacy law, he envisions it to allow us to "look beyond the narrow confines of what passes for privacy regulation in the U.S. and consider new legal paradigms *that can rein in data extraction and its attendant power asymmetries and injustices*."[240] In a similar vein, as Anita Allen proposes her African American Online Equity Agenda, she notes that "[t]he new generation of laws would ideally include provisions specifically geared toward *combatting privacy- and data-protection-related racial inequalities enabled by online platforms*."[241]

In the minds of several of the participants of privacy's algorithmic turn, information privacy law should not only realize a desirable future where

[237] Charles Reich, *The New Property*, 73 YALE L.J. 733, 785 (1964).

[238] Schwartz & Treanor, *supra* note 1, at 2180.

[239] Hartzog & Richards, *Privacy's Constitutional Moment*, *supra* note 117, at 1694 (emphasis added).

[240] Waldman, *The New Privacy Law*, *supra* note 116, at 41 (emphasis added).

[241] Allen, *Black Opticon*, *supra* note 116, at 910 (emphasis added).

individuals are autonomous and in control of what happens to their data.[242] Rather, privacy is expected to take society to a much more ambitious future, where the information economy's data extractive business model has limits, big tech actors' power is reined in and redistributed and, therefore, individuals and social groups can effectively achieve social justice and equality.

In his essay *Data and the Good?*, Daniel Susser encourages surveillance studies scholars and privacy scholars—himself included—to put forward alternative substantive conceptions of a good digital society.[243] Drawing on Sheila Jasanoff and Sang-Hyun Kim's concept of "sociotechnical imaginaries," he asks scholars to develop "new understandings of the goals and aspirations digital technologies should aim to achieve."[244] I am not completely sure that the scholars' "ideas about what data-driven technologies could do and mean"[245] could be described as "sociotechnical imaginaries."[246] I can, however, state with certainty that American privacy law scholars do have visions of the desirable futures that could be achieved *through the regulation of technology*. And that those visions may have recently changed.[247]

B. Possible Implications

Privacy's algorithmic turn can, as seen, be a response to a combination of several factors, such as changes in legal systems around the world, social circumstances, technological developments, or even the scholars' evolving normative commitments. Even more relevant, however, are the following implications, which not only may affect the concept of information privacy, but the field of information privacy law as a whole.

1. A potential threat to information privacy's instrumental efficacy (in favor of its symbolic value)

The first feature of privacy's algorithmic turn (novel information privacy harms) awakens worries about the internal coherence of the concept of information privacy. As Ryan Calo and I contend in *Distinguishing Privacy Law: A Critique of Privacy as Social Taxonomy*, as more data-driven harms are

[242] According to Ari Waldman, for example, "Second wave practices, governance, and ideology suggest that these laws see *privacy as an individual right to control what happens to one's data*. Whether these proposals can achieve that — *and whether that is the goal we need from privacy law — is contestable*." Waldman, *The New Privacy Law*, *supra* note 116, at 37-38 (emphasis added).

[243] Daniel Susser, *Data and the Good?*, 20 SURVEILLANCE & SOC'Y 297 (2022).

[244] *Id*. at 297.

[245] *Id*. at 300.

[246] I have struggled myself with adopting this concept in *meso* environments, such as when it comes to a professional field or a group of people. For a further discussion of this issue, see Part I in María P. Angel, *Understanding the Techno-legal Imaginaries of American Privacy Law Scholars,* 2023 We Robot Conference (forthcoming) (on file with author).

[247] For a further discussion of this change, see *id*.

recognized as privacy harms, the concept of information privacy broadens, starting to encompass more general values and additional individual rights.[248] While this has been beneficial for the growth and flourishing of the field,[249] it risks diffusing the concept into a meaningless catchall term,[250] or even worse, collapsing it into broader and more established fields of law, such as consumer protection.[251]

How capacious can the concept of information privacy be and still retain coherence? In answering this type of question usually posed by philosophers,[252] Anita Allen—a philosopher herself—argues that philosophically technical prescriptive definitions "often proceed in a political vacuum, seemingly oblivious to the politics of privacy,"[253] and "are not clarifying for most practical purposes, and invite frustrated dismissal of privacy claims as too conceptually vague or contentious for law or policy."[254] According to Allen, limiting the scope of such a political concept strips vulnerable populations of a powerful tool that allows them to speak out against injustices they are experiencing.

Daniel Solove offered a similar response some time ago. In 2007, when explaining his pluralistic conception of privacy—earlier materialized in his 2006 taxonomy of privacy—he argued:

> Some might object to the lack of clear boundaries, but this objection assumes that having definitive boundaries matters. The quest for a traditional definition of privacy has led to a rather fruitless and unresolved debate. *In the meantime, there are real problems that must be addressed, but they are either conflated or ignored because they do not fit into various prefabricated conceptions of privacy*. The law often neglects to see the problems and instead ignores all things that do not fall into a particular conception of privacy. In this way, *conceptions of privacy can prevent the examination of problems*. The problems still exist regardless of whether we classify them as being "privacy" problems."[255]

There is no doubt that Allen and Solove are right. If privacy has an agenda setting power—as it certainly does today—it is more than wise to use its symbolic efficacy to raise awareness of neglected societal harms. In fact, that is partly what I alluded to when describing the "win-win strategic movement"

[248] María P. Angel & Ryan Calo, *Distinguishing Privacy: A Critique of Privacy as Social Taxonomy*, 124 COLUM. L. REV. 2 (2024).

[249] Hartzog, *supra* note 4, at 1681.

[250] *See* Calo, *Boundaries of Privacy Harm*, *supra* note 122, at 1137.

[251] *See* Zarsky, *supra* note 212, at 168.

[252] Anita L. Allen, *Privacy, Health, and Race Equity in the Digital Age,* 22 AM. J. BIOETHICS 60, 61 (2022) ("Philosophers often see their contribution to learning as what I call 'analytic definitional prescription'—prescribing ideal definitions of terms like 'privacy' to guide clear thinking and coherent practice.").

[253] *Id*.

[254] *Id*. at 62.

[255] Solove, *Misunderstandings of Privacy*, *supra* note 118, at 759 (emphasis added).

driver. As Allen argues, it is the responsibility of philosophers—or policymakers more prominently—and not of vulnerable groups "to understand and uncover what is being sought and withheld through privacy discourse and explain why it matters."[256]

However, the problem arises when, beyond drawing attention to ignored harms, privacy does not offer effective tools to address them. Or even worse, when by doing so, information privacy undermines its own instrumental efficacy as a legal tool.

Certainly, partly as a result of the now common association between algorithmic discrimination and information privacy, equality advocates were able to see, for example, a Civil Rights Protections Section in the American Data Privacy and Protection Act ("ADPPA"). Although unsuccessful in Congress, the last version of the ADPPA included a section (207(a)) prohibiting covered entities to "collect, process, or transfer covered data in a manner that discriminates in or otherwise makes unavailable the equal enjoyment of goods or services on the basis of race, color, religion, national origin, sex, or disability."[257]

This bill's approach (commonly referred to as "binary governance"[258]), however, is not effective to tackle most of the other novel types of harms that the participants of the algorithmic turn care about. Indeed, that is precisely the reason why these scholars have gradually moved away from individual data privacy rights and towards a *regulatory* information privacy law. According to the participants of privacy's algorithmic turn, individual rights and compliance mechanisms by themselves do not upset the power asymmetries currently in play against individuals. Therefore, when it comes to America, information privacy may raise awareness about these issues, but as of today, it does not possess particular comparative advantages for tackling most of them.

Likewise, when it comes to addressing these novel harms in court, the outlook does not look better. Despite the optimism about the cognizable character of the new type of harms,[259] due to their objective and architectural nature, providing proof of their existence in court will not be easy. As Cofone has rightly claimed, "these consequential injuries often do not materialize until much later and, when they materialize, causality is extremely difficult to establish, leading to such injuries frequently being left unaddressed."[260] Besides, the architectural nature of harms such as online manipulation could make them in some cases similar to generalized grievances. "Privacy-reducing actions that produce generalized grievances," Cofone highlights, "are a bad candidate for standing because, by definition, everyone suffers their effects in an undifferentiated way. Therefore,

[256] Allen, *supra* note 252, at 62.

[257] American Data Privacy and Protection Act, H.R. 8152, 107th Cong. § 207(a) (2022).

[258] *See* Kaminski, *supra* note 200, at 1552-81.

[259] As exposed in Part III.A.2 of this Article.

[260] Cofone, *supra* note 125, at 1372.

these losses would keep failing to meet the particularity requirement under Supreme Court case law."[261]

Finally, including these novel harms in the existing list of privacy harms may even worsen the chances that "traditional" privacy harms—such as emotional stress caused by a privacy loss—have to be recognized in court. By adding objective harms that stem from the actual processing of data, courts will probably have even more reasons than before to dismiss any dignitary/, subjective/, or intrinsic privacy harms unless the processing of the breached data generates *another* downstream privacy harm. As Ignacio Cofone has pointed out, "[w]hat is needed, instead, is a way to identify privacy injuries even when consequential harms (such as Financial) are absent."[262]

As seen, the possible diffusion of the concept of information privacy into a meaningless catch-all term is not simply a semantic issue. Rather, it implies a renunciation of the instrumental efficacy of privacy in favor of its symbolic value.

2. The emergence of a new privacy paradigm

On a more positive note, the second feature of privacy's algorithmic turn (a transformation of the tools proposed as part of privacy law) has a different implication: it signals that a portion of American privacy law scholars may be finally moving forward and detaching privacy from the control paradigm proposed by Alan Westin, Jerry Kang, and others long time ago.[263] Since the early 2000's, several scholars have been arguing that "alternatives to the privacy-as-data control paradigm are needed to guide our urgent philosophical and policy understandings of privacy and its protection in the age of the Internet."[264] Until very recently, however, it was still unclear what the new paradigm would look like. Finally, it seems like a considerable group of American privacy law scholars are beginning to walk together towards what Dennis Hirsch has termed as a "protection paradigm."[265]

Despite some remaining concerns,[266] it appears that worries about the paternalistic nature of this approach have been mostly overcome.[267] There is,

[261] *Id*. at 1407-08.

[262] *Id*. at 1373.

[263] ALAN F. WESTIN, PRIVACY & FREEDOM (1967); Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193 (1998).

[264] Anita L. Allen, *Privacy-as-Data Control: Conceptual, Practical, and Moral Limits of the Paradigm*, 32 CONN. L. REV. 861, 862 (2000).

[265] Hirsch, *supra* note 116, at 462.

[266] *See e.g.*, Solove, *supra* note 140 (manuscript at 44) ("Privacy law should focus primarily on issues of structure and power. But a regime of privacy regulation cannot exclude consent without becoming too paternalistic").

[267] *See e.g.*, Cohen, *Turning Privacy Inside Out*, *supra* note 116, at 24 ("Protecting privacy effectively requires a willingness to depart more definitively from subject-centered

however, still a lot to discuss with regard to defining how this new paradigm should operate in practice. In particular, at present there are only a few examples of how the different protection-type proposals could play out as a regulatory *system*.

For instance, in *Privacy's Constitutional Moment and the Limits of Data Protection*, Woodrow Hartzog and Neil Richards offer a framework of privacy governance composed of four related and overlapping landscapes for privacy regulation: corporal, relational, informational, and external.[268] According to the scholars,

> Each landscape invokes a different set of rules, structural changes, and dynamics. . . . *Corporal* privacy rules would include structural questions regarding the corporate form and piercing the corporate veil, corporate licensing and registration requirements, and taxation issues. Meanwhile, *Relational* privacy rules would look to the relative power disparities within information relationships and the vulnerabilities of those who expose themselves to data collectors. *Informational* protection rules focus on data like the fair processing requirements of the GDPR that follow the data regardless of corporal form or the nature of relationships between parties. The final tier of laws would target External consequences—the external costs (what an economist would call "externalities") imposed on society by the personal data industrial complex, including environmental pollution, corrosion of democratic self-governance, and reduced well-being through the hijacking of attention.[269]

Similarly, in *The Case for Data Privacy Rights (Or 'Please, a Little Optimism')* Margot Kaminski has also offered a brief sketch of what a regulatory data privacy law would look like "in a perfect world." Although clearly skeptical about its achievability and critical about its expected outcomes, Kaminski pictures the following:

> It probably starts with some bans: . . . Then they come up with exceptions to the bans. Then they mandate some design elements (like prominent visceral notice and clear consent streams), while prohibiting others (like dark patterns). Maybe they institute licensing requirements: you can't process or use personal data without approval of your practices by a regulator. . . . An enforcing agency probably conducts rulemaking to get public input into clarifying everything (the bans, the exceptions, the design requirements, the licensing standards), and maybe issues ongoing cyclical guidance in consultation with a variety of stakeholders. Then they build up a huge,

frameworks in favor of condition-centered frameworks — and to refrain from labeling the latter as offensive because they are 'paternalistic.'").

[268] Hartzog & Richards, *Privacy's Constitutional Moment,* supra note 117, at 1738-60.

[269] *Id*. at 1740-41.

costly, expert enforcement apparatus, monitor the market for wrongdoings, and impose big sanctions when they happen.[270]

Would these different models be politically feasible and constitutionally invulnerable?[271] What exact types of bans, design requirements, and licensing standards would make sense *as a system*? Although the "protection paradigm" seems to have already emerged, the way in which the different proposed measures would interact with and complement each other is still to be defined.

3. An open window for impact on American public policy about privacy

In the 117th legislative session, the U.S. public policy discussion about privacy revolved mainly around ADPPA, the first U.S. federal privacy bill to gain bipartisan support.[272] This bill, whose legislative path was "the closest U.S. Congress has ever been to passing comprehensive federal privacy legislation," not only reflects the "Brussels Effect" of the General Data Protection Regulation (GDPR),[273] but also resembles ideas *long* held by American privacy scholars about the need for individual data privacy rights.

As Schwartz and Treanor clearly described in 2003, as early as 1999 participants of the "new privacy" advocated for the mandatory implementation of the FIPs. "A more comprehensive incorporation of the Fair Information Practices, as developed by HEW and expanded upon by the OECD and the European Union Privacy Directive, would go far towards addressing the privacy problem as I have characterized it,"[274] argued Daniel Solove back in 2001. However, it took policymakers around twenty years to take these ideas seriously. And, as I hope to have shown throughout this article, they are no longer part of the privacy discourse found in a significant portion of American privacy law scholarship nowadays.

On the other hand, a concomitant discussion about privacy has also been taking place in the FTC. As noted earlier, in August 2022, the FTC announced a Commercial Surveillance and Data Security Rulemaking.[275] Although not expressly included in the rulemaking tittle, this initiative was framed by diverse

[270] Kaminski, *supra* note 152, at 396-97.

[271] Especially, considering the potential First Amendment implications Kaminski also mentions in passing. *See id*. at 396.

[272] *American Data Privacy and Protection Act*, IAPP, https://iapp.org/resources/topics/adppa/ [https://perma.cc/C6FA-DFHM].

[273] *See* BRADFORD, *supra* note 195. For a different position on the impact of the GDPR in America, see Anupam Chander, Margot E. Kaminski & William McGeveran, *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733 (2021); Waldman, *Privacy, Practice, and Performance*, *supra* note 116.

[274] Solove, *supra* note 131, at 1461.

[275] *Commercial Surveillance and Data Security Rulemaking*, FTC (Aug. 11, 2022), https://www.ftc.gov/legal-library/browse/federal-register-notices/commercial-surveillance-data-security-rulemaking [https://perma.cc/GC4H-J2KX].

stakeholders[276]—the FTC itself included[277]—as a privacy rulemaking. However, in contrast to the ADPPA, the text of the Advance Notice of Proposed Rulemaking ("ANPR") contains a striking number of parallels with the ideas proposed today by the participants of privacy's algorithmic turn.

First, the overview of the Advanced Notice points out:

> Recent Commission actions, news reporting, and public research suggest that harmful commercial surveillance and lax data security practices may be prevalent and increasingly unavoidable. These developments suggest that *trade regulation rules reflecting these current realities may be needed to ensure Americans are protected from unfair or deceptive acts or practices. New rules could also foster a greater sense of predictability for companies and consumers* and minimize the uncertainty that case-by-case enforcement may engender. . . . Through this ANPR, the Commission is beginning to consider *the potential need for rules and requirements* regarding commercial surveillance and lax data security practices. [278]

In a similar tone, the Statement of Chair Lina M. Khan reads:

> The data practices of today's surveillance economy can create and exacerbate deep asymmetries of information—exacerbating, in turn, imbalances of power. . . .

[276] *See e.g.*, Joseph Duball, *FTC Officially Launches Privacy Rulemaking Endeavor*, IAPP (Aug. 11, 2022), https://iapp.org/news/a/ftc-officially-launches-privacy-rulemaking-endeavor/ [https://perma.cc/37WC-NZB7]; Omer Tene, *The FTC's Privacy Rulemaking: Risks and Opportunities*, IAPP (Aug. 17, 2022), https://iapp.org/news/a/the-ftcs-privacy-rulemaking-risks-and-opportunities/ [https://perma.cc/EY3U-VPDE]; Megan L. Brown, Duane C. Pozza, Kathleen E. Scott, Jeremy J. Broggi, Tyler Bridegan & Stephen J. Conley, *FTC Launches National Privacy Rulemaking*, WILEY (Aug. 11, 2022), https://www.wiley.law/alert-FTC-Launches-National-Privacy-Rulemaking [https://perma.cc/F4A5-755B]; Mark MacCarthy, *Why the FTC Should Proceed with a Privacy Rulemaking*, BROOKINGS (June 29, 2022), https://www.brookings.edu/blog/techtank/2022/06/29/why-the-ftc-should-proceed-with-a-privacy-rulemaking/ [https://perma.cc/37K4-JNZL]; Janis C. Kestenbaum, Meredith B. Halama, Rebecca S. Engrav & Aaron Haberman, *FTC Kicks Off Wide-Ranging Privacy Rulemaking*, PERKINS COIE (Aug. 16, 2022), https://www.perkinscoie.com/en/news-insights/ftc-kicks-off-wide-ranging-privacy-rulemaking.html [https://perma.cc/98X2-2GXF]; Tatiana Rice, Felicity Slater & Chloe Suzman, *Record Set: Assessing Points of Emphasis from Public Input on the FTC's Privacy Rulemaking*, FUTURE OF PRIV. F. (Dec. 12, 2022), https://fpf.org/blog/record-set-assessing-points-of-emphasis-from-the-public-input-on-the-ftcs-privacy-rulemaking/ [https://perma.cc/T8MP-F6Z8].

[277] FTC, *supra* note 275 ("The Federal Trade Commission is asking the public to weigh in on whether new rules are needed to protect people's privacy and information in the commercial surveillance economy.").

[278] FTC Advance Notice of Proposed Rulemaking, 87 Fed. Reg. 51273, 51276-77 (Aug. 22, 2022).

> Highlighted below are a few topics from the ANPR on which I am especially eager for us to build a record:
>
> - Procedural protections versus substantive limits: Growing recognition of the limits of the ''notice and consent'' framework *prompts us to reconsider more generally the adequacy of procedural protections, which tend to create process requirements while sidestepping more fundamental questions about whether certain types of data collection and processing should be permitted in the first place*. Are there contexts in which our unfairness authority reaches a greater set of substantive limits on data collection? When might bans and prohibitions on certain data practices be most appropriate?[279]

Even, the Dissenting Statement of then Commissioner Noah Joshua Phillips gives further light to the turn that the FTC seems to have taken with this rulemaking. According to Commissioner Phillips, the ANPR "goes far afield from *traditional* data privacy and security."[280] In his view,

> Perhaps the most shocking aspect of this ANPR is not what it contains, but *what it leaves out: privacy*. Missing from this document is any meaningful discussion about whether there should be different rules based on the sensitivity of data, a traditional area of privacy concern reflected in particular federal laws, which provide greater protection for data considered more sensitive, like health data, financial data, and data collected from children. . . . In another departure from most privacy frameworks, the ANPR includes little discussion of how a rule should incorporate important principles like access, correction, deletion, and portability. *The majority is so focused on justifying limiting or banning conduct* now apparently disfavored that *they spare no thought for how best to empower consumers. If you were hoping that the FTC would use its expertise and experience to develop rules that would give consumers greater transparency and control over their personal data, you must be very disappointed*.[281]

In the context of this Article, the evident focus of the FTC's ANPR on emerging imbalances of power and the possible establishment of substantive limits is remarkable. Leaving aside questions about the scope of the FTC's rulemaking authority under Magnuson-Moss,[282] participants of the algorithmic turn may have encountered a more fertile ground than Congress to grow their ideas.

---

[279] *Id*. at 51287.

[280] *Id*. at 51294.

[281] *Id*. at 51297.

[282] Notably, there is an ongoing debate on whether, and to what extent, the FTC can promulgate data privacy and security regulations through its statutory authority. *See e.g.,* Allison Grande, *FTC's Broad Privacy Rulemaking Faces Bumpy Path Forward*, LAW360 (Sept. 1, 2022, 6:50 PM), https://www.law360.com/articles/1523495/ftc-s-broad-privacy-rulemaking-faces-bumpy-path-forward [https://perma.cc/ZLR5-Q94V].

CONCLUSION

This Article has sought to provide a new chapter in the history of the concept of information privacy in a significant portion of American privacy law scholarship. Following Schwartz and Treanor's description of the "new privacy," here I have looked to trace and describe a new transformation of the concept: privacy's algorithmic turn.

Against the framework of the transition to AI and algorithmic decision-making systems, a large portion of American privacy law scholars have transformed their conception of information privacy. There is now a growing recognition that information privacy harms can include issues such as algorithmic discrimination, online manipulation, and subordination. Unlike previous types of privacy harms, these novel harms tend to be objective, architectural, and stem from the actual processing of data. And it is precisely due to these characteristics that the FIPs are now being rejected as ineffective or insufficient tools, while calls are made for more holistic solutions to address the power imbalances of the digital economy.

This "algorithmic turn" can, as seen, be the result of a combination of several factors, including reactions to changes in legal systems around the world, social circumstances, technological developments, and even the scholars' cognitive structures. Whatever the drivers, its implications should not be underestimated. On the one hand, this turn privileges information privacy's symbolic value, to the detriment of its instrumental efficacy. On the other hand, a new privacy paradigm seems to be emerging, and a new opportunity for American privacy law scholars to influence public policy has opened up. A group of regulators (current FTC commissioners) appears to be sympathetic to this post-algorithmic approach to information privacy. But the emerging paradigm needs to be operationalized, to prove that it works as a regulatory *system*.

As with the "new privacy," time will tell if this new evolution of the information privacy concept was worthwhile. For now, acknowledging its existence gives American privacy law scholars the opportunity to reflect on their journey and the future directions they want the field to pursue.

ARTICLE

NON-FUNGIBLE TOKEN LITIGATION: THE EARLY YEARS

JESSICA RIZZO*

CONTENTS

* Attorney, Montgomery McCracken Walker & Rhoads.

ABSTRACT

NFTs, or non-fungible tokens, present a valuable case study of the ways in which courts fill in the gaps where technological development gets ahead of regulation. In this Article, I offer a descriptive account of the first three years of litigation involving NFTs to come before federal district courts. These early cases implicate intellectual property and "traditional" property disputes, fraud and breach of contract claims, securities regulation, alleged criminal conduct, and service of process issues. This Article will be of particular interest to practitioners advising clients in the crypto industry and to legal scholars teaching or writing about law and innovation in general or crypto in particular.

NFTs caught many consumers, courts, and lawmakers off guard in 2021 when they started selling for vertiginous prices despite the fact that they do not, in certain key respects, exist. Some predict that NFTs, or non-fungible tokens, will come to assume an increasingly central role in art and commerce, while others see NFTs as an unfortunate trend that has already passed its expiration date. Whatever the NFT's fate, it will not be the last disruptive technology to capture the public imagination and excite the market, with enthusiasm fast outpacing lawmakers' ability to make sense of the innovation and propose sensible guardrails for its use. This Article tells the story of one such technology that has challenged settled assumptions about art, ownership, and value.

INTRODUCTION

According to one legal scholar, NFTs constitute "a new type of ownership."[1] In the words of one art historian, NFTs are a conceptual art innovation representing "the apotheosis of ownership."[2] Others say they are just another Ponzi scheme.[3] To some in the art world, the NFT signifies a profane reversal of the Duchampian readymade tradition, "a social contract that values property over material experience" and "deploys the category of art to extract private property from freely available information."[4] To others, this technology is the contested site upon which artists, philosophers, and lawmakers will negotiate the terms of "the next phase of our digital sociality."[5] Depending on who you ask, NFTs will, whether we like it or not, be the way we access essential goods and services in

[1] EDWARD LEE, CREATORS TAKE CONTROL: HOW NFTS REVOLUTIONIZE ART, BUSINESS, AND ENTERTAINMENT 47 (2023) ("NFTs create a new type of ownership that I call *interactive ownership*").

[2] *See* Greg Noone, '*The Apotheosis of Ownership': What is the Future of NFTs?*, TECH MONITOR (June 3, 2021, updated Sep. 1, 2022, 11:16 AM), https://techmonitor.ai/technology/emerging-technology/future-of-nfts [https://perma.cc/WFU4-TH83].

[3] *See* Matt Levine, *The Crypto Story*, BLOOMBERG (Oct. 25, 2022, 5:00 AM), https://www.bloomberg.com/features/2022-the-crypto-story [https://perma.cc/N7ZV-PG82].

[4] David Joselit, *NFTs, or The Readymade Reversed*, 175 OCTOBER 3, 4 (Winter 2021).

[5] Charlotte Kent, *Blockchain's Conceptual Landscape*, *in* PROOF OF ART: A SHORT HISTORY OF NFTS FROM THE BEGINNING OF DIGITAL ART TO THE METAVERSE 146, 153 (Alfred Weilinger ed., 2021).

the Metaverse.[6] Or they are just another played-out speculative investment vehicle, the umpteenth coming of tulipmania, a bubble that burst before most people had a chance to figure out what the uninspiring abbreviation even stood for.[7]

In this Article, I take no position on any of the above. Instead, I contribute to the burgeoning[8] literature on NFTs by offering a descriptive account of

[6] *See* Constantin Kogan, *Increased Adoption of Metaverse NFTs Will Power the Next NFT Growth Cycle*, COINTELEGRAPH (Apr. 24, 2022), https://cointelegraph.com/news/increased-adoption-of-metaverse-nfts-will-power-the-next-nft-growth-cycle [https://perma.cc/3CZK-FVDK].

[7] *See* Trevor Jackson, *The Price of Crypto*, N.Y. REV. OF BOOKS (June 8, 2023), https://www.nybooks.com/articles/2023/06/08/the-price-of-crypto-the-cryptopians-laura-shin/ [https://perma.cc/XN8W-VZD2] (explaining that NFTs "were briefly a craze in late 2021 and 2022. . . . the NFT market has crashed so hard that services have appeared offering to buy worthless NFTs in exchange for tax write-offs.").

[8] The academic literature on NFTs is nascent. *See, e.g.*, Brian L. Frye, *After Copyright: Pwning NFTs in a Clout Economy*, 45 COLUM. J.L. & ARTS 341 (2022) (articulating theory of NFT value based on clout, describing trajectory of market for NFTs, and reflecting on the ways in which the NFT market has the potential to transform authorship); Michael D. Murray, *Trademarks, NFTs, and the Law of the Metaverse*, 6 ARIZ. L.J. EMERGING TECH. 1, 2 (2023) (describing early encounters of NFT, trademarks, and the United States legal system); Juliet M. Moringiello & Christopher K. Odinet, *The Property Law of Tokens*, 74 FLA. L. REV. 607, 609-57 (2022) (considering the "tokenization phenomenon" in light of the limitations of existing property law and arguing that NFTs are backed neither by the practical economic considerations nor the theoretical underpinnings associated with traditional tokens); Juliet M. Moringiello & Christopher K. Odinet, *Blockchain Real Estate and NFTs*, 64 WM. & MARY L. REV. 1131, 1131-49 (2023) (questioning the use of distributed ledger technologies as a method of facilitating and verifying the transfer of physical assets); Stephanie L. Tang, *Cryptocurrency, NFTs and the "Metaverse": Addressing the Expanding World of Virtual Assets in Divorce Proceedings*, 127 PENN ST. L. REV. 1, 2 (2022) (setting forth a proposed framework for identifying, characterizing, valuing, and dividing digital assets in dissolution of marriage cases); R. Marcus House, *Non-Fungible Tokens: Implications of Intellectual Property in Sports Law*, 27 INTELL. PROP. & TECH. L.J. 1 (2022) (explaining how NFTs work and analyzing hypothetical intellectual property problems implicating NFTs); Michael D. Murray, *NFTs and the Art World—What's Real, and What's Not*, 29 UCLA ENT. L. REV. 25, 26-27 (2022) (interrogating the "myths" that: 1. NFTs are artworks, 2. NFTs create artificial scarcity, 3. NFT valuation is irrational, 4. Smart contracts are like regular contracts, 5. NFTs created artists' ability to receive resale royalties, and 6. NFTs will allow all artists the chance to make "serious" money from their art); Michael D. Murray, *NFT Ownership and Copyrights*, 56 IND. L. REV. 367, 368 (2023) (discussing NFTs, smart contracts, registration and verification on blockchains, and the rights NFTs convey and do not convey); Brian L. Frye, *The Art of the Token*, 5 STAN. J. BLOCKCHAIN L. & POL'Y 238, 239-40 (2022) (using original conceptual art projects to demonstrate that NFTs are de facto securities, reflect on the history of securities art, investigate what it means to own an NFT, and illustrate the copyright puzzles posed by NFTs); DeJuawn Griffin, *Mining the NFT Goldrush: A Prospective Guide to Drafting NFT Contracts*, 74 MERCER L. REV. 693, 695-731 (2023) (student comment surveying the terms, conditions, and licenses granted by brands and outlining the spectrum of approaches to drafting strong, comprehensive NFT licensing agreements); Zachary L. Catanzaro, *NFT-Tethered*

significant litigation that has arisen in the first few years of the NFT's existence. These early cases are of interest not only because they are first, and therefore likely to carry outsize precedential weight for the foreseeable future in this particular industry, but because they present an opportunity to observe our courts laboring to apply existing law to a disruptive and, to many, puzzling new technology. A secondary contribution this Article makes is an analytic one—while existing law easily accommodates some cases involving NFTs, other cases illustrate a misalignment of law and hitherto uncontemplated facts or raise complicated questions about the relationship between art, commerce, and the law. Where warranted, I consider the implications of these more ticklish cases at greater length and make occasional recommendations.

In Part II, I offer a brief introduction to crypto, attending to the technical and sociocultural aspects of blockchain technology. In Part III, I describe the rise of the NFT. In Part IV, I summarize the major developments in NFT-related litigation to date, analyzing cases involving intellectual property and "traditional" property disputes, fraud and breach of contract claims, securities regulation, alleged criminal conduct, and service of process issues. In Part V, I briefly conclude.

I. CRISES OF TRUST AND BLOCKCHAIN TECHNOLOGY

Cryptocurrency rose from the ashes of the 2008 financial crisis.[9] Bitcoin, the first cryptocurrency, emerged at a time when global market shocks were fast

Sound Recordings and Digital Resale, 14 HARV. J. SPORTS & ENT. L. 17, 18 (2023) (arguing that when someone purchases an ownership interest in NFT-tethered sound recordings, she is purchasing a fractionalized interest in a phonorecord from the copyright owner); Thomas N. Doty, *Blockchain Will Reshape Representation of Creative Talent*, 88 UMKC L. REV. 351, 361-62 (2019) (introducing blockchain technology, discussing the technology's application for creative professionals, and addressing the technology's potential challenges and opportunities); Beckett Cantley & Geoffrey Dietrich, *The Metaverse: A Virtual World with Real World Legal Consequences*, 49 RUTGERS COMPUTER & TECH. L.J. 1, 2 (2022) (providing overview of virtual worlds and their economies and surveying intellectual property, criminal law, tort law, property law, and antitrust issues); Brian Elzweig & Lawrence J. Trautman, *When Does a Non-Fungible Token (NFT) Become a Security?*, 39 GA. ST. U. L. REV. 295, 295-96 (2023) (explaining evolution of digital world and virtual economies, describing blockchain technology and growth of virtual currencies, explaining NFTs, discussing the conditions under which an NFT is an security, and exploring SEC interpretations of crypto assets as securities); Kimberly A. Houser & John T. Holden, *Navigating the Non-Fungible Token*, 2022 UTAH L. REV. 891, 938-39 (2022) (analyzing specific use cases for NFTs and proposing joint committee made up of diverse representatives from the SEC, CFTC, FTC, Justice Department, Treasury Department, academia, the tech industry, and social science fields to create a regulatory sandbox framework for NFT development and use).

[9] *See* David Yaffe-Bellany, *Has Bitcoin Benefited From the Banking Crisis? Not in the Way Its Fans Hoped*, N.Y. TIMES (Mar. 31, 2023), https://www.nytimes.com/2023/03/31/technology/bitcoin-banks-crisis.html [https://perma.cc/6ZUH-E5H2]; *but see* Noelle Acheson, *Crypto Long & Short: No, Bitcoin Was Not a Response to the Financial Crisis*, COINDESK (Sep. 14, 2021, EDT 7:01 AM),

eroding trust in traditional institutions.[10] When the US subprime mortgage bubble burst, it caused cascading failures at Lehman Brothers, Bear Stearns, and other major banks and financial services firms linked by shared debt and other intertwined obligations.[11] In a move much criticized by some taxpayers, the US Federal Reserve responded by bailing out many of the banks deemed "too big to fail," sowing resentment of government in some quarters.[12] The crisis quickly spread from the US to the rest of the world.[13] Millions of people lost their jobs, their homes, and their savings.[14] With the banks benefitting from federal aid while so many ordinary people suffered, it seemed to some that the regulatory guardrails of the traditional financial system existed only to benefit elites—

https://www.coindesk.com/markets/2021/01/24/crypto-long-short-no-bitcoin-was-not-a-response-to-the-financial-crisis/ [https://perma.cc/MWQ8-RUL6] (describing early proponents of the new technology touting Bitcoin as a safer long-term alternative to traditional banks and fiat currencies: "The financial crisis was not the reason for Bitcoin. It was a symptom of the reason for Bitcoin.").

[10] *See* Julie Pinkerton, *The History of Bitcoin, the First Cryptocurrency*, U.S. NEWS (May 10, 2023), https://money.usnews.com/investing/articles/the-history-of-bitcoin; Henry E. Brady & Thomas B. Kent, *Fifty Years of Declining Confidence & Increasing Polarization in Trust in American Institutions,* 151.4 DAEDALUS 43 (2022); Scott Malone, *Global Trust in Business Plummeted in 2008: survey*, REUTERS (Jan. 27, 2009), https://www.reuters.com/article/us-corporate-trust/global-trust-in-business-plummeted-in-2008-survey-idUSTRE50Q1K920090127 [https://perma.cc/SH2P-2GFC].

[11] *See* David Z. Morris, *Satoshi Wept: How Crypto Replayed the 2008 Financial Crisis*, COINDESK (July 12, 2022 EDT 1:39 PM, updated May 11, 2023, EDT 1:02 PM), https://www.coindesk.com/layer2/2022/07/12/satoshi-wept-how-crypto-replayed-the-2008-financial-crisis/ [https://perma.cc/BF28-CHZQ].

[12] *See* Zoe Thomas, *Why Do Many Americans Mistrust the Federal Reserve?*, BBC (Dec. 15, 2015), https://www.bbc.com/news/business-35079495 [https://perma.cc/5PQQ-54AR].

[13] *See* Neil Irwin, *Global Markets Fear a Return to Financial Catastrophe*, WASH. POST (June 17, 2011, EDT 8:16 PM), https://www.washingtonpost.com/politics/global-markets-fear-a-return-to-financial-catastrophe/2011/06/17/AGQJnzYH_story.html [https://perma.cc/9V2A-Z6B7].

[14] *See* Burton Frierson, *Jobs Data Miserable, Regional Factories Slump*, REUTERS (Nov. 20, 2008), https://www.reuters.com/article/us-usa-economy/jobs-data-miserable-regional-factories-slump-idUSTRE4AH85920081120 [https://perma.cc/V498-H8H8]; Marc Lifsher, *More Misery in Jobs Report*, L.A. TIMES (June 21, 2008 2:37 PM), https://www.latimes.com/archives/la-xpm-2008-jun-21-fi-caljobs21-story.html [https://perma.cc/V3YX-2BGU]; Colleen Shalby, *The Financial Crisis Hit 10 Years Ago. For Some, it Feels Like Yesterday*, L.A. TIMES (Sep. 15, 2018, PT 10:00 AM), https://www.latimes.com/business/la-fi-financial-crisis-experiences-20180915-html-story.html [https://perma.cc/Y9NA-T6CA]; *see also* Melanie Haiken, *More Than 10,000 Suicides Tied To Economic Crisis, Study Says*, FORBES (June 12, 2014, EDT 5:39 PM), https://www.forbes.com/sites/melaniehaiken/2014/06/12/more-than-10000-suicides-tied-to-economic-crisis-study-says [https://perma.cc/X2UA-CVK4].

institutions, large corporations, and the well-connected, highly-compensated executives who ran them.[15]

It was against this backdrop that Bitcoin's mysterious pseudonymous creator Satoshi Nakamoto proposed "a system for electronic transactions without relying on trust."[16] Nakamoto wrote that centralized financial institutions "must be trusted not to debase the currency, but the history of fiat currencies is full of breaches of that trust."[17] The "trustless" system Nakamoto proposed to replace traditional finance was blockchain technology.[18]

A blockchain is a decentralized online ledger consisting of linked "blocks" of electronic transactions.[19] Identical copies of the ledger are stored on each of the thousands of computers that make up the blockchain's network.[20] Because each change to the ledger is recorded in this decentralized ledger, with every node in the computer network registering the transaction, no individual blockchain user has to know or trust any other individual blockchain user for the system to work, at least in theory.[21]

[15] *See, e.g.*, Robert Trigaux, *Where's My Bailout?*, TAMPA BAY TIMES (Oct. 30, 2008), https://www.tampabay.com/archive/2008/10/30/where-s-my-bailout/ [https://perma.cc/4PUH-TPNN] ("Hedge fund managers—some of whom were paid more than $1-billion apiece last year—are now lobbying for federal aid. They have lifestyles to maintain, summer mansions in the Hamptons to keep up, swank parties to throw. Hank [Paulson], my 1991 van needs washing. Lend me some, too.").

[16] Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System* (2008), https://bitcoin.org/bitcoin.pdf [https://perma.cc/QNX2-MJWR].

[17] Satoshi Nakamoto, *Bitcoin Open Source Implementation of P2P Currency*, SATOSHI NAKAMOTO INSTITUTE (Feb. 11, 2009, UTC 22:27), https://satoshi.nakamotoinstitute.org/posts/p2pfoundation/1/#selection-45.1-45.539 [https://perma.cc/2WC9-EUKU].

[18] *See* Klint Finley, *The WIRED Guide to Bitcoin*, WIRED (Feb. 1, 2018), https://www.wired.com/story/guide-bitcoin/.

[19] *See* Wired Staff, *The WIRED Guide to the Blockchain*, WIRED (Feb. 2, 2023), https://www.wired.com/story/guide-blockchain/.

[20] *See id.*

[21] *But see* Bruce Schneider, *There's No Good Reason to Trust Blockchain Technology*, WIRED (Feb. 6, 2019), https://www.wired.com/story/theres-no-good-reason-to-trust-blockchain-technology/ (arguing that blockchains shift some of the trust in people and institutions to trust in technology, and that this trust is often misplaced).

There are many different blockchains.[22] Bitcoin is a blockchain.[23] Litecoin, servicing the first "altcoin" or alternative coin, is another blockchain.[24] Ethereum is a different blockchain.[25] Ethereum is special, though not unique.[26] While Bitcoin and similar protocols were only designed to support the exchange of digital currencies, Ethereum and similar blockchains are decentralized computing networks capable of operating "smart contracts," or self-executing transaction protocols.[27] Some of crypto's devotees have expressed enthusiasm for the idea that smart contracts might come to replace traditional legal frameworks facilitating the exchange of property.[28]

Unlike traditional contracts, which are generally written in natural language, smart contracts are software written in the formal language of code.[29] If one

[22] *See A Beginner's Guide to the Different Types of Blockchain Networks*, COINTELEGRAPH (last visited Nov. 7, 2023) https://cointelegraph.com/learn/a-beginners-guide-to-the-different-types-of-blockchain-networks [https://perma.cc/2EYT-N2BT] (explaining the four main kinds of blockchains: 1) public blockchain networks, 2) private blockchain networks, 3) consortium blockchain networks, 4) permissioned blockchain networks).

[23] *See* Nathaniel Popper, *What is the Blockchain? Explaining the Tech Behind Cryptocurrencies*, N.Y. TIMES (June 27, 2018), https://www.nytimes.com/2018/06/27/business/dealbook/blockchains-guide-information.html [https://perma.cc/W42A-PCQE].

[24] Brooke Becher, *What Is Litecoin?*, BUILT IN (May 22, 2023), https://builtin.com/blockchain/what-is-litecoin [https://perma.cc/8SXZ-TH6Q] (describing Litecoin launching as a "hard fork" or spinoff from Bitcoin designed to facilitate faster transactions than the original cryptocurrency). Confusingly, when the words Bitcoin or Litecoin are capitalized, the writer is generally referring to a blockchain protocol. References to lowercase bitcoins or litecoins are to the currencies, the coins used as units of account. *See Why Motherboard Is Capitalizing 'Bitcoin' Again*, VICE (Aug. 28, 2017, 10:00 AM), https://www.vice.com/en/article/qvve7q/why-motherboard-is-capitalizing-bitcoin-again [https://perma.cc/65UG-LWGQ].

[25] *See* David Rodeck, *What Is Ethereum? How Does It Work?*, FORBES (updated Feb. 16, 2023, 10:49 AM), https://www.forbes.com/advisor/investing/cryptocurrency/what-is-ethereum-ether/ [https://perma.cc/BQ7P-WCYG].

[26] *See* Floyd, *Why Ethereum is Special*, MEDIUM (Mar. 3, 2018), https://medium.com/@weswfloyd/why-ethereum-is-special-d916570a43cd [https://perma.cc/E8YK-2V57]. While Ethereum remains by far the most popular blockchain protocol for NFTs, any blockchain that supports smart contracts can support NFTs, and such blockchains have proliferated in recent years. *See* Ekin Genç and Toby Bochan, *What Are the Top NFT Blockchains?*, COINDESK (Mar. 8, 2023, 5:23 PM), https://www.coindesk.com/learn/what-are-the-top-nft-blockchains [https://perma.cc/4GM4-2CS5].

[27] *See* Shaanan Cohney and David A. Hoffman, *Transactional Scripts in Contract Stacks*, 105 MINN. L. REV. 319, 320-23 (2020) (proposing that "transactional script" is a preferable, more precise term for "smart contract," which the authors define as follows: "A transactional script is a persistent piece of software residing on a public blockchain. When executed as a part of an exchange, the code effectuates a consensus change to the state of a ledger.").

[28] Jessica Rizzo, *The Dune NFT Fiasco Is the Least of Crypto's Legal Worries*, WIRED (Jan. 19, 2022, 7:00 AM), https://www.wired.com/story/nft-cryptocurrency-art-regulation-law/.

[29] *Id.*

party breaches a traditional contract, the injured party can seek to compel performance or obtain damages by taking the breaching party to court.[30] Because litigation is expensive, however, the better-resourced of the two contracting parties is often free to breach with relative impunity.[31] Theoretically, smart contracts cannot be breached like traditional contracts because their terms are effectuated automatically.[32] There are theoretically no promises to keep or lawyers to pay when promises are broken.[33] In reality, as the lawsuits described in Part IV of this Article demonstrate, there are still a host of ways for smart contract-based transactions to go awry.[34]

II. NFTS: INNOVATING ART AND COMMERCE

An NFT, or non-fungible token, is an encrypted unit of data stored on a smart contract-enabled blockchain like Ethereum's.[35] NFTs do not themselves contain any visual content.[36] They merely refer to, say, works of digital art by linking to them.[37] NFTs allow digital files, which would ordinarily be infinitely replicable, to be given a unique and immutable record of ownership on the relevant blockchain.[38] There have also been attempts to use NFTs for things like music, gaming, event ticketing, and real estate, but these markets are considerably less

[30] *Id*.

[31] *Id*.

[32] *Id*.

[33] *But see* Cohney and Hoffman, *supra* note 28, at 326 ("Code that embodies commercially-significant scripts will inevitably contain ambiguities, and disappointed parties will ask judges to adjudicate their rights."); Michael del Castillo, *Relax Lawyers, Nick Szabo Says Smart Contracts Won't Kill Jobs*, COINDESK (Dec. 8, 2016, 8:55 AM), https://www.coindesk.com/markets/2016/12/08/relax-lawyers-nick-szabo-says-smart-contracts-wont-kill-jobs/ [https://perma.cc/57EV-PKUM] (reporting on inventor of smart contract concept reassuring lawyers that the work they do is "mostly complimentary to a smart contract" because smart contracts "are mostly making possible new things that haven't been done before.").

[34] *See, e.g.*, David Yaffe-Bellany, *Thefts, Fraud and Lawsuits at the World's Biggest NFT Marketplace*, N.Y. TIMES (June 6, 2022), https://www.nytimes.com/2022/06/06/technology/nft-opensea-theft-fraud.html; Lois Beckett, *'Huge Mess of Theft and Fraud:' Artists Sound Alarm as NFT Crime Proliferates*, GUARDIAN (Jan. 29, 2022, 4:00 AM), https://www.theguardian.com/global/2022/jan/29/huge-mess-of-theft-artists-sound-alarm-theft-nfts-proliferates [https://perma.cc/TQG2-33F6].

[35] *See* AMY WHITAKER & NORA BURNETT ABRAMS, THE STORY OF NFTS: ARTISTS, TECHNOLOGY, AND DEMOCRACY 31 (2023).

[36] *See* Rizzo, supra note 29.

[37] *Id*. While it is not strictly accurate to refer to the image associated with an NFT as an NFT, many do. In this Article, I will sometimes adopt this shorthand to avoid the unwieldiness of repeating the phrase "an image associated with an NFT."

[38] *See* WHITAKER & BURNETT ABRAMS, *supra* note 36.

mature.[39] The market for NFT-associated digital visual art has only been a multimillion dollar one since 2019 and it rose to giddy heights in 2021, reaching its zenith with the sale of an artist called Beeple's *EVERYDAYS: THE FIRST 5000 DAYS* for $69 million at the international auction house Christie's.[40] While this market euphoria was what first launched NFTs into mainstream awareness, Amy Whitaker and Nora Burnett Abrams have persuasively advanced an account of NFTs as originating in market-resistant impulses that have a long history in conceptual art.[41]

One version of this history begins with Sol LeWitt, who started making wall drawings at the Paula Cooper Gallery in 1968.[42] By putting his work directly onto the surface of the gallery wall, LeWitt avoided producing a portable, saleable art object like a painting or sculpture.[43] For LeWitt, "the concept or idea of the work was the work[.]"[44] Such works were designated bona fide LeWitts with certificates of authenticity signed by the artist.[45] A bona fide LeWitt could also be executed by someone other than LeWitt following the artist's instructions, as long as the owner of the piece held onto the certificate.[46] If an individual had a drawing executed on their dining room wall, but then sold the certificate, that drawing immediately ceased to be a LeWitt.[47] As Whitaker and Burnett put it,

[39] Shalini Nagarajan, *7 Real-World NFT Use Cases That Should Be on Your Radar*, BLOCKWORKS (Apr. 2, 2023, 11:32 AM), https://blockworks.co/news/7-nft-use-cases; Ellen Glover, *10 Popular NFT Use Cases*, BUILT IN (Dec. 19, 2022), https://builtin.com/nft-non-fungible-token/nft-use-cases [https://perma.cc/FD4Z-75YL].

[40] OMAR KHOLEIF, INTERNET_ART: FROM THE BIRTH OF THE WEB TO THE RISE OF NFTS 243-244 (2023). This marked the third-highest auction sale price achieved by a living artist. Only Jeff Koons (with the 2019 sale of his sculpture *Rabbit* for $91 million) and David Hockney (with the 2018 sale of his painting *Portrait of an Artist (Pool with Two Figures)*) have seen their work sold for more.

[41] *See* WHITAKER & BURNETT ABRAMS, *supra* note 36, at 25-33. Lest we overlook other histories, it bears noting that the birth of the blockchain did not coincide with the birth of digital art. Digital art has a rich, decades-long history that predates NFTs. *See* Mark Anderson, *Brief History of Digital Art*, THE WORLD ART NEWS (Jan. 23, 2023), https://worldart.news/2023/01/23/brief-history-of-digital-art/ [https://perma.cc/FQ8G-X7LB] (describing John Whitney's work with computer-generated abstract animations in the 1960s, Harold Cohen and Vera Molnar's work created with early computer graphics software in the 1970s, and the rise of digital photography in the 1980s); Ben Luke, *The NFT Bubble Has Popped, But There's Still Untapped Potential in Digital Art*, THE ART NEWSPAPER (Mar. 10, 2023), https://www.theartnewspaper.com/2023/03/10/the-nft-bubble-has-popped-but-theres-still-untapped-potential-in-digital-art (describing exhibitions highlighting early computer art by conceptual artists Stanley Brouwn, Charles Gaines, and Emmett Williams and early Net Art pioneers Eva and Franco Mattes).

[42] *See id.* at 30.

[43] *See id.*

[44] *See id.*

[45] *See id.*

[46] *See id.*

[47] *See id.* at 31.

"The image and the ownership of it became untethered—much as would later happen with many NFTs."[48] Like one of LeWitt's certificates of authenticity, the NFT is meant to certify works of digital art as authentic.[49] Many people can have an identical LeWitt drawing on their wall, just as many people can "right-click save" identical JPEG files of the same digital image, but only one person can have the LeWitt certificate or the NFT.[50]

Crypto artists have also resisted the economic model imposed by the traditional art market by working to ensure that many of the smart contracts controlling NFT sales contain provisions for artist royalties.[51] This maneuver has both legal and art historical traditions.[52] Artists have been attempting to use private agreements to retain the right to a resale royalty percentage since Grant Wood saw his painting *Daughters of the American Revolution* resold by his dealer for four times the original purchase price.[53] Irate, Wood vowed that subsequent sale agreements for his work would include a provision entitling Wood to 50 percent of the profits for each secondary sale.[54] In 1969, the New York City-based Art Workers' Coalition pushed for a percentage of the profit realized on the resale of an artist's work to revert to the artist or her heirs.[55] One legacy of the Coalition's work is *The Artist's Reserved Rights Transfer and Sale Agreement* or "Artist's Contract," a model document written by gallerist Seth Siegelaub and

[48] *See id.*

[49] *See id.*

[50] *See Right-Click, Save As*, KNOW YOUR MEME, https://knowyourmeme.com/memes/right-click-save-as [http://perma.cc/Z5EU-E6GX]. The phrase "right-click save" originated as online shorthand for the argument that crypto art is worthless because those who own it cannot exclude others from it, upsetting traditional property assumptions. Someone who pays $1 million for a Bored Ape and uses it as their Twitter profile picture cannot prevent someone else on the internet from "right-click saving" that same Bored Ape and using it as her own profile picture without paying a dime. Crypto art enthusiasts have ironically reclaimed the phrase, which has become a running joke at the expense of those who supposedly miss the point of crypto art by failing to understand the significance of the NFT as proof of provenance. Today, there is even an online art magazine devoted to crypto art that has adopted the phrase as its title. *See* RIGHT CLICK SAVE, https://www.rightclicksave.com/ [https://perma.cc/E8TQ-X878].

[51] Rizzo, *supra* note 29.

[52] *Id.* Grant Wood is best known for American Gothic, his iconic 1930 painting of a pitchfork-bearing farmer and his daughter standing in front of a Midwestern farmhouse. *See* Sarah Rose Sharp, *How Grant Wood's "American Gothic" Continues to Inspire Artists*, HYPERALLERGIC (Mar. 30, 2022), https://hyperallergic.com/719745/how-grant-woods-american-gothic-continues-to-inspire-artists/ [http://perma.cc/4TMD-76E8].

[53] Neil F. Siegel, *The Resale Royalty Provisions of the Visual Artists Rights Act: Their History and Theory*, 93 DICKINSON L. REV. 1, 2 (1988).

[54] *Id.*

[55] Lucy Lippard, *The Art Workers Coalition: Not a History*, STUDIO INTERNATIONAL, 171, 172 (Nov. 1970).

attorney Robert Projansky.[56] The Artist's Contract included provisions granting artists control over future exhibition of their work, the right to know who owns their work, and the right to a 15 percent royalty each time the work was resold on the secondary market.[57] Artists who tried to use the Artist's Contract to sell their work included Hans Haacke and Adrian Piper, but the agreement could not be enforced because the artists lacked privity of contract with the secondary buyers who had never agreed to pay a resale royalty.[58] In 1973, art collector Robert Scull auctioned off *Thaw*, an assemblage by Robert Rauschenberg that he had originally purchased for $900 in 1958.[59] At auction, the piece went for $85,000, with a distressed Rauschenberg receiving none of the proceeds.[60] The sale became something of a scandal and prompted the introduction of resale royalty bills in Congress and in several states.[61]

While "droit de suite" resale royalty laws have been in effect in France since 1920 and in other European countries for decades, US legislation designed for similar purposes has failed.[62] Only one such bill, in California, was ever passed into law.[63] Enacted in 1977, the California Resale Royalties Act ("CCRA") gave artists and their estates the right to 5% of the proceeds of any resale of the artist's work under certain circumstances.[64] In 2011, photographer Chuck Close and light artist Laddie John Dill brought a putative class action against Sotheby's Christie's, and eBay, alleging that they were due royalties that ought to have been paid to them under the CRRA.[65] The defendants argued that the CCRA was preempted by the 1976 Copyright Act, which retained the first sale doctrine codified by the 1909 Copyright Act.[66] The first sale doctrine provides that a copyright owner's exclusive distribution right is exhausted with the first sale of the copyrighted work.[67] The Ninth Circuit agreed with the defendants and invalidated the CCRA, concluding that the state law impermissibly sought to fundamentally reshape the contours of federal copyright law's existing distribution right.[68]

---

[56] *See* WHITAKER & BURNETT ABRAMS, *supra* note 36, at 46.

[57] *See id*.

[58] Brian L. Frye, *Royalties and the New Collector Economy*, RIGHT CLICK SAVE (Feb. 27, 2023), https://www.rightclicksave.com/article/royalties-and-the-new-collector-economy [https://perma.cc/9P5E-PNJ6].

[59] Siegel, *supra* note 54, at 3.

[60] *Id*.

[61] *Id*.

[62] *See Close v. Sotheby's, Inc*., 894 F.3d 1061 (9th Cir. 2018).

[63] Siegel, *supra* note 54, at 3.

[64] *Close*, 894 F.3d at 1064.

[65] *Id*.

[66] *See id*. at 1067-68.

[67] *See id*. at 1068.

[68] *See id*. at 1071.

Crypto artists have rescued resale royalties from the dustheap of US legal history.[69] Smart contracts have given them the tools to ensure that they automatically receive a royalty when their work is resold.[70]

Certain art world commentators also watched the rise of cryptocurrency and NFTs in the hope that blockchain technology would "create a new social and political model of transparency."[71] Such transparency would mark a pronounced shift away from the opaque art world status quo.[72] In the traditional art market, there is little visibility into primary-market art pricing.[73] Galleries seldom make price lists publicly available, creating an informational asymmetry between art dealers and prospective buyers.[74] On the secondary market, billions of dollars' worth of art is sold every year with little public scrutiny.[75] Buyers may not have any idea who they are purchasing from.[76] Nor do sellers typically know who is buying from them.[77] Even at public auctions, the real parties to a transaction often operate through surrogates and shell companies.[78] Buying art requires none of the paperwork that transfers of stock, real estate, or other substantial assets do, making it difficult for regulators or other interested parties to track art sales and profits.[79] Once sales are complete, works of art purchased for millions of dollars might end up hidden away in a tax-sheltered free port, never to be seen again.[80]

In contrast, some crypto art enthusiasts and other digital utopians imagined, having every transaction permanently noted on a public blockchain would "enshrine a sense of accountability within the user community."[81]

---

[69] *See* Rizzo, *supra* note 29.

[70] *But see* Peter Csathy, *Why NFT Creators Are Up in Arms Over Royalties—and Rightly So*, THE WRAP (Mar. 7, 2023), https://www.thewrap.com/nft-opensea-royalties-resale/ [https://perma.cc/SU3A-ZWTK] (describing NFT platform OpenSea's decision to stop enforcing resale royalties).

[71] KHOLEIF, s*upra* note 41, at 244.

[72] *See* Brian Boucher, *It's Not All in Your Head—the Art World Really Is Unfair. Here are 9 Reasons Why*, ARTNET (Dec. 12, 2019), https://news.artnet.com/art-world/9-reasons-art-world-is-unfair-1726653 [https://perma.cc/NVE6-78UD].

[73] *See id.*

[74] *See id.*

[75] *See* Graham Bowley, *As Money Launderers Buy Dalís, U.S. Looks at Lifting the Veil on Art Sales*, N.Y. TIMES (Jun. 19, 2021, updated June 22, 2023), https://www.nytimes.com/2021/06/19/arts/design/money-laundering-art-market.html [https://perma.cc/34UL-9CLF].

[76] *Id.*

[77] *Id.*

[78] *Id.*

[79] *Id.*

[80] *Id.*

[81] KHOLEIF, *supra* note 41, at 244.

NFTs are no longer fetching the eye-popping sums they were when the mania was at its height.[82] Today, some traditional art institutions are scaling back the infrastructure they invested in when it seemed that the crypto art craze would never end.[83] The 2021 bubble attracted many to crypto art who were more interested in financial speculation than in art for art's sake, making the shadowy art world more transparent and egalitarian, or in redistributing wealth to make it easier for artists to support themselves through sales of their art.[84] But these febrile past few years have also seen a number of rigorous experiments with the new forms made available by blockchain technology.[85] NFTs have already changed the lives of some artists by giving them access to resale royalties.[86] Many true believers report being pleased that NFTs are ceasing to be good targets for financial speculation because the market correction "will separate the wheat from the chaff."[87] As the market either evolves or finds itself supplanted by the next new digital asset class, attorneys will need to understand the kinds of causes of action that can arise when technological innovation outpaces the development of regulation, or even basic norms surrounding the technology's use.

III. SIGNIFICANT EARLY LITIGATION INVOLVING NFTS

In this Part, I describe the major cases involving NFTs that have come before US federal district courts to date and analyze their implications.[88] While beyond the scope of this Article, litigation involving NFTs in state courts may warrant similar scholarly attention in the coming years. In the interest of being reasonably comprehensive, even cases in which NFTs play only bit parts are also catalogued here, though they are generally disposed of succinctly in the footnotes.[89]

---

[82] *See, e.g.*, David Z. Morris, *The Broke Ape Yacht Crash: Lessons for Justin Bieber and Other NFT Collectors*, COINDESK (July 5, 2023, EDT 3:42 PM) https://www.coindesk.com/consensus-magazine/2023/07/05/the-broke-ape-yacht-crash-lessons-for-justin-bieber-and-other-nft-collectors/ [https://perma.cc/H9SR-H4UC]; Carola Padtberg, *What Remains of the NFT Hype*, DER SPIEGEL INTERNATIONAL (Apr. 11, 2022), https://www.spiegel.de/international/zeitgeist/the-crypto-art-crash-what-remains-of-the-nft-hype-a-7213968b-7e13-408c-ac08-83a8c3d94cc4 [https://perma.cc/97MR-G8M3].

[83] *See, e.g.*, Shanti Escalante-De Mattei & Angelica Villa, *Sotheby's Cuts Multiple Senior Staffers and NFT Specialists Amid Market Softening*, ARTNEWS (July 12, 2023, 4:29 PM), https://www.artnews.com/art-news/news/major-staffing-changes-hit-sothebys-phillips-layoffs-1234673955/ [https://perma.cc/ZJ92-XUM9].

[84] *See* Padtberg, *supra* note 83.

[85] *See id.*; *see also* Brian L. Frye, *How to Sell NFTs Without Really Trying*, 13 HARV. J. OF SPORTS & ENT. L. 113, 113 (2022).

[86] *See* Rizzo, *supra* note 29.

[87] *See, e.g.*, Carola Padtberg, *supra* note 83.

[88] This is a highly dynamic area of the law, and new cases are bound to appear on federal dockets before this article goes to press, but I have endeavored to stay as up to date as possible.

[89] *See, e.g., Johnson v. Everyrealm, Inc.*, No. 22 CIV. 6669 (PAE) (S.D.N.Y. Feb. 24, 2023), 2023 WL 2216173, at *6 (plaintiff alleged race and sex discrimination and

Cases in which NFTs play a more significant role but raise substantially duplicative issues are also sometimes disposed of succinctly in the footnotes.

A. Intellectual Property Disputes

To date, most litigation involving NFTs has sprung from intellectual property disputes. Confusion about the application of trademark and copyright law to the various kinds of artwork and other expressive content that can be associated with an NFT has been so widespread that in June of 2022, Senators Patrick Leahy, Vermont Democrat, and Thom Tillis, North Carolina Republican, sent a letter to the directors of the U.S. Patent and Trademark Office (USPTO) and the US Copyright Office requesting a study of the intellectual property issues raised by NFTs.[90] In November, the Copyright Office and the USPTO responded by announcing a joint study into the intellectual property law and policy issues implicated by NFTs.[91] The agencies issued a notice of inquiry soliciting public comment and scheduling a series of roundtables.[92]

The study arrives not a moment too soon. While it is not always easy to tell the naïve from the nefarious in the crypto industry, promoters of NFT projects have repeatedly gotten ahead of themselves in recent years, either misunderstanding or intentionally misrepresenting the intellectual property rights conferred by ownership of an NFT. For example, in 2020, a decentralized autonomous organization (DAO) called Spice DAO paid $3 million for a rare copy of Alejandro Jodorowsky's production book for *Dune*, the never-made film adaptation of Frank Herbert's novel, which has acquired a cult following among science fiction fans.[93] The DAO tweeted its intention to "tokenize" the book.[94] It planned to create an animated series inspired by the book and sell it to a

whistleblower retaliation when he was terminated after reported his concerns about employer digital real estate company's development of likely illegal crypto gambling scheme involving NFTs representing professional soccer players' cards).

[90] *See* Letter from Sen. Thom Tillis and Sen. Patrick Leahy to Kathi Vidal, Under Sec'y of Com. for Intell. Prop. and Dir. of U.S. Pat. and Trademark Off., and Shira Perlmutter, Reg. of Copyrights and Dir. (June 9, 2022), https://www.copyright.gov/laws/hearings/response-to-june-9-2022-letter.pdf [https://perma.cc/MU87-6ZTF].

[91] *See Non-Fungible Token Study*, U.S. COPYRIGHT OFF., https://copyright.gov/policy/nft-study/?loclr=eanco [https://perma.cc/7FCE-M36E] (last visited Oct. 27, 2023).

[92] *See* Study on Non-Fungible Tokens and Related Intellectual Property Law Issues, 87 Fed. Reg. 71584 (Nov. 23, 2022), https://www.govinfo.gov/content/pkg/FR-2022-11-23/pdf/2022-25211.pdf [https://perma.cc/3RZH-3EW9].

Id. at 71585.

[93] Gabriella Angeleti, *Crypto Group Shamed for Spending $3m on 'Dune' Book, Mistakenly Believing it Had Acquired Copyright to Produce NFTs*, ART NEWSPAPER (Jan. 17, 2022), https://www.theartnewspaper.com/2022/01/17/nft-group-shamed-jodorowsky-dune-book-copyright [https://perma.cc/HC9R-NFZ9].

[94] Rizzo, *supra* note 29.

streaming service.[95] The group dissolved after it became clear that owning a physical copy of the book did not give the DAO the right to create reproductions of its illustrated pages or prepare derivative works.[96] Similarly, in 2021, an NFT of a drawing by Jean-Michel Basquiat was offered for sale on the platform OpenSea, with the seller claiming that the purchaser would acquire "reproduction and IP rights."[97] The NFT was withdrawn from the platform after the Basquiat estate made it clear that the seller did not hold any of those rights.[98]

Costly and embarrassing, some of these intellectual property quandaries have also led to litigation. In the following Sections, I will summarize the major cases involving NFTs and trademark and copyright disputes. Some of these cases have helped to clarify the application of longstanding principles of intellectual property law to NFTs, while others have invited questions about a mismatch between outmoded legal regimes and new technologies in need of legislative attention.[99]

[95] Adi Robertson, *What Exactly is the Jodorowsky's Dune Crypto Collective Trying to Make, Anyway?*, THE VERGE (Jan. 17, 2022, EST 3:40 PM), https://www.theverge.com/2022/1/17/22887948/jodorowsky-dune-bible-spice-dao-derivative-script [https://perma.cc/S9DH-7CGY].

[96] Jason Nelson, *Spice DAO to Dissolve After Infamous 'Dune' Book Auction*, DECRYPT (July 28, 2022), https://decrypt.co/106196/spice-dao-to-dissolve-after-infamous-dune-book-auction [https://perma.cc/Q7P8-ZGXS].

[97] Anny Shaw, *Basquiat NFT Withdrawn from Auction After Artist's Estate Intervenes*, ART NEWSPAPER (Apr. 28, 2021), https://www.theartnewspaper.com/2021/04/28/basquiat-nft-withdrawn-from-auction-after-artists-estate-intervenes [https://perma.cc/N6GV-946P].

[98] *Id*.

[99] In *Driessen v. Best Buy Co., Inc*., the one patent case involving NFTs to have come before the courts as of the time of this writing, the holder of a patent directed to a "retail point of sale for the Internet" claimed for the first time during an oral argument before the Patent Trial and Appeal Board that his patent was directed to NFTs. No. 2022-1907, 2023 WL 2422441, at * 1 (Fed. Cir. Mar. 9, 2023). The patent described "a card sold as a retail item in an in-person transaction" that provided "a method of controlling web access." This method allowed the purchaser to access content or merchandise at a specific web page designated by the seller. *Id*. Best Buy, Target, and Walmart filed a petition for *inter partes* review, alleging that the patent's claims were unpatentable because they were directed to obvious subject matter under 35 U.S.C. §103(a). *Id*.. The Patent Trial and Appeal Board agreed with the corporations, and the patent holder appealed, arguing that the Board erred by not construing the claims as being directed to a non-fungible token. *Id*.

The Federal Circuit did not need to reach the merits of this untimely argument, but it noted that it disagreed with the inventor's NFT-based construction anyway, explaining that the inventor's patent was silent regarding blockchain technology or non-fungible tokens. *Id*. at *3. "The patent instead only mentions tokens in a disclaimer," the court wrote, "stating that '[t]his invention is *not* an Internet cash token system used as an anonymous means to get money to spend on the Internet.'" *Id*. The Federal Circuit declined to expand the scope of the claims beyond anything described in the inventor's claims or specification. *Id*.

1. Trademark Disputes

In this Section, I discuss major trademark litigation involving NFTs.[100]

i. Playboy Enterprises v. www.playboyrabbitars.app

In one of the first cases involving NFTs to result in a written judicial opinion, Playboy Enterprises sued the anonymous operators of www.playboyrabbitars.app, a now defunct counterfeit version of the website Playboy created in October of 2021 to sell NFTs associated with "Rabbitars."[101] Like Bored Apes or CryptoPunks, Rabbitars are collectible characters linked to the Ethereum blockchain.[102] Loosely inspired by Playboy's iconic rabbit-in-a-bowtie logo, each Rabbitar is a variation on the same image: a humanoid rabbit depicted from the waist up, returning the viewer's gaze, often with a weirdly lascivious look on its fuzzy face.[103] The props and costumes vary.[104] Some Rabbitars are nursing a martini.[105] Others are smoking a cigar or a carrot.[106] Many wear clothes emblazoned with the Playboy logo, creating a kind of sad, late capitalist *mise-en-abîme* effect.[107] Playboy alleged that the counterfeiters set up a Discord channel and messaged users to "warn" them that the authentic website was fake.[108] Providing a link to the counterfeit website, they steered users away from Playboy's website and towards their own.[109] They used Playboy's logo as their user icon and signed their messages as "The Playboy Team."[110] According to Playboy, the counterfeiters fooled over a thousand people.[111] Those who were taken

[100] *See also Tari Labs, LLC v. Lightning Labs, Inc.*, No. 3:22-CV-07789-WHO, 2023 WL 2480739 (N.D. Cal. Mar. 13, 2023) (trademark infringement action alleging unauthorized use of name TARO for blockchain-based protocol designed to facilitate transfer of digital assets including NFTs); *UMG Recordings, Inc. v. OpenDeal Inc.*, No. 21 CIV. 9358 (AT), 2022 WL 2441045 (S.D.N.Y. July 5, 2022)(trademark infringement action brought by major music company known as "Republic Records" against financial technology firm using name "Republic Music" for music investment platform allowing investors to purchase securitized NFTs in a particular artist's song or album).

[101] *Playboy Enters. Int'l, Inc. v. www.playboyrabbitars.app*, No. 21 CIV. 08932 (VM), 2021 WL 5299231 (S.D.N.Y. Nov. 13, 2021) (order granting preliminary injunction).

[102] *See Meet the Playboy Rabbitars,* PLAYBOY, https://www.playboy.com/custom/playboy-rabbitars [https://perma.cc/L9RK-FNQB] (last visited Oct. 27, 2023).

[103] *See Playboy Rabbitars Official*, OPENSEA, https://opensea.io/collection/playboyrabbitars (last visited Oct. 27, 2023).

[104] *See id.*

[105] *See id.*

[106] *See id.*

[107] *See id.*

[108] *See* Complaint at para. 77, *Playboy Enters. Int'l, Inc. v. www.playboyrabbitars.app*, No. 21 CIV. 08932 (VM), (S.D.N.Y. Nov. 13, 2021), 2021 WL 5299231.

[109] *See id.*

[110] *See id* at paras. 79, 81.

[111] *See id* at para. 84.

in mistook the fake website for the real one and collectively paid over a million dollars for Rabbitars they never received.[112]

Invoking the Lanham Act and violations of New York common law trademark and unfair competition law, Playboy asked for a preliminary injunction and got it.[113] The counterfeiters hid their identities behind Discord user names and Hotmail email addresses and never even bothered to respond to the complaint, so Playboy also ultimately obtained a default judgment as well.[114] While Playboy will undoubtedly have a difficult time collecting, the court also awarded the company statutory damages of $30,000 per registered trademark, for a total damages award of $1,050,000.[115] While an early entrant, this was not a case that would add much in the way of badly-needed legal definition for NFTs. The court did not need to parse the novel issues presented by the technology to decide that the counterfeit website should come down. The case did, however, confirm that the law does not simply disintegrate when one enters the world of web3.[116]

ii. Nike v. Stockx

Another well-known brand became embroiled in a trademark dispute involving NFTs when Detroit-based online marketplace StockX allegedly minted NFTs featuring, *inter alia*, Nike's well-established "Swoosh" and "JumpMan" marks.[117] Like eBay, StockX operates a secondary market platform for the resale of various brands of sneakers, apparel, luxury handbags, electronics, and other collectibles.[118] Unlike eBay, StockX serves as an active intermediary, taking physical possession of name-brand second-hand goods and authenticating them to ensure that buyers avoid paying good money for a knock off.[119]

In January of 2022, StockX announced the launch of StockX "Vault NFTs," a collection of NFTs associated with specific physical items—like, say, a pair of Air Jordans—held in StockX's custody until the NFT holder decides to claim the physical item by surrendering the NFT.[120] The images to which the NFTs

[112] *See id.*

[113] Complaint at para. 1, *Playboy Enterprises Int'l, Inc.*, No. 1:21-cv-08932 (VM), (S.D.N.Y. Nov. 15, 2021), 2021 WL 5299231.

[114] *See Playboy Enterprises Int'l, Inc. v. playboyrabbitars.app*, No. 1:21-cv-08932 2021 WL 5299231, at *1, (S.D.N.Y. Oct. 13, 2022) (Judgment and Order Granting Plaintiff's Motion for Default Judgment and Related Relief).

[115] *See id* at *4.

[116] Jessica Rizzo, *The Future of NFTs Lies With the Courts*, WIRED (Apr. 3, 2022 7:00 AM) https://www.wired.com/story/nfts-cryptocurrency-law-copyright/.

[117] Amended Complaint at para. 5, *Nike, Inc. v. StockX, LLC*, No. 22-CV-0983 (VEC), (S.D.N.Y May 25, 2022).

[118] *Id.* at para. 48.

[119] *Id.* at para. 49.

[120] *Id.* at para. 56.

linked were depictions of the associated products, sneakers prominently bearing Nike's marks, for example.[121]

Nike sued, alleging trademark infringement and dilution, as well as unfair competition, false designation of origin, and various state law claims.[122] The Vault NFTs had already engendered actual confusion, Nike argued, pointing to Twitter and Reddit posts in which members of the public speculated that Nike likely "gets a cut of the fees" for the NFTs and complained about the project being "a stupid scam for Nike to make money."[123] StockX's unauthorized use of the marks was all the more likely to confuse consumers, Nike alleged, because Nike was already conspicuously active in the digital goods space.[124] In 2021, for example, Nike launched a line of NFTs called "CryptoKicks" that, much like the StockX NFTs, featured images of Nike sneakers.[125] Nike had also previously filed applications to register its marks with the USPTO for use in connection with "[d]ownloadable virtual goods, namely computer programs featuring footwear," and "[r]etail store services featuring virtual goods, namely footwear."[126]

StockX denied most of Nike's allegations, arguing that their Vault NFTs were not independent infringing products, but rather "claim ticket[s]" for particular, authenticated physical items held in StockX's vault.[127] According to StockX, the platform's NFTs represented an innovative cost-saving measure for StockX's many customers who were interested in acquiring products not to incorporate into their personal wardrobe rotation, but to immediately resell.[128] "Until recently," StockX explained, "these customers had to incur the transaction costs and shipping times commonly associated with e-commerce experiences, even though physical possession was unnecessary to these customers' goals and needs."[129] StockX's use of images of Nike's sneakers constituted nominative fair use and fell within the protections of the first sale doctrine, the platform argued.[130]

Nike, rejected these arguments, calling the "claim ticket" explanation a "post hoc rationalization" belied by the fact that some of StockX's Vault NFTs had sold for "thousands of dollars above the price of the physical shoe that said ticket supposedly claims."[131]

---

[121] *Id*. at para. 5.

[122] *See id* at paras. 68-69.

[123] *Id*. at paras. 99, 103.

[124] *Id*. at para. 10.

[125] *Id*. at para. 10.

[126] *Id*. at para. 42.

[127] Answer to Amended Complaint at para. 57, *Nike, Inc*., No. 22-CV-0983 (VEC), (S.D.N.Y June 6, 2022).

[128] *Id*. at para. 4.

[129] *Id*.

[130] *Id*. at paras. 2, 3.

[131] Amended Complaint at para. 6, *Nike, Inc*., No. 22-CV-0983 (VEC), (S.D.N.Y May 25, 2022).

The outcome of the case could help determine the viability of the "claim ticket" or "digital receipt" use case for NFTs. If the Vault NFTs are determined to be freestanding assets, StockX will not be protected by the first sale doctrine, and the practice of using NFTs to demonstrate ownership of physical goods—particularly branded ones—could be over before it ever really began.

iii. UMG Recordings, Inc. v. OpenDeal Inc.

Another novel use case for NFTs is at the center of *Universal Music Group Recordings, Inc. v. OpenDeal Inc*.[132] Universal Music Group ("UMG") is the music company that owns Republic Records, home to popular stars including Taylor Swift, Nicki Minaj, and Ariana Grande.[133] Republic Records has been around since 1995, and UMG owns five trademark registrations for the "Republic Records" brand, one for use in connection with "musical sound recordings" and one for use in connection with "production and publishing of music."[134]

In 2016, fintech firm OpenDeal Inc. ("ODI"), doing business as "Republic," began offering crowdfunded securities to the public, giving consumers the ability to purchase fractionalized shares in real estate, entertainment, and consumer products.[135] In 2021, ODI announced the launch of "Republic Music," a "way for artists to raise capital from their fans through investing, and in exchange, the fans receive equity in the rights to the royalties" from that artist's music.[136] The music investment venture allowed investors to purchase securitized NFTs associated with a particular artist's song or album.[137] ODI had some early success with this model when it created an opportunity for investors to buy into "Mona Lisa," a new single by rapper Lil Pump.[138] The "Mona Lisa" offering reached its target investment goal of $500,000 in just two hours.[139]

UMG brought an action against ODI alleging trademark infringement, unfair competition, false designation of origin, and various state law claims.[140] UMG

[132] *UMG Recordings, Inc. v. OpenDeal Inc.*, No. 21 CIV. 9358 (AT), 2022 WL 2441045 (S.D.N.Y. July 5, 2022).

[133] *See* Amended Complaint at para. 18, *UMG Recordings, Inc.,* 2022 WL 2441045 (S.D.N.Y. Aug. 26, 2022).

[134] *UMG Recordings, Inc.*, 2022 WL 2441045 * 1 (S.D.N.Y. July 5, 2022).

[135] *See id.*

[136] *See id.* at *2.

[137] *See id.*

[138] *See id.*

[139] *See* Answer to Complaint at para. 34, *UMG Recordings, Inc.*, No. 21 CIV. 9358 (AT), (S.D.N.Y. Jan. 18, 2022).

[140] UMG also named blockchain platform Opulous as a defendant, alleging that Opulous supplied the NFTs to ODI and promoted ODI's allegedly infringing music-related services. Opulous was no stranger to NFT-related litigation, having previously been sued for, *inter alia*, trademark infringement by Miles Parks McCollum, aka "Lil Yachty," the famous rapper. *See McCollum v. Opulous*, No. CV2200587MWFMARX, 2022 WL 17218072 at *2 (C.D. Cal. Aug. 3, 2022). In May 2021, McCollum agreed to meet with Opulous to hear a pitch for a collaboration between the artist and the company involving NFTs. The meeting did not result

sought a preliminary injunction enjoining ODI from using the marks "Republic" or "Republic Music" in connection with music-related goods and services.[141] Asserting that ODI's music-related investment offerings had resulted in confusion as to the source of the NFTs, UMG pointed to, *inter alia*, the fact that a crypto company executive mistakenly congratulated a UMG executive on the success of the "Mona Lisa" offering.[142]

The court denied UMG's motion for a preliminary injunction, concluding that UMG had failed to demonstrate that it would suffer irreparable harm in the absence of injunctive relief and failed to demonstrate a likelihood of success on the merits.[143] In applying the *Polaroid* factors to assess UMG's likelihood of succeeding on its infringement claim, the court gave considerable weight to ODI's demonstrated lack of "bad faith."[144] Almost immediately after receiving a cease-and-desist letter from UMG, ODI had removed its Republic Music page from its website and stopped using the "Republic Music" phrase in connection with its social media and marketing materials.[145] It also added a disclaimer to its website clarifying that its platform was distinct from Republic Records.[146]

Unlike *Nike v. StockX*, the outcome of *UMG v. ODI* is not likely to play a significant role in deciding the legal fate of any particular NFT use case. The viability of using NFTs as vehicles for fractionalized ownership of intellectual properties will be determined by the market or superseding legislative or administrative intervention. This dispute arose because of a coincidental similarity

in a deal, but seven days later, Opulous launched an ad campaign falsely representing McCollum as being affiliated with Opulous. *Id.* at *1. In social media posts, Opulous claimed that "exclusive music NFT drops" by Lil Yachty, a name McCollum had trademarked, would be available through Opulous soon. *Id.* at *7. Though no such NFTs were forthcoming, Opulous allegedly raised millions of dollars for its platform by publicizing the collaboration with Lil Yachty, who had already achieved considerable success in crypto with the launch of $YACHTY, a cryptocurrency that sold out within just 21 minutes of its release. Complaint at para. 10, *McCollum*, No. CV2200587MWFMARX. While Opulous's alleged infringement would have been no different had the advertised product been a book or physical trading card bearing Lil Yachty's mark, the case exemplifies the ways in which crypto promoters seem, as a group, strikingly more susceptible than other entrepreneurs to old-fashioned fraud.

[141] *See* Memorandum of Law in Support of Plaintiff's Motion for Preliminary Injunction at 2, *UMG Recordings, Inc.*, No. 21 CIV. 9358 (AT) (S.D.N.Y. Jan. 18, 2022).

[142] *See id.* at 24.

[143] *UMG Recordings, Inc.*, 2022 WL 2441045. To assess the likelihood of confusion between the two marks, the court applied the eight-factor balancing test described in *Polaroid Corp. v. Polarad Electronics Corp.*, 287 F.2d 492 (2d Cir. 1961) ((1) strength of the trademark; (2) similarity of the marks; (3) proximity of the products and their competitiveness with one another; (4) evidence that the senior user may "bridge the gap" by developing a product for sale in the market of the alleged infringer's product; (5) evidence of actual consumer confusion; (6) evidence that the imitative mark was adopted in bad faith; (7) respective quality of the products; and (8) sophistication of consumers in the relevant market.).

[144] *UMG Recordings, Inc.*, 2022 WL 2441045 *9 (S.D.N.Y. July 5, 2022)

[145] *See id.* at *2.

[146] *See id.* at *2.

between entity names, and it will be resolved using settled criteria for establishing priority. The case does, however, demonstrate how quickly the market for novel, NFT-associated investment products is becoming a crowded one—UMG alleged that Republic Records was itself planning to expand into the NFT space.[147]

iv. Hermès International v. Rothschild

In other trademark cases involving NFTs, corporate interests are going up against the value of artistic expression in the emerging web3 landscape, with potentially wide-reaching consequences. For example, in *Hermès International v. Rothschild*, the French luxury design house sued artist Mason Rothschild for selling a series of NFTs he called "Metabirkins."[148] According to Hermès, the MetaBirkins consist of "blurry images of" its iconic Birkin handbag.[149] Among the most fetishized objects in fashion, Birkin bags sell for anywhere from $8,500 to $300,000.[150] They are not, however, readily available to just anyone with the requisite disposable income.[151] At one point, there was a six-year waiting list for a new Birkin, even for celebrities.[152] Fashion bloggers trade tips on how a mere mortal might possibly be able to secure a bag before she dies by nurturing relationships with particular Hermès sales associates.[153] "It is reliably reported," one blogger maintains, "that spending a cool six figures plus at an Hermès boutique may make some bags reserved for VIPs available to you."[154] Hermès sued Rothschild over his blurry images, claiming trademark infringement, trademark dilution, and cybersquatting.[155] The company alleged that consumers and members of the media had expressed actual confusion about the provenance of the MetaBirkins, mistakenly assuming that the NFTs were the product of a partnership between Hermès and Rothschild.[156] Hermès also noted that the MetaBirkins

[147] *See* Amended Complaint at para. 26, *UMG Recordings, Inc*., No. 21 CIV. 9358 (AT).

[148] *Hermes Int'l v. Rothschild*, 603 F. Supp. 3d 98, 100 (S.D.N.Y. 2022).

[149] *See* Amended Complaint at para. 78, *Hermes Int'l*, 603 F. Supp. 3d 98 (No. 22-CV-384 (JSR)).

[150] *Why Are Birkin Bags so Expensive? And Worth the Price*, MADISON AVENUE COUTURE (Mar. 7, 2022), https://madisonavenuecouture.com/blogs/news/why-are-birkin-bags-so-expensive-and-worth-the-price [https://perma.cc/B2UD-ZYNC].

[151] *How To Buy An Hermès Bag: Everything You Need To Know*, MADISON AVENUE COUTURE (Oct. 11, 2021), https://madisonavenuecouture.com/blogs/news/how-to-buy-an-hermes-bag-the-hard-way-and-the-easy-way.

[152] *Hermes First Time Buyer Guide,* BAGHUNTER, https://baghunter.com/blogs/insights/hermes-handbag-first-time-buyer-guide [https://perma.cc/46P7-Y26M].

[153] *How To Buy An Hermès Bag: Everything You Need To Know*, *supra* note 152.

[154] *Id*.

[155] *See* Amended Complaint at para. 16, *Hermes Int'l*, 603 F. Supp. 3d 98 (No. 22-CV-384 (JSR)).

[156] *Id*. at para. 14. The *New York Post* and the magazines *Elle* and *L'Officiel* all mistakenly reported that the MetaBirkins were being created and sold by Hermès in collaboration with Rothschild. *Hermes Int'l*, 603 F. Supp. 3d at 102.

have sold for prices that rival those of real-world Birkin handbags.[157] Unlike Playboy or Nike, Hermès does not itself sell NFTs, but the design house maintains that it has the right to enter this market "at the time and manner of its choosing."[158]

According to Rothschild, his images are not blurry, but furry.[159] The bags are "depicted as fur-covered," he explained in a motion to dismiss.[160] The images, he said, offer a visual critique of the animal cruelty attending the production of each Birkin.[161] Unlike the designer bags, "which are made from the tanned hides of slaughtered animals," Rothschild argued, the MetaBirkins are not handbags at all; "they carry nothing but meaning."[162] Comparing his work to Andy Warhol's, Rothschild situated himself within a recognized tradition of pop artists who have taken up iconic commercial brands as subject matter.[163] Rothschild argued that he has a First Amendment "right to respond in the marketplace of ideas to the inescapable corporate brand messages by which we are bombarded every day, virtually everywhere we look."[164] While Hermès contended that Rothschild was using the Birkin mark in commerce to brand a product line, attract public attention, and signify source, Rothschild argued that he was using the MetaBirkin mark as the title of an artwork, entitling him to protection under the test the Second Circuit articulated in *Rogers v. Grimaldi*.[165]

In *Rogers*, the Second Circuit held that while titles can be source indicators, this function is "inextricably intertwined" with their expressive, artistic functions.[166] Artists "frequently rely on word-play, ambiguity, irony, and allusion in titling their works," the court noted.[167] Though consumers of artistic works have an interest in "not being misled," they also "have an interest in enjoying the results of the author's freedom of expression."[168] The *Rogers* court concluded

[157] Amended Complaint at paras. 8, 112, 120-21, *Hermes Int'l*, 603 F. Supp. 3d 98 (No. 22-CV-384 (JSR))..

[158] *Id*. at para. 14.

[159] *See* Memorandum of Law in Support of Defendant's Motion to Dismiss, *Hermes Int'l*, 603 F. Supp. 3d 98 (No. 22-CV-384 (JSR)).

[160] *Id*.

[161] *Id*.

[162] *Id*.at 3.

[163] *Id*. at 9.

[164] *Id*. at 2.

[165] *Id*. at 1.

[166] *Rogers v. Grimaldi*, 875 F.2d 994, 998 (2d Cir. 1989). At issue in *Rogers* was a film by the Italian auteur Federico Fellini titled *Ginger and Fred*. *Id*. at 996. The film tells the story of Pippo and Amelia, two fictional Italian cabaret performers who imitated Ginger Rogers and Fred Astaire, becoming known in Italy as "Ginger and Fred." *Id*. at 997. After the film was distributed in the US, the real Ginger Rogers brought an action for, *inter alia*, false designation of origin under the Lanham Act. *Id*. According to Rogers, the title misled prospective moviegoers as to Rogers' involvement with the film. *Id*.

[167] *Id*.

[168] *Id*.

that the Lanham Act "should be construed to apply to artistic works only where the public interest in avoiding consumer confusion outweighs the public interest in free expression."[169] In the context of "allegedly misleading titles using a celebrity's name," the *Rogers* court held, "that balance will normally not support application of the Act unless the title has no artistic relevance to the underlying work whatsoever, or if it has some artistic relevance, unless the title explicitly misleads as to the source or the content of the work."[170] Since *Rogers*, the Second Circuit has found that the *Rogers* test is "generally applicable to Lanham Act claims against works of artistic expression."[171]

Evaluating Rothschild's motion to dismiss, the *Hermès* court found that, while the *Rogers* test applied the MetaBirkins, Hermès had adequately alleged that Rothschild's use of the disputed mark was not artistically relevant and that the use of the mark was misleading.[172] Importantly, however, the court clarified that Rothschild's use of the novel NFT technology did not change the application of *Rogers*.[173] "[B]ecause NFTs are simply code pointing to where a digital image is located and authenticating the image," the court held, "using NFTs to authenticate an image and allow for traceable subsequent resale and transfer does not make the image a commodity without First Amendment protection any more than selling numbered copies of physical paintings would make the paintings commodities for purposes of *Rogers*."[174] Denying the parties' subsequent cross-motions for summary judgment, the court identified a "genuine factual dispute as to whether Rothschild's decision to center his work around the Birkin bag stemmed from genuine artistic expression or, rather, from an unlawful intent to cash in on a highly exclusive and uniquely valuable brand name."[175]

The case proceeded to trial, a jury sided with Hermès on all counts,[176] and the court denied Rothschild's motion for judgment notwithstanding verdict.[177] This outcome was a great loss for freedom expression in general and artists' First Amendment rights in particular. While artists are attempting to use the tools of web3 to open up a new frontier for human creativity, companies like Playboy, Nike, and Hermès will continue to fight those efforts, urging courts and legislators to treat each successive iteration of the Internet as an annex-in-waiting for their existing commercial activities.[178]

---

[169] *Id.*at 994.

[170] *Id*.

[171] *Cliffs Notes v. Bantam Doubleday Dell Pub. Group*, 886 F.2d 490, 495 (2d Cir. 1989).

[172] *Hermes Int'l*, 603 F. Supp. 3d at 105.

[173] *Id*. at 104.

[174] *Id*.

[175] *Hermes Int'l v. Rothschild*, 654 F. Supp. 3d 268 at *280 (S.D.N.Y. 2023).

[176] *Hermes Int'l v. Rothschild*, No. 22-CV-384 (JSR), 2023 WL 4145518 at *1 (S.D.N.Y. June 23, 2023).

[177] *Id*. at *7.

[178] *See id*.; Rizzo, supra note 117; Victoria Song, *StockX Hits Back at Nike in Legal Battle over NFTS and Counterfeit Sneaker,* THE VERGE (June 6, 2022 EDT 3:22 PM)

Another concerning aspect of *Hermès* was the willingness the court demonstrated to treat as presumptively suspect any artist with a day job. In its amended complaint, Hermès attempted to cast aspersions on Rothschild by insinuating that he is somehow not a "real" artist because he sometimes does other things in order to pay the bills.[179] For example, Hermès pointed to the fact that Rothschild identifies himself as a "marketing strategist" on LinkedIn.[180] "Defendant is a marketing strategist who," Hermès argued, "had no reputation as an artist and no prior experience launching successful NFT collections before he appropriated the BIRKIN Mark."[181] To question Rothschild's artistic integrity on the basis of his, in 2021, having "no prior experience launching successful NFT collections" is a little like questioning the artistic integrity of the Lumière brothers on the basis of their having had no prior experience producing successful motion pictures when they screened *La Sortie de l'usine Lumière à Lyon* in 1885.[182] But the court followed Hermès' lead, referring to Rothschild as a marketing strategist or "entrepreneur," but never once as an "artist" in its orders denying his motion to dismiss, the parties' summary judgment motions, or Rothschild's motion for judgment notwithstanding verdict.[183] While it was obligated to take all *facts* in Hermès' amended complaint as true, nothing compelled the court to give such wide berth to the appellation "artist," one of several associated with Rothschild offered up by Hermès in its papers.[184] This may seem like a minor issue of nomenclature, but the court's word choice here should be disturbing to anyone who cares about the First Amendment. In a country that provides only relatively trivial state financial support for artists, evidence that an artist has found alternative ways to make a living should be afforded no weight whatsoever in a situation like Rothschild's.

When the case against Rothschild was permitted to move forward, Hermès wisely demanded a jury trial, then did everything possible to screen out any juror with any appreciation for or understanding of art.[185] The design house's *voir dire* questions included "Do you have any education, training, or experience in art or art history?"[186] Hermès also convinced the judge to exclude a report prepared by

https://www.theverge.com/2022/6/6/23156515/nike-stockx-nfts-counterfeit-sneakers-lawsuit [https://perma.cc/48EC-NJAF].

[179] Amended Complaint at para. 8, *Hermes Int'l*, No. 22-CV-00384-AJN-GWG (S.D.N.Y. March 02 2022), 2022 WL 1564597.

[180] *Id*. at para. 9.

[181] *Id*. at para. 8.

[182] Sarah Pruitt, *The Lumière Brothers, Pioneers of Cinema*, HISTORY (Oct. 3, 2014, updated June 1, 2023), https://www.history.com/news/the-lumiere-brothers-pioneers-of-cinema.

[183] *Hermes Int'l*, No. 22-CV-384 (JSR) at *2 (S.D.N.Y. May 18, 2022), 2022 WL 1564597.

[184] *See Ashcroft v. Iqbal*, 556 U.S. 662, 679 (2009).

[185] *See* Proposed Voir Dire Questions at 2, *Hermes Int'l*, No. 22-CV-00384 (JSR) (S.D.N.Y. Jan. 25, 2023).

[186] *Id*.

art critic Blake Gopnik that situated the MetaBirkins in a lineage that included work by Warhol and Damien Hirst.[187]

At trial, Hermès doubled down on its strategy of vilifying Rothschild by presenting evidence that he hoped to make money from the MetaBirkins project.[188] The jury, apparently laboring under the delusion that "real" artists are able to subsist on sunlight and air, found for Hermès on all counts.[189] In addition to finding that Rothschild was liable for trademark infringement and dilution, the jury found that the First Amendment was not a bar to Rothschild's liability for the MetaBirkins.[190]

Rothschild has noticed an appeal to the Second Circuit.[191] When the verdict was announced, he expressed frustration that the jury had discounted his artistic bona fides because he sold his work for money and lacked a legitimizing pedigree that included a stint at a "world class art school."[192] As the crypto art movement continues to attract more and more first-time artists from nontraditional backgrounds like computer science, we will no doubt see other plaintiffs adopt Hermès' methods in attempts to discredit those artists. Judges should categorically reject this kind of evidence and these kinds of arguments.

v. Yuga Labs v. Ryder Ripps

Inspired by the freewheeling, open-source ethos of the Internet in general and web3 in particular, many crypto artists and project architects have embraced more permissive intellectual property arrangements than those that remain the norm in the traditional art world.[193] Yuga Labs, the startup behind the now-iconic Bored Ape Yacht Club (BAYC) NFT project grants owners of Bored Ape NFTs "an unlimited, worldwide license to use, copy, and display the purchased Art for the purpose of creating derivative works based upon the Art ('Commercial Use')."[194] This has led to a variety of spin-off projects, including Bored Ape-derived musical acts, a Bored Ape taco truck, and a Bored Ape hard

[187] Zachary Small, *Hermès Wins MetaBirkins Lawsuit; Jurors Not Convinced NFTs Are Art*, N.Y. TIMES (Feb. 8, 2023), https://www.nytimes.com/2023/02/08/arts/hermes-metabirkins-lawsuit-verdict.html.

[188] *See id.*

[189] *See* Verdict Sheet, *Hermes Int'l*, No. 22-CV-384 (JSR) (S.D.N.Y. Feb. 8, 2023).

[190] *See id.*

[191] Notice of Appeal, *Hermes Int'l*, No. 22-CV-384 (JSR), (S.D.N.Y. July 21, 2023).

[192] Eileen Kinsella, *Hermès Wins Its Lawsuit Against the Digital Artist Who Made 'MetaBirkins,' Setting a Precedent for NFT Copyright Cases*, ARTNET (Feb. 8, 2023), https://news.artnet.com/art-world/hermes-wins-lawsuit-against-digital-artisr-2252270.

[193] *See* Andrew Hayward, *Why Ethereum NFT Creators Are Giving Away Commercial Rights—To Everyone*, DECRYPT (Aug. 4, 2022), https://decrypt.co/106761/why-ethereum-nft-creators-are-giving-away-commercial-rights-to-everyone.

[194] *See BAYC Terms & Conditions*, https://boredapeyachtclub.com/#/terms [https://perma.cc/YY8P-3KT8]. The Bored Apes are a collection of 10,000 NFTs built on the Ethereum blockchain, each a slightly different image of a cartoon ape generated by an algorithm.

seltzer.[195] Even when unauthorized Bored Ape copies and adaptations pop up, Yuga Labs has generally refrained from taking legal action to shut them down.[196]

This laissez-faire approach to enforcement was tested in 2021 when the conceptual artist Ryder Ripps began criticizing Yuga Labs.[197] A more established artist than Rothschild, Ripps, has shown work in respected New York galleries and designed album covers and websites for well-known musicians including Grimes and Ye (née Kanye West).[198] Like many artists of his generation, Ripps makes much of his work by appropriating and repurposing materials found online.[199] More interested in thematizing art's delivery systems and cultural contexts than in making technically accomplished objects of aesthetic contemplation, Ripps often incorporates trickery and misdirection into his practice.[200] Before a 2015 gallery exhibition, for example, Ripps spread the rumor that he had hired Jeff Koons's assistants to do the actual painting of his work.[201] That was not true.[202] After the US Central Intelligence Agency (CIA) launched a new website in 2021, Ripps falsely claimed credit for the site's new look, prompting the agency to issue a statement making clear that Ripps "had absolutely nothing to do with our website redesign."[203] Ripps has been described as "an impish prankster who brought the worst of the internet into the space of the art gallery" and someone who has "perfected the art of provocation."[204] He has been likened to Italian artist Maurizio Cattelan, who famously installed a solid gold toilet titled *America* in the Guggenheim Museum in 2016 and sold his 2019 piece *Comedian*, a banana duct taped to a wall, at Art Basel Miami Beach for $120,000.[205]

In 2021, Ripps targeted the Bored Apes, claiming on social media that Yuga Labs had deliberately embedded racist, neo-Nazi, and alt-right dog whistles in

[195] *See* LEE, *supra* note 2 at 167-168.

[196] *See id.* at 175.

[197] *See* Joseph Bernstein, *What's More Provocative Than Sincerity?*, N.Y. TIMES (Mar. 30, 2023), https://www.nytimes.com/2023/03/30/style/ryder-ripps-bored-apes-kanye.html.

[198] *See id.*

[199] *See id.*

[200] *See, e.g.*, Taylor Dafoe, *Ryder Ripps* Ho, BROOKLYN RAIL (Mar. 2015), https://brooklynrail.org/2015/03/artseen/ryder-ripps-ho [https://perma.cc/KR5N-GZ79].

[201] *See* Zach Sokol, *Artist Ryder Ripps Turned a Woman's Instagram Photos into Distorted Hyper-Realistic Paintings*, VICE (Jan. 23, 2015, 2:00 PM), https://www.vice.com/en/article/qbey9v/looking-into-the-instagram-abyss-with-artist-ryder-ripps-111 [https://perma.cc/9JQH-TY45].

[202] *See, e.g.*, Taylor Dafoe, *supra* note 201.

[203] *See* Ian Bourland, *Did an Artist Rebrand the CIA?*, FRIEZE (Jan. 18, 2021), https://www.frieze.com/article/did-artist-rebrand-cia [https://perma.cc/RCA5-Z67N].

[204] Shanti Escalante-De Mattei, *The Art World's Digital Troll Is Determined To Take Down Bored Ape Yacht Club's $4 Billion Empire*, ARTNEWS (Sept. 15, 2022, 11:03 AM), https://www.artnews.com/list/art-news/news/bored-ape-yacht-club-lawsuit-ryder-ripps-1234638475/a-digital-native/ [https://perma.cc/G3T9-F7VL].

[205] *See id.*; Elise Taylor, *The $12,000 Art Basel Banana Explained* VOGUE (Dec. 10, 2019), https://www.vogue.com/article/the-120000-art-basel-banana-explained-maurizio-cattelan.

the Bored Ape NFTs and the BAYC logo.[206] He created a website cataloging these covert messages, arguing that the art project was an example of "simianization," the act of disparaging a particular racial or ethnic group by likening people of that group to apes or monkeys.[207] The purpose of simianization, Ripps explained, is "to justify violence and racism against another group by dehumanizing them."[208] Ripps claimed that the BAYC logo looked "very similar to the Nazi Totenkopf emblem," that the Ape images incorporated anti-Black and anti-Asian symbolism, and that Bored Ape founders used online aliases that were racist anagrams—rearrange the letters and they spelled out hateful slurs.[209] Ripps encouraged his readers to spread the word about the BAYC's "cryptofascism" because "covertly infiltrating culture with hate to an unaware audience" was, he said, "wrong and evil."[210]

In May of 2022, Ripps also created an NFT collection of his own called the Ryder Ripps Bored Ape Yacht Club (RR/BAYC).[211] The NFTs in this collection "pointed" to the same digital images as the original BAYC NFTs but used unique entries on the Ethereum blockchain.[212] This was a bridge too far for Yuga Labs, and the company sued Ripps for, *inter alia*, false designation of origin,[213] false advertising,[214] cybersquatting,[215] and common law trademark infringement.[216] Ripps mounted a vigorous defense, asserting that his "use of pointers to the same images is a form of 'appropriation art'" that exposed Yuga Labs' use of racist, neo-Nazi, and alt-right messages and demanded accountability, all while providing much-needed public education about how NFTs work on a technical level.[217] Yuga Labs countered that Ripps was seeking to devalue the original Bored Apes by flooding the market with copycat NFTs. "This is no mere monkey business," Yuga Labs argued in its Complaint.[218] "It is a deliberate

[206] *See Yuga Labs, Inc. v. Ripps*, CV 22-4355, 2023 WL 2683124. (C.D. Cal Mar. 17, 2023).

[207] *See* Ryder Ripps, *Bored Ape Yacht Club Is Racist and Contains Nazi Dog Whistles*, GORDON GONER (Jan. 2022), https://gordongoner.com [https://perma.cc/3Y7N-4L6V].

[208] *Id*.

[209] *Id*.

[210] *Id*.

[211] Order Granting in Part and Denying in Part Plaintiff Yuga Labs, Inc.'s Motion for Summary Judgment at 2, *Yuga Labs, Inc. v. Ripps*, No. 22-cv-04355 (C.D. Cal. Apr. 21, 2023).

[212] *Id*.

[213] 15 U.S.C. § 1125(a).

[214] *Id*.

[215] *Id*. at § 1125(d).

[216] Order Granting in Part and Denying in Part Plaintiff Yuga Labs, Inc.'s Motion for Summary Judgment at 2, Yuga Labs, Inc. No. 22-cv-04355. The remaining causes of action were common law unfair competition; unfair competition (Cal. Bus. & Prof. Code §§ 17200 et seq.); false advertising (Cal. Bus. & Prof. Code §§ 17500 et seq.); unjust enrichment; conversion; intentional interference with prospective economic advantage; and negligent interference with prospective economic advantage. *Id*.

[217] *Id*.

[218] *Id*. at 3.

effort to harm Yuga Labs at the expense of consumers by sowing confusion about whether these RR/BAYC NFTs are in some way sponsored, affiliated, or connected to Yuga Labs' official Bored Ape Yacht Club," the company said.[219] Ripps's attempt to get the case dismissed by invoking California's Anti-SLAPP law was unavailing, and the court subsequently sided with Yuga Labs in granting summary judgment on the company's false designation of origin and cybersquatting claims.[220] The court also granted Yuga Labs summary judgment on Ripps's First Amendment/*Rogers* and fair use affirmative defenses.[221]

"Although Defendants' [*sic*] argue that the larger RR/BAYC 'project' is an expressive artistic work protected by the First Amendment," the court opined, "Defendants' sale of what is admittedly a collection of NFTs that point to the same online digital images as the BAYC collection is the only conduct at issue in this action and does not constitute an expressive artistic work protected by the First Amendment."[222] In the court's view, Ripps's NFTs do not "express an idea or point of view, but, instead, merely point to the same online digital images associated with the BAYC collection."[223] The court's conclusion betrayed a lamentable misunderstanding of Ripps's conceptual intervention. In creating new NFTs that pointed to the existing BAYC images, Ripps deconstructs the NFT as a form by demonstrating the severability of art object and token. Simultaneously, he is offering up an intelligible political critique that ought to fall within the protective ambit of the First Amendment regardless of whether that critique is particularly hard-hitting or even particularly sincere.[224]

---

[219] *Id*.

[220] *Id*. at 3, 22. To prevail on its cybersquatting claim, Yuga Labs had to establish that Ripps acted "with a bad faith intent to profit" from his use of the BAYC mark. To determine whether Ripps had exhibited such bad faith, the court turned to the nine-factor test articulated in *United Artists v. United Artist Studios LLC*, No. CV 19-828, 2020 WL 4369778, at *15 (C.D. Cal. July 7, 2020). One of the *United Artist* factors is "the defendant's intent to divert consumers from the mark owner's online location to a site accessible under the domain name that could harm the goodwill represented by the mark, either for commercial gain or with the intent to tarnish or disparage the mark, by creating a likelihood of confusion as to the source, sponsorship, affiliation, or endorsement of the site." Since Ripps' explicit goal was to harm the goodwill represented by the BAYC mark, it was no stretch for the court to find that this prong of the *United Artists* test was satisfied. Such a standard, however, makes it difficult to distinguish between a conceptual artist attempting to criticize existing commercial structures from within and scam artists like the Playboy Rabbitars counterfeiters. Here, the court succumbed to the same binary thinking that led the Metabirkins court astray when it concluded that one must be *either* a high-minded artist or a low-minded economic actor. An artist who dares to mix mediums is suspect.

[221] Order Granting in Part and Denying in Part Plaintiff Yuga Labs, Inc.'s Motion for Summary Judgement at 22, Yuga Labs, Inc., No. 22-cv-04355 (C.D. Cal. Apr. 21, 2023)..

[222] *Id*. at 16.

[223] *Id*.

[224] *See* Shanti Escalante-De Mattei, *Judge Says Lawsuit Over Artist Ryder Ripps's NFTs Protesting Bored Ape Yacht Club Must Proceed*, ARTNEWS (Dec. 19, 2022, 1:25 PM),

2. Copyright Disputes

In this Section, I discuss major copyright litigation involving NFTs.[225]

i. Roc-A-Fella Records v. Dash

One of the earliest high-profile copyright disputes involving NFTs, *Roc-A-Fella Records v. Dash* exemplifies the ways in which the crypto hype machine has frequently succeeded in severing all ties with reality.[226] In 2021, the NFT platform SuperFarm announced that it would be collaborating with Roc-A-Fella co-founder Damon Dash to auction off an NFT of Dash's ownership of the copyright to rapper Jay-Z's first album *Reasonable Doubt*.[227] SuperFarm touted the sale as "a groundbreaking landmark—both for the crypto space and the broader music industry."[228] The newly minted NFT would, it said, "provide ownership of the album's copyright, transferring the rights to all future revenue generated by the album from Damon Dash to the auction winner."[229] The only problem with this plan was that Dash did not actually own the copyright to Reasonable Doubt.[230] Roc-A-Fella Records did.[231] Dash only owned a one-third ownership interest in Roc-A-Fella Records.[232]

https://www.artnews.com/art-news/news/yuga-labs-ryder-ripps-refusal-to-dismiss-lawsuit-anti-slapp-1234650893 [https://perma.cc/W8Z4-2YKJ]. As one of Ripps' attorneys told ARTnews: "There's no question that what Ryder was criticizing here was what he perceived as incredibly offensive, racist and neo-Nazi imagery and that that is an important part of the case. . . In the disclaimer, Ryder wrote that if you're buying [an RR/BAYC NFT], you're buying this to protest them, it's a 'fuck you' to Yuga Labs. That's [sic] a pretty clear statement that distinguished one project from another[.]"

[225] *See also* Order Re Defendant's Motion for Summary Judgement; Plaintiff's Motion for Preliminary Injunction; Plaintiff's Motion for Sanctions, *Notorious B.I.G. LLC v. Yes. Snowboards*, No. LA CV19-01946 (C.D. Cal. June 3, 2022), 2022 WL 2784808, at *1-3. Hip hop artist's estate sued to enjoin the defendant photographer from selling NFTs derived from his photographs of Notorious B.I.G., alleging, *inter alia*, a violation of the hip hop artist's right of publicity under New Jersey law. *Id*. The Court denied in part the plaintiff's motion for a preliminary injunction, concluding that the hip hop artist's right of publicity claim as it related to the disputed NFTs was preempted by Section 301 of the Copyright Act. *Id*.

[226] Complaint, *Roc-A-Fella Records, Inc. v. Dash*, 1:21-cv-05411-JPC (S.D.N.Y. June 18, 2021).

[227] *See* Adi Robertson, *An NFT of Jay-Z's First Album Has Sparked a Record Label Lawsuit*, THE VERGE (June 21, 2021, 2:55 PM EDT), https://www.theverge.com/2021/6/21/22543753/jay-z-nft-lawsuit-reasonable-doubt-roc-a-fella-damon-dash [https://perma.cc/NQ6V-28MG].

[228] Rizzo, *supra* note 117.

[229] *Id*.

[230] *Id*.

[231] *See id*.

[232] *See* Robertson, *supra* note 228.

Roc-a-Fella sued, asserting claims for declaratory relief regarding the ownership of Reasonable Doubt, breach of fiduciary duty, conversion, replevin, and unjust enrichment.[233]

Dash claimed the whole thing was a misunderstanding.[234] SuperFarm, he said, mischaracterized what he was trying to do.[235] Dash had only planned to mint a "hologram," which would act as a "digital representation" of his one-third interest in Roc-A-Fella Records and net him, he hoped, north of $10 million at auction.[236] Notably, in his answer to Roc-A-Fella's complaint, Dash never said anything about taking steps to correct SuperFarm's egregious mischaracterization.[237] SuperFarm only called off the auction after receiving a cease-and-desist letter from Roc-A-Fella, at which point the NFT platform also terminated its contractual relationship with Dash.[238] Ignoring this inconvenient fact, Dash claimed that Roc-A-Fella was acting in bad faith, trying to "create a toxic environment" that would make it impossible for Dash to sell his one-third interest in the company for its fair market value.[239] Having scared away potential buyers, Dash alleged, Jay-Z would be free to swoop in and acquire Dash's interest for well below market price.[240]

Roc-a-Fella sought and obtained a temporary restraining order enjoining Dash from "selling, assigning, pledging, encumbering, contracting with regard to, or in any way disposing of any property interest in Reasonable Doubt, including its copyright."[241] The parties subsequently filed a joint stipulation asking the court to enter a final judgment dismissing the case.[242] The parties also asked the court to declare that Roc-a-Fella owned all rights to Reasonable Doubt, including its copyright, and that Dash was prohibited from disposing of Roc-a-Fella's property interest in the album unless authorized by Roc-a-Fella.[243] The court did as requested, bringing the case to a close.[244]

---

[233] Complaint at 8-10, *Roc-A-Fella Records, Inc*., No. 21-cv-05411 (S.D.N.Y. June 18, 2021).

[234] *See* Answer with Counterclaim at 7-9, *Roc-A-Fella Records, Inc*., No. 21-cv-05411 (S.D.N.Y. July 16, 2021).

[235] *See id*.

[236] *See id*. at 8.

[237] *See* Answer with Counterclaim at 7-9, *Roc-A-Fella Records, Inc*., No. 21-cv-05411 (S.D.N.Y. July 16, 2021).

[238] *See id*. para. 16

[239] *Id*.para. 18.

[240] *See id*. para. 8.

[241] Order to Show Cause and Temporary Restraining Order at 1, *Roc-A-Fella Records, Inc*., No. 21-cv-05411 (S.D.N.Y. June 22, 2021).

[242] Joint Stipulation at 2, *Roc-A-Fella Records, Inc*., No. 21-cv-05411 (S.D.N.Y. June 13, 2022).

[243] *Id*. at 4.

[244] Final Judgement, *Roc-A-Fella Records, Inc*., No. 21-cv-05411 (S.D.N.Y. June 27, 2022).

ii. Whitley v. Maguire

Many crypto artists extol the virtues of the unusually supportive, inclusive crypto art "community," but some copyright disputes over NFTs have drawn back the veil on some of that community's more contentious corners.[245] In *Whitley v. Maguire*, Plaintiff Taylor Whitley brought an action arising out of Whitley's ouster from the digital art community he founded.[246] In June 2021, Whitley set up a Discord server known as the Art Discord and worked to drum up interest and recruit members.[247] Discord is an online chat platform originally built for video game enthusiasts to congregate that has become an important site of communication and commerce for crypto artists and their supporters.[248] The "owner" of a Discord server is a kind of "superuser" with access to everything the server contains.[249] An owner can change the server's settings, add or remove roles, upload media files, manage permissions, kick other users off of the server as they see fit, change the server's name, and create or delete channels.[250] Whitley opened a channel of the Art Discord for defendant Antonius Wiriadjaja to use to market his NFTs, and the Art Discord community thrived under Whitley and Wiriadjaja's joint leadership.[251] By October 2021, the Art Discord had thousands of members and required a full staff to keep it running smoothly.[252] Defendant Clare Maguire was hired as a community manager.[253] Whitley promoted his own crypto art on the Discord, and the Discord was where he stored various digital

[245] Kelsey Ables, *Crypto Artists Have Been Building a Rebellious, Underground Community of Outsiders for Years. Now They're Making a Living Selling NFTs*, WASHINGTON POST: MUSEUMS (May 8, 2021, EDT 7:00 AM), https://www.washingtonpost.com/entertainment/museums/beeple-crypto-art-sales-nfts/2021/05/05/ecef3452-ac0d-11eb-acd3-24b44a57093a_story.html [https://perma.cc/Y6LU-WGEC]. Artists who sell their work as NFTs appreciate both the financial advantages of resale royalties and the relative lack of barriers to entry in crypto, as distinguished from the traditional art world with its entrenched hierarchies and powerful institutional gatekeepers. In the crypto art world, no one particularly cares if you are "Brooklyn-based" or went to a fancy art school, and most connections are made on the internet, where it mostly does not matter what you look like or how brightly you sparkle at cocktail parties.

[246] Order Granting in Part & Denying in Part Motion to Dismiss, *Whitley v. Maguire*, No. 22-cv-01837 (C.D. Cal. Dec. 5, 2022), 2022 WL 17418624, at *1.

[247] *Id.*

[248] Jamie Wilde, *Discord Isn't Just for Gaming, It's for Crypto Too*, MORNING BREW: CRYPTO (Aug. 22, 2022), https://www.morningbrew.com/daily/stories/2022/07/11/discord-isn-t-just-for-gaming-it-s-for-crypto-too [https://perma.cc/8PYX-WBRP].

[249] Aaron Donald, *How to Check Who Owns a Discord Server*, ALPHR: DISCORD (Sept. 27, 2021), https://www.alphr.com/check-who-owns-discord-server [https://perma.cc/V6MP-P5QX].

[250] *Id.*

[251] Order Granting in Part & Denying in Part Motion to Dismiss, *Whitley*, No. 22-cv-01837, (C.D. Cal. Dec. 5, 2022), 2022 WL 17418624, at *1.

[252] *Id.* at *2.

[253] *Id.*

assets, including art, data and contact information about the art community and collectors, client lists, and plans for future art projects.[254]

Whitley and other defendant members of the Art Discord collaborated on an NFT collection they called Caked Apes, which are more outré versions of the Bored Apes from which they are derived.[255] The Caked Apes share the general contours of the Bored Apes, but the creatures they depict are neon set off against neon backgrounds and generally dripping with some sort of third kind of neon ooze.[256] Their creators describe them as "[w]hat happens when a group of apes working in a bakery gets pissed on by birds putting out a fire set by potatoes."[257] There are 8,888 of them, and no two have exactly the same combination of funny outfit, whimsical props, and zonked-out expression.[258] The collection was originally Whitley's idea, and he invested nearly $200,000 in launching it.[259] He also authorized the use of a series of logo designs to which he alone held the copyright in many of the Caked Apes images.[260] The parties agreed that Whitley would receive a fixed percentage of all revenue generated by the Caked Apes, and by the time the lawsuit was filed, the Caked Apes had generated approximately $1.9 million in primary sales revenue and $225,000 in royalties from secondary sales.[261] Whitley's authorization to use his logo design in the Caked Apes images was contingent on his receiving his agreed-upon cut of the revenue.[262]

What Whitley did not know was that, before the project launched, his collaborators created a "multi-signature wallet" to receive funds transmitted as payment for Caked Apes NFTs and send Whitley his percentage of the proceeds.[263] Whitley soon noticed that he was not being paid as promised for the Caked Apes that sold.[264] According to Whitley, he reached out to the defendants to resolve

[254] *Id*. at *1.

[255] *Id*. at *2.

[256] Cakedapescreator, *Caked Apes Official*, OPENSEA, https://opensea.io/collection/cakedapesofficial (Jan. 2022).

[257] *See id*.

[258] *See id*.

[259] Order Granting in Part & Denying in Part Motion to Dismiss, *Whitley*, No. 22-cv-01837 (C.D. Cal. Dec. 5, 2022), 2022 WL 17418624, at *2.

[260] *Id*.

[261] *Id*.

[262] *Id*.

[263] *Id*. A multi-signature wallet requires two authorized individuals to approve each monetary transaction.

[264] *Id*. at *2. According to the terms of the parties' deal, Whitley was to receive 10% of all revenue from the Caked Apes project and WTF.Industries, a company solely owned by Whitley, would receive 30% of all primary sales of Caked Apes and 45% of all royalties from secondary sales. Whitley formed the digital art agency WTF.Industries in late 2021 in order to develop, market, and profit from the sales of digital assets. Defendants never distributed any of the profits from Caked Apes sales to WTF.Industries.

the issue, but was ignored.[265] In January of 2022, the defendants revoked Whitley's access to all social media accounts associated with the Caked Apes and exiled Whitley from the Art Discord itself.[266] Whitley was never paid the full revenue share he had been promised for the Caked Apes that sold.[267]

Whitley sued for, *inter alia*, copyright infringement.[268] When the defendants failed to pay him what he was owed and removed him from the Art Discord, Whitley claimed, he revoked his authorization to use the logo design.[269] Nevertheless, the defendants persisted selling Caked Apes that used the design.[270] The defendants countered that Whitley had given them a license to use the design and that they had not exceeded the scope of that license.[271]

In granting defendant's motion to dismiss in part, the court concluded that Whitley failed to allege a copyright violation.[272] Rather, the court held, his claims "present a straightforward breach of contract dispute that lacks a nexus to Whitley's exclusive rights of copyright."[273]

iii. Miramax v. Tarantino

Merely by generating storms of publicity on the subject, high-profile NFT litigation may indirectly influence the way parties negotiate intellectual property agreements going forward.[274] Film studios have long sought to promote their would-be blockbusters with movie tie-ins like *Star Wars*-themed McDonalds

[265] Complaint para. 40-41, *Whitley*, No. 22-cv-01837 (C.D. Cal. Dec. 5, 2022).

[266] Order Granting in Part & Denying in Part Motion to Dismiss, *Whitley*, No. 22-cv-01837 (C.D. Cal. Dec. 5, 2022), 2022 WL 17418624, at *3.

[267] *Id*. at *2.

[268] *Id*. at *4.

[269] *Id*.

[270] *Id*.

[271] *Id*.

[272] *Id*.

[273] *Id*. (internal quotations omitted). Some of Whitley's other claims, including intentional misrepresentation, breach of fiduciary duty, dissolution of implied partnership, and defamation, survived the motion to dismiss. The case was subsequently referred to alternative dispute resolution. *See also Smith v. Compton*, No. CV228439MWFPLAX (C.D. Cal. Feb. 15, 2023), 2023 WL 4291672, at *6 (NFT creator sued former lover and former friend for posting messages on public sites frequented by NFT market participants disparaging plaintiff by claiming he was dishonest and untrustworthy).

[274] *See, e.g.*, Johnny Diaz, *Miramax Sues Quentin Tarantino Over Planned 'Pulp Fiction' NFTs*, N.Y. TIMES (Nov. 17, 2021), https://www.nytimes.com/2021/11/17/business/miramax-tarantino-nft-pulp-fiction.html [https://perma.cc/X9D5-YKXA]; Joe Flint, *Miramax Sues Quentin Tarantino Over 'Pulp Fiction' NFT Plans*, WALL. ST. J. (Nov. 16, 2021), https://www.wsj.com/articles/miramax-sues-quentin-tarantino-over-pulp-fiction-nft-plans-11637092902 [https://perma.cc/RGZ2-QSSM]; Gene Maddaus, *Quentin Tarantino's Attorney Responds to 'Pulp Fiction' NFT Lawsuit: 'Miramax is Wrong,'* VARIETY (Nov. 16, 2021, PT 1:01 PM), https://variety.com/2021/film/news/miramax-tarantino-pulp-fiction-nft-1235113383/ [https://perma.cc/G6AN-5UA5].

Happy Meal toys,[275] *Spider Man*-themed Kellogg's Pop Tarts,[276] and even, in one instance, a *Jurassic Park*-themed Hot Topic "Dilophosaurus dress."[277] The film industry has taken notice of NFTs, with production companies and individual artists racing to find ways to use this new technology to create additional buzz around coming attractions.[278] Some have seen opportunities to use NFTs to derive new revenue streams from older properties.[279] In *Miramax v. Tarantino*, for example, the film studio sued *Pulp Fiction* director Quentin Tarantino for announcing plans to auction off "exclusive scenes" from his 1994 cult classic "in the form of NFTs," according to the complaint.[280] In his answer to Miramax, Tarantino argued that the studio was using "the concept of NFTs to confuse the public and mislead this Court in an effort to deny artists such as Tarantino their hard earned and long-standing rights."[281] The director said he

[275] Seb Santabarbara, *15 Best Happy Meal Toys of All Time*, RETRO DODO (July 1, 2023), https://retrododo.com/best-happy-meal-toys/ [https://perma.cc/YZ98-CV6U].

[276] Timothy Donohoo, *2002's Spider-Man Movie Tie-In Pop-Tarts Were Peak Marvel Merchandising*, COMIC BOOK RESOURCES (Nov. 12, 2022), https://www.cbr.com/2002-spider-man-poptart-marvel-movie-tie-ins/ [https://perma.cc/3225-T6ZU].

[277] *See* Shane Romanchick, *'Jurassic World Dominion' Tie-in Merchandise Roars It's Way Into Stores*, COLLIDER (June 4, 2022), https://collider.com/jurassic-world-dominion-merchandise-images/ [https://perma.cc/C9SW-3ZLP].

[278] *See, e.g.*, Richard Lawler, *Space Jam: A New Legacy Launch Includes a 91,000 Item NFT Tie-In*, THE VERGE (July 12, 2021, EDT 9:30 PM), https://www.theverge.com/2021/7/12/22574752/niftys-nft-space-jam-lebron-james-warner-looney-tunes (describing debut of themed NFT collection coinciding with release of new television show) [https://perma.cc/4TGX-UZCY]; Thomas Buckley, *Coming Soon From the Producers of The Wolf of Wall Street: NFTs*, BLOOMBERG (Apr. 19, 2023, EDT 7:00 AM), https://www.bloomberg.com/news/articles/2023-04-19/-wolf-of-wall-street-producer-with-1mdb-ties-to-sell-nfts-of-film-scenes (describing release of NFTs linked to scenes from hit 2013 Martin Scorsese film as "a way to protect the intellectual property of the film," according to production company's chief financial officer); Zabrina Lo, *Classic Hong Kong Movies Minted as NFTs by Legendary Director Wing Shya*, TATLER (June 20, 2022), https://www.tatlerasia.com/lifestyle/arts/classic-hong-kong-movies-minted-as-nfts-by-legendary-director-wing-shya [https://perma.cc/4Q6N-EHHB] (describing Hong Kong film director's launch of NFT collection recreating scenes from class Hong Kong film as 3D-animated video clips associated with NFTs).

[279] *See, e.g.*, Todd Spangler, *Warner Bros. to Sell 1978 'Superman' NFT Movie Bundles, Priced at 430 or $100*, VARIETY (June 5, 2023, PT 6:00 AM) https://variety.com/2023/digital/news/superman-nft-web3-movies-bundles-1235632135/ [https://perma.cc/PNX5-AYP2] (describing release of "The Superman Web3 Movie Experience," a "multimedia NFT that includes the [1978] film [Superman] in 4K Ultra HD format, plus extras like image galleries and artist renderings by notable DC [Comics] artists.").

[280] Complaint para. 1, *Miramax, LLC v. Tarantino*, No. 2:21-cv-08979 (C.D. Ca. Nov. 16, 2021).

[281] Answer at 1, *Miramax, LLC*, No. 2:21-cv-08979 (C.D. Ca. Dec. 9, 2021).

had only planned to sell NFTs associated with digital scans of his original handwritten screenplay pages.[282]

Back in the early 1990s, when Miramax and Tarantino were negotiating their agreement, it never would have occurred to either of them to ask for language providing for who retained the right to mint and sell NFTs associated with *Pulp Fiction*.[283] In the contract the parties ultimately signed, Tarantino granted Miramax "all rights" to the film except a handful of specifically reserved rights.[284] These reserved rights included the right of "print publication (including, without limitation, screenplay publication . . .)."[285]

Miramax argued, creatively, that "the proposed sale of a few original script pages. . .as an NFT is a one-time transaction, which does not constitute publication."[286] More persuasively, the studio also argued that it controlled the right to sell NFTs associated with excerpts of Tarantino's screenplay because the 1993 contract granted the studio the right to distribute Pulp Fiction "in all media now or hereafter known."[287] The contractual language assigning Tarantino his more limited reserved rights was neither so expansive nor so forward looking.[288]

After some discovery-related scrimmages, Miramax and Tarantino agreed to settle the case, foreclosing the possibility that the dispute will produce instructive caselaw.[289] Nevertheless, the attention generated by the litigation will likely prompt artists and their attorneys to specifically negotiate for the right to create NFTs associated with a piece of intellectual property going forward.[290]

---

[282] *Id*.

[283] *See* Mark Seal, *Cinema Tarantino: The Making of Pulp Fiction*, VANITY FAIR (Feb. 13, 2013), https://www.vanityfair.com/hollywood/2013/03/making-of-pulp-fiction-oral-history [https://perma.cc/9YFU-KTSU] (recounting Tarantino's attorney negotiating for specific wording of Tarantino's writing credit).

[284] Complaint para. 20, *Miramax, LLC*, No. 2:21-cv-08979 (C.D. Ca., Nov. 16, 2021).

[285] *Id*. para. 28, at 7.

[286] *Id*. para. 46, at 13. *But see* Aaron Moss, *Miramax, Tarantino and a Fight Over Bright Shiny Objects*, COPYRIGHT LATELY (Nov. 21, 2021), https://copyrightlately.com/miramax-tarantino-and-a-fight-over-bright-shiny-objects/ [https://perma.cc/KB94-KSDB] ("Most sales are one time transactions, unless you happen to be one of those people who returns half-eaten birthday cakes to Costco.").

[287] Complaint para. 52, at 15, *Miramax, LLC*, No. 2:21-cv-08979 (C.D. Ca., Nov. 16, 2021).

[288] *See* Answer para. 20, at 5-6, *Miramax, LLC*, No. 2:21-cv-08979 (C.D. Ca., Dec. 9, 2021).

[289] Adi Robertson, *Quentin Tarantino Settles NFT Lawsuit with Miramax*, THE VERGE (Sep. 9, 2022, EDT 12:11 PM), https://www.theverge.com/2022/9/9/23344441/quentin-tarantino-pulp-fiction-nft-miramax-lawsuit-settled [https://perma.cc/CZJ9-NVMY].

[290] *See, e.g.,* Order Granting in Part Preliminary Injunction, *Hidden Empire Holdings, LLC v. Angelone*, No. CV 22-6515-MWF (AGRx), 2022 WL 17080131, at *2 (C.D. Cal. Sept. 30, 2022). Independent film studio Hidden Empire sued for, *inter alia*, copyright infringement after defendant digital media producer created an unauthorized video game derived from Hidden Empire's film Fear. *Id*. The game incorporated non-fungible tokens that use elements from Fear, as well as scenes and unique characters from the film. *Id*. Defendants claimed the

B. Property Dispute

A novel theory of digital ownership was tested in *Free Holdings v. McCoy*. Kevin McCoy and Anil Dash are widely credited with creating the first NFT, *Quantum*, which McCoy sold for $1.5 million at the Sotheby's "Natively Digital" sale in 2021.[291] McCoy originally minted *Quantum* on May 2, 2014 on an early blockchain called Namecoin, made up of a system of unique alphanumeric "names" that can be claimed and traded by users.[292] Namecoin required periodic re-registration.[293] If a user failed to update her registration, others were free to claim that user's records of ownership.[294] The Namecoin registration for McCoy's Quantum subsequently expired, and Free Holdings claimed it.[295] On May 28, 2021, McCoy minted another NFT indexing the identical *Quantum* image, this time on the Ethereum blockchain.[296] The Ethereum version was the one offered for sale by Sotheby's.[297] The auction house and McCoy explained that the original Namecoin Quantum entry was destroyed, and that the provenance chain had been "irrevocably transferred" to a "more modern and stable specification on the Ethereum blockchain."[298]

After the sale, Free Holdings brought an action against McCoy, seeking a declaratory judgment providing that 1) Free Holdings was the rightful owner of the original Namecoin *Quantum*, 2) the Namecoin *Quantum* had not been destroyed, and 3) the statements made by McCoy and Sotheby's in connection with the sale of the Ethereum *Quantum* were false and misleading.[299] Free Holdings also claimed, *inter alia*, unjust enrichment and slander of title, arguing that the company had been denied its rightful opportunity to profit from the Sotheby's sale.[300] The court granted McCoy's motion to dismiss for failure to state a claim,

creation of the derivative game was authorized by oral agreement. Plaintiff succeeded in obtaining a preliminary injunction enjoining the defendants from continuing to market the likely infringing game. *Id*.

[291] Shanti Escalante-De Mattei, *Code is Not Law: Case on Who Owns the First NFT Dismissed by Judge*, ARTNEWS (Mar. 23, 2023, 5:03 PM), https://www.artnews.com/artnews/news/kevin-mccoy-quantum-case-dismissed-free-holdings-sothebys-1234662076/ [https://perma.cc/3QUD-S4P7].

[292] *Free Holdings Inc. v. McCoy*, No. 22-CV-881 (JLC) (S.D.N.Y. Mar. 17, 2023), 2023 WL 2561576, at *1 (noting that there is ongoing debate "about the status of names that expire and are then re-registered: Namely, whether re-registered names become new NFTs or are the same NFTs that were previously claimed.").

[293] *Id*.

[294] *Id*.

[295] *Id*. at *4.

[296] *Id*. at *5.

[297] *Id*.

[298] *Id*.

[299] Complaint at para. 109, *Free Holdings Inc*., No. 22-CV-881 (JLC) (S.D.N.Y. Mar. 17, 2023), 2023 WL 2561576, at *1.

[300] *See Free Holdings Inc*., No. 22-CV-881 (JLC) (S.D.N.Y. Mar. 17, 2023), 2023 WL 2561576, at *6.

explaining that Free Holdings had not alleged an interest in the Ethereum Quantum sold at auction, only in the Namecoin Quantum, which remained under Free Holding's control, according to the complaint.[301] As the court pointed out, Free Holdings "allege[d] that the two 'are different NFTs.'"[302] In dismissing the unjust enrichment claim, the court wrote that Free Holdings had "demonstrated nothing more than an attempt to exploit open questions of ownership in the still-developing NFT field to lay claim to the profits of a legitimate artist and creator."[303]

C. Fraud and Breach of Contract Disputes

As the market for NFTs exploded in 2021, so did the scams.[304] Crypto crime far outpaced law enforcement's capacities.[305] A tiny fraction of those who claimed to have wronged by negligent or dishonest actors in the industry have attempted to recover in civil actions, but few of these cases have proceeded to bench trials resulting in published opinions. As a result, there is still little in the way of an independent body of case law specifically focused on NFT fraud, and courts will continue to draw on traditional fraud cases in adjudicating such disputes going forward.[306]

[301] *See id*. at *10.

[302] *Id*.

[303] *Id*. at *13.

[304] *See, e.g*., Lonnie Lee Hood, *NFT Marketplace Admits That 80 Percent of NFTs are Spam, Scams and Fraud*, FUTURISM (Jan. 29, 2022), https://futurism.com/the-byte/nft-marketplace-fraud-scams [https://perma.cc/CBF3-W3J2].

[305] *See* Jessica Rizzo, *Are You a Victim of Crypto Crime? Good Luck Getting Help*, WIRED (Sep. 29, 2022, 9:00 AM), https://www.wired.com/story/cryptocurrency-cybercrime-law-enforcement/.

[306] In addition to the cases discussed at greater length infra, *see* Order, *Trapenard v. Clester*, No. 6:22-CV-660-RBD-LHP (M.D. Fla. Mar. 24, 2023), 2023 WL 2633335, at *1 (fraud action alleging that defendant "scam artist" manipulated plaintiff into joining a group purchase of an NFT by "Bullmarket Girlfriend." Plaintiff transferred the equivalent of $165,000 to the scam artist, who disappeared without facilitating the planned group purchase.); Memorandum & Order, *XMOD Indus. v. Kennedy*, No. 1:22-CV-11464-IT (D. Mass. May 19, 2023), 2023 WL 3572379, at *1 (Metaverse company sued its retained consultant for allegedly stealing approximately $564,000 in proceeds from NFT sale through fraudulent use of the company's social media, marketing outlets, and partner relations); Order, *Digiart, LLC v. Casale*, No. 6:22-CV-494-WWB-RMN (M.D. Fla. Sept. 15, 2023), 2023 WL 6038109, at *1, *report and recommendation adopted*, No. 6:22-CV-494-WWB-DAB, 2022 WL 18492551 (M.D. Fla. Nov. 18, 2022) (plaintiff digital art company sued partner NFT creator for breach of contract and fraud upon discovering that NFT creator was marketing and selling his NFTs independently through other platforms, in violation of the parties' exclusivity agreement); *Jonna v. Latinum*, 617 F. Supp. 3d 758, 770 (E.D. Mich. 2022) (investors alleged, *inter alia*, fraud by crypto company for making misrepresentations regarding NFT partnership with Grammy-nominated recording artist that falsely induced plaintiffs to invest in Latinum cryptocurrency).

1. McKimmy v. OpenSea

Timothy McKimmy brought an action against the NFT platform OpenSea in 2022, alleging negligence and breach of fiduciary duty, trust, contract, and implied contract.[307] He claimed that his Bored Ape was stolen in February of 2022 due to a security vulnerability on the platform that allowed a bad actor to "illegally enter through OpenSea's code" and access McKimmy's NFT wallet.[308] According to McKimmy's complaint, the thief listed the stolen ape, properly valued at millions of dollars, for a nominal sum, and it sold immediately.[309] The ape was then quickly flipped again for about $600,000.[310] McKimmy reached out to OpenSea, hoping that they would "reverse" the transaction, but OpenSea did not oblige, likely because there is no way for a platform like OpenSea to undo such an action once the sale has been immutably recorded on the blockchain.[311]

Because McKimmy agreed to OpenSea's terms of service by clicking a "Continue" button when he registered with the platform, the court concluded that he had consented to be bound by the arbitration provision the terms contained.[312] The case was dismissed.[313]

[307] *See* Complaint, *McKimmy v. OpenSea*, No. 4:22-CV-00545 (S.D. Tx. Feb. 8, 2022).

[308] *See id.* OpenSea had been criticized for its insecurity in the past. *See* Eliza Gkritsi, *OpenSea Bug Allows Attackers to Get Massive Discount on Popular NFTs*, COINDESK (Jan. 24, 2022, EST 8:31 AM, updated May 11, 2023, EDT 1:05 PM), https://www.coindesk.com/tech/2022/01/24/opensea-bug-allows-attacker-to-get-massive-discount-on-popular-nfts/ (reporting on bug that allowed hackers to purchase popular NFTs at older, lower prices, and then sell them at a profit); Lucas Ropek, *Gullible OpenSea Users Were Vulnerable to 'Malicious NFT' Attacks, Researchers Say*, GIZMODO (Oct. 13, 2021), https://gizmodo.com/gullible-opensea-users-were-vulnerable-to-malicious-nft-1847850437 [https://perma.cc/VR4E-ND3H] (reporting on scams involving "trojan-ized" digital art used to lure OpenSea users into connecting their digital wallet to thieves).

[309] Complaint, *McKimmy*, No. 4:22-CV-00545.

[310] *See id.*

[311] *See id.*; *see also* Mike Orcutt, *Once Hailed as Unhackable, Blockchains are Now Getting Hacked*, MIT TECHNOLOGY REVIEW (Feb. 19, 2019), https://www.technologyreview.com/2019/02/19/239592/once-hailed-as-unhackable-blockchains-are-now-getting-hacked/ ("Blockchains are particularly attractive to thieves because fraudulent transactions can't be reversed as they often can be in the traditional financial system.").

[312] *See* Order Granting Motion to Compel Arbitration, *McKimmy*, No. 4:22-CV-00545 at 10 (S.D. Tx. Mar. 22, 2023).

[313] *See* Order, *Armijo v. Ozone Networks, Inc.*, No. 3:22-cv00112-MMD-CLB (D. Nev. Jan. 19, 2023), 2023 WL 319577 at *1. Plaintiff sued OpenSea, Yuga Labs, and NFT platform LooksRare for breach of contract, breach of the implied covenant of good faith and fair dealing, and negligence after alleged theft of plaintiff's Bored Ape and Mutant Ape NFTs when plaintiff clicked on phishing link. *Id.* The court found that the economic loss doctrine barred plaintiff's negligence claims against OpenSea and dismissed the claims against Yuga Labs for lack of personal jurisdiction. *Id.*

2. Thayer v. Furie

Halston Thayer sued crypto artist Matt Furie for allegedly misrepresenting the rarity of an NFT titled FEELSGOODMAN, for which Thayer paid over half a million dollars after winning a auction.[314] FEELSGOODMAN depicted Pepe, the oft-memed green cartoon frog relaxing near a waterfall.[315] According to Thayer's complaint, Furie artificially inflated the value of the NFT offered for sale by claiming that it was the only one out of an edition of 100 that would be auctioned.[316] The other 99 identical NFTs would be withheld from circulation indefinitely, Furie promised.[317] Almost immediately after the auction, however, Furie distributed 46 of the 99 for free, resulting in the value of Thayer's purchase plunging, he alleged, from half a million to just $30,000.[318] Thayer claimed it was all a scheme to induce him to "grossly overbid" on FEELSGOOODMAN and sued for, *inter alia*, fraudulent inducement and intentional misrepresentation.[319]

[314] *See* Mathew Gault, *Rare Pepe NFT Is Not Rare Enough, $500K Lawsuit Alleges*, VICE (Mar. 25, 2022, 9:00 AM), https://www.vice.com/en/article/dypj37/rare-pepe-nft-is-not-rare-enough-dollar500k-lawsuit-alleges [https://perma.cc/62FY-UWWM].

[315] Furie originally created Pepe the Frog as a lovable slacker character in his indie comic, *Boys Club*. The character caught on and was shared widely in various online subcultures. At some point, Pepe started becoming so popular with the "normies" of mainstream culture that Pepe's original devotees tried to reclaim Pepe for the weirdos of the internet. To alienate the normies, Pepe fans created versions of Pepe that were less and less conventionally palatable. Suddenly racist Pepes, homophobic Pepes, and antisemitic Pepes were everywhere. In 2016, Pepe became a symbol of the alt-right movement then helping propel the rise of Donald Trump, prompting Hillary Clinton to publicly denounce the cartoon frog. The Anti-Defamation League added Pepe to its list of hate symbols. With the help of a law firm working pro bono, Furie launched a campaign to use copyright law and DMCA takedown notices to prevent Pepe from being used to promote ideologies he found repugnant, but Pepe continues to have a life of his own. *See* Andrew Limbong, *'Feels Good Man' Traces Pepe The Frog From Hate Symbol To Democracy Icon*, NPR (Sep. 4, 2020, ET 4:04 PM), https://www.npr.org/2020/09/04/902617699/feels-good-man-traces-pepe-the-frog-from-hate-symbol-to-democracy-icon; Rachael Revesz, *Hillary Clinton attacks Donald Trump for posting Pepe the Frog meme*, INDEPENDENT (Sep. 13, 2016, BST 11:09), https://www.independent.co.uk/news/world/americas/donald-trump-hillary-clinton-pepe-frog-instagram-breitbart-white-supremacist-alex-jones-milo-yiannopoulus-a7240581.html [https://perma.cc/3S4G-U7WF]; Matthew Gault, *Pepe the Frog's Creator Goes Legally Nuclear Against the Alt-Right*, VICE (Sep. 18, 2017, 1:43 PM), https://www.vice.com/en/article/8x8gaa/pepe-the-frogs-creator-lawsuits-dmca-matt-furie-alt-right.

[316] *See* Complaint para. 6, *Thayer v. Furie*, No. 2:22-cv-01640 (C.D. Ca., Mar. 12, 2022).

[317] *See id.* at para. 7.

[318] *See id.* at paras. 7-8.

[319] *See id.* at 2. Thayer also claimed negligent misrepresentation, violations of California unfair competition law, and violations of California's consumer protection laws. In the alternative, sought rescission of the contract for sale of the NFT, claiming mistake of fact, breach of contract, breach of the implied covenant of good faith and fair dealing, and unjust enrichment.

The parties jointly stipulated to dismissal of the case.[320]

3. Banq, Inc. v. Purcell

NFT wallet company Banq Inc. filed a fraud and misappropriation of trade secrets action against three former executives, claiming that the defendants stole confidential company information and absconded to form rival NFT platforms.[321] Banq was formed in 2019, according to the complaint, to develop a platform with cryptocurrency-friendly payment applications that would make it easy for users to transfer digital assets.[322] Over several years, Banq allegedly invested millions of dollars in the development of proprietary technology and intellectual property.[323]

In 2021, while serving as Banq's CEO, defendant Purcell "unilaterally decided to execute 'a major pivot' at the company to focus instead on NFTs," according the complaint.[324] Simultaneously, Purcell was preparing to jump ship.[325] While still employed by Banq, Purcell allegedly formed a new web3 infrastructure company as a repository for "assets, opportunities, technology, and resources stolen from Banq."[326] Purcell allegedly poached key Banq personnel, pretextually firing engineers and then rehiring them at Purcell's new NFT company.[327] He allegedly gave the new company access to Banq's code so that new technology replicating Banq's could be created.[328] According to the complaint, he then directed Banq to sell all of Banq's computers to the new company for "bargain basement" prices that the company's board never would have approved had it been consulted.[329] The computers contained Banq's "corporate assets, trade secrets, intellectual property, and other proprietary technology."[330] Purcell unilaterally began winding down Banq's operations, allegedly destroying "substantial amounts of Banq's corporate documents and records to cover up their

[320] Stipulated Order of Dismissal of Plaintiff's Complaint, *Thayer*, No. 2:22-cv-01640 (C.D. Ca., Aug. 24, 2022).

[321] *See* Order Granting Motion to Compel Arbitration & Denying Motion to Dismiss as Moot, *Banq, Inc. v. Purcell*, No. 2:22-cv-00773-APG-VCF (D. Nev. Jan. 17, 2023), 2023 WL 205759. In addition to fraud and violations of Nevada state and federal trade secrets laws, Banq. Inc. alleged conversion, interference with prospective economic advantage, breach of fiduciary duty, negligence for spoliation of evidence, unjust enrichment, and violations of various state and federal computer fraud laws.

[322] *See* Complaint, *Banq, Inc.*, No. 2:22-cv-00773 (D. Nev. May 16, 2022).

[323] *See id.*

[324] *Id.* at para. 24.

[325] *See id.* at para. 29.

[326] *Id.* at para. 31.

[327] *See id.* at para. 32.

[328] *See id.* at para. 33.

[329] *See id.* at para. 34.

[330] *Id.*

wrongdoing" in the process.[331] Shortly thereafter, Purcell's new company issued a press release announcing the release of "a cross-chain, embeddable, API-driven nonfungible token (NFT) wallet," the "exact product that Banq was developing" prior to Purcell's departure from Banq, according to the complaint.[332]

The defendants moved to compel arbitration based on arbitration clauses in the employment agreements each individual defendant signed, and the court granted the motion.[333] A few months later, Banq filed for bankruptcy under Chapter 11, detailing in its plan of reorganization how the misconduct of the defendants had forced Banq to temporarily suspend the majority of its day-to-day business operations.[334]

D. Securities Litigation

Legal scholar and crypto artist Brian Frye has long taken the provocative, not to say tongue-in-cheek, position that NFTs are securities.[335] According to Frye, "[t]he art market has always been a securities market, we just couldn't see it, because objects got in the way. The art market is the market for 'art as an investment.'"[336] What you are "really" buying when you buy an NFT, Frye says, is "[a] fractional interest in the commercial goodwill associated with an artist, or rather, a share of the artist's 'clout.'"[337] If the artist's star rises, your investment appreciates, but if the artist's career goes nowhere, your investment fails.[338]

To Frye, this dynamic aligns perfectly with the Supreme Court's 1946 *Howey* test.[339] In *Howey*, the Securities and Exchange Commission ("SEC") brought an action against a company that sold tracts of orange groves to buyers in Florida, who then leased the land back to the company, Howey.[340] Most buyers had no

[331] *See id*. at para. 46.

[332] *Id*. at para. 50.

[333] *See* Order Granting Motion to Compel Arbitration & Denying Motion to Dismiss as Moot, *Banq, Inc*., No. 2:22-cv-00773-APG-VCF (D. Nev. Jan. 17, 2023), 2023 WL 205759, at *1.

[334] *See* Plan of Reorganization, *In re: Banq Inc*., No. 23-12378-nmc at 9 (Bankr. D. Nev. June 13, 2023). The plan of reorganization also described Banq being forced into bankruptcy as a direct result of a $3 million loan Purcell took out on Banq's behalf as he was preparing to launch his new company with Banq's technology. Banq alleged that the lender of the $3 million was a substantial investor in Purcell's new company. The lender brought a lawsuit related to the $3 million loan. As a result of the defendants misappropriation of Banq's assets and the expenses associated with defending against the lender's claims, Banq was left with insufficient resources to resume its business operations or pay its creditors, the company said.

[335] Brian Frye, *NFTs Are Securities and It's Great*, COINDESK (Dec. 28, 2022, EST 9:48 AM), https://www.coindesk.com/consensus-magazine/2022/12/28/nfts-are-securities-and-its-great/.

[336] *Id*.

[337] *Id*.

[338] *See id*.

[339] *See id*.

[340] *See S.E.C. v. W.J. Howey Co*., 328 U.S. 293, 294-95 (1946).

experience in agriculture and had nothing to do with tending the land.[341] Howey staff were responsible for cultivating the orange groves and selling the oranges.[342] In determining that the leaseback arrangements qualified as investment contracts that needed to be registered with the SEC, the Court held that an investment contract is 1) an investment of money 2) in a common enterprise 3) with the expectation of profit 4) to be derived from the efforts of others.[343] The people who purchased Howey's orange groves made their investment in a common enterprise counting on the labor and expertise of others who would work the land, hopefully generating a profit.[344] Analogously, Frye argues, "[e]very investment in artwork or NFTs is an investment in an artist's career, with the expectation (or at least hope) of profit, by virtue of the artist becoming famous."[345]

The analogy can be extended to other kinds of NFTs, like collectibles, and the SEC reportedly began a serious investigation into whether NFT creators and marketplaces have violated securities regulations in 2022.[346] In the absence of formal guidance from the SEC, private plaintiffs have taken steps to clarify the application of this body of law to NFTs.[347] When making a public offering of

[341] *Id*. at 296.

[342] *Id*.

[343] *See id*. at 300.

[344] *See id*.

[345] Brian Frye, *supra* note 336. Frye goes on to explain that, while the SEC *could* regulate NFTs as securities using the Howey test, it never will, as the SEC is really only in the business of regulating things that "look like" traditional securities, like stocks and bonds.

[346] Matt Robinson, *SEC Scrutinizes NFT Market Over Illegal Crypto Token Offerings*, BLOOMBERG (Mar. 2, 2022, EST 4:56 PM), https://www.bloomberg.com/news/articles/2022-03-02/sec-scrutinizes-nft-market-over-illegal-crypto-token-offerings; Jeff Benson, *SEC Targets NFT Creators, Marketplaces Over ICO-Like Sales: Report*, DECRYPT (Mar. 2, 2022), https://decrypt.co/94268/sec-targets-nft-creators-marketplaces-ico-sales-report.

[347] Prominent corporate and individual leaders in the crypto industry have criticized the SEC for failing to develop a workable regulatory framework for crypto. *See, e.g*. Brief of Amicus Curiae Coinbase, Inc. in Support of Defendants's Motion to Dismiss, *S.E.C. v. Wahi, et al*., No. 2:22-cv-01009-TL (W.D. Wa. Mar. 13, 2023); *Coinbase Petition for Rulemaking—Digital Asset Securities Regulation,* (July 21, 2022), https://assets.ctfassets.net/c5bd0wqjc7v0/5NRidtW8lvwVEf-SHpndWQm/78f95afa4f0ebaaefb303e1a4f172d03/Coinbase_petition_for_SEC_rulemaking.pdf [https://perma.cc/6NPU-EH5T]; *Coinbase Petition for Rulemaking—"Proof-of-Stake" Blockchain Staking Services,* (Mar. 20, 2023), https://assets.ctfassets.net/c5bd0wqjc7v0/37LaXLBCdgLHa7GE4TPnmw/7824df367e12f4136951db794a5df63d/Staking_Comment_Letter_3-20-2023_FINAL.pdf [https://perma.cc/PAV4-2Y6N]. The federal judiciary has also joined in the chorus of critique. *See* Dietrich Knauth, *SEC Objections to Voyager-Binance Deal Criticized by U.S. Judge*, REUTERS (Mar. 2, 2023, EST 8:09 PM), https://www.reuters.com/legal/sec-objections-voyager-binance-deal-criticized-by-us-judge-2023-03-02/ [https://perma.cc/BFM4-8SFD]. These critics accuse the SEC of regulating by enforcement alone, doing unwarranted damage to well-intentioned actors. As

NFTs, some of these plaintiffs have argued, issuers should have to comply with the same disclosure requirements required for any other public securities offering, as such disclosures deter fraud, promote transparency, and give investors access to certain basic facts about investments prior to purchase.[348]

The class action *Friel v. Dapper Labs* brought together plaintiffs who had purchased National Basketball Association ("NBA") Top Shot "Moments," NFTs associated with video clips of highlights from NBA games.[349] When someone purchases a Moment, she acquires no intellectual property, no rights to the basketball highlight depicted in the video clip or anything other than the NFT itself.[350] The plaintiffs sued Dapper Labs, the studio behind the Moments, arguing that the NFTs are unregistered securities.[351] Because Dapper Labs failed to comply with the securities disclosure requirements, the plaintiffs allege, thousands of unsophisticated buyers purchased Moments without fully understanding what they were acquiring.[352] Looking to get rich quick, the buyers were not prepared for the volatility of the market for Moments.[353] Nor were they prepared to wait months to cash out because of the Top Shot platform's lengthy withdrawal delays.[354]

The case survived Dapper Labs motion to dismiss, with the court holding that the plaintiffs had adequately alleged that Dapper Labs's offer of the Moments was an offer of an "investment contract" and therefore a security required to be registered with the SEC.[355] The Court analyzed the Moments using the traditional Howey test.[356]

---

cryptocurrency platform Coinbase puts it, "[t]ell us the rules and we will follow them. Give us an actual path to register, and we will register the parts of our business that need registering." Paul Grewal, *We Asked the SEC for Reasonable Crypto Rules for Americans. We Got Legal Threats Instead.*, COINBASE BLOG (Mar. 22, 2023), https://www.coinbase.com/blog/we-asked-the-sec-for-reasonable-crypto-rules-for-americans-we-got-legal.

[348] Daniel M. Gallagher, *The Importance of the SEC Disclosure Regime*, HARVARD LAW SCHOOL FORUM ON CORPORATE GOVERNANCE (July 16, 2013), https://corpgov.law.harvard.edu/2013/07/16/the-importance-of-the-sec-disclosure-regime/ [https://perma.cc/28DB-4FZZ].

[349] *See Friel v. Dapper Labs, Inc.*, No. 21 CIV. 5837 (VM), 2023 WL 2162747 (S.D.N.Y. Feb. 22, 2023).

[350] *See id.* at *5.

[351] *See id.*

[352] *See id.*

[353] *See* Elizabeth Lopatto, *NBA Top Shot Seemed Like a Slam Dunk—So Why Are Some Collectors Crying Foul?*, THE VERGE (June 7, 2022, 8:30 AM), https://www.theverge.com/23153620/nba-top-shot-nft-bored-ape-yacht-club.

[354] Jon Sarlin, *NBA Top Shot Customers Can't Get Their Money Out. Experts are Confounded*, CNN BUSINESS (Apr. 27, 2021, 1:52 PM), https://www.cnn.com/2021/04/27/investing/top-shot-withdrawal-nba-nft/index.html [https://perma.cc/84VU-AMGB].

[355] *Dapper Labs, Inc.*, No. 21 CIV. 5837 (VM), 2023 WL 2162747 at *22 (S.D.N.Y. Feb. 22, 2023).

[356] *See id.* at *8.

Plaintiffs easily satisfied the "investment of money" prong of Howey.[357] At the height of the 2021 NFT boom, buyers were paying as much as $210,000 for the most coveted Moments.[358]

The court also held that the plaintiffs had alleged a common enterprise.[359] In the Second Circuit, the existence of a common enterprise can be established under the theory of "vertical commonality" or the theory of "horizontal commonality."[360] Vertical commonality exists where the fortunes of investors are tied to the fortunes of the promoter, rising and falling together.[361] Horizontal commonality exists where 1) there is a sharing or pooling of the funds of the investors and 2) the fortunes of each investor are tied to one another and to the success of the overall venture.[362] Pooling occurs when the funds received by the promoter through an offering are reinvested by the promoter in the business, increasing the value of the instrument offered.[363] The court found that the plaintiffs adequately pled pooling by alleging that Dapper Labs's sale of packs of Moments and the transaction fees on the Top Shot marketplace generated revenue used to support and grow the Flow blockchain undergirding the marketplace.[364] The court also found that the Moments purchasers' fortunes were tied to the overall success of Dapper Labs.[365] Moments can only be sold on the Top Shot marketplace—if the platform collapses, purchasers are out of luck.[366] Accordingly, the *Friel* court concluded that the plaintiffs had adequately alleged horizontal commonality.[367]

The plaintiffs also adequately alleged that Dapper Labs's offer of Moments came with a "reasonable expectation of profits to be derived from the entrepreneurial or managerial efforts of others."[368] To determine whether this prong of

[357] *See id.* at *9.

[358] *See* Michael Burns, *Highest Selling Top Shot Moments in 2021*, HOOP SOCIAL (Jul. 22, 2021), https://hoop-social.com/highest-selling-top-shot-moments-2021/ [https://perma.cc/GNU8-E6G5].

[359] *Dapper Labs, Inc.*, No. 21 CIV. 5837 (VM) (S.D.N.Y. Feb. 22, 2023), 2023 WL 2162747 at *14.

[360] *See id.* *10.

[361] *See id.* at *22 (citing *Revak v. SEC Realty Corp.*, 18 F.3d 81, 87 (2d Cir. 1994)). This is what is known as "strict vertical commonality." Other circuits also recognize what is known as "broad vertical commonality," which is established by showing that the fortunes of investors are tied to the *efforts* of the promoter. The Friel court found that plaintiffs failed to adequately allege strict vertical commonality.

[362] *See id.* at *22 (citing *Revak v. SEC Realty Corp.*, 18 F.3d 81, 87 (2d Cir. 1994)).

[363] *See id.* at *12.

[364] *See id.* at *12. Plaintiffs further alleged that purchasers' capital was then held by Dapper Labs in wallets controlled by Dapper Labs, and that Dapper Labs retained those funds for months after withdrawals were requested in order to artificially prop up the platform.

[365] *See id.* at *13.

[366] *See id.*

[367] *See id.* at *14.

[368] *See id.* at *16 (quoting *United Hous. Found., Inc. v. Forman*, 421 U.S. 837, 839 (1975)).

the Howey test is satisfied, courts must examine the offering from an objective perspective and decide whether purchasers were "led to expect" by the promoter.[369] The Friel court looked to Dapper Labs's Tweets and found that the company promoted recent sales of Moments, listing prices along with "rocket ship," "stock chart," and "money bags" emoji.[370] "And although the literal word 'profit' is not included in any of the Tweets," the court held, the "emoji objectively mean one thing: a financial return on investment."[371]

Finally, the court held that the plaintiffs had adequately alleged that the expected profits were to be derived from the efforts of others, satisfying the fourth prong of the *Howey* test.[372] Dapper Labs controlled the Moments marketplace and had the power to bring trading to a halt.[373] Dapper Labs and its partners maintained complete control over the intellectual property underlying the images associated with the Moments.[374] "Like those who invested and expected the Howey Company to care for and cultivate the citrus trees in Howey, Moments purchasers 'lack the knowledge, skill, and equipment necessary for the care and cultivation of' a blockchain and thus would not be expected to exercise control over the value creating proposition here," the court concluded.[375] With the plaintiffs satisfying all four prongs of the *Howey* test, the case was permitted to continue.[376]

If the court were to ultimately determine that the Moments are securities, Dapper Labs would be required to either go through the registration process or verify that the purchasers were accredited investors.[377] A verdict against Dapper Labs would also create uncertainty in the larger market for crypto art and collectibles.[378] The *Friel* case alone will not necessarily be dispositive for the entire industry.[379] There is tremendous variation in the NFT projects on the market today, and whether any particular offering is subject to traditional securities regulations will be a fact-specific inquiry.[380] But while a verdict against Dapper Labs

[369] *See id*. at *17.

[370] *Id*. at *17.

[371] *Id*. Other evidence that Dapper Labs promised profits to potential purchasers included Dapper Laps CEO Gharegozlou's public admissions of a profit motive. He was quoted promoting Moments to "younger generations" as an opportunity to "benefit financially" from the purchase and held his own Moments holdings out as "valuable."

[372] *See id*. at *19.

[373] *See id*. at *20.

[374] *See id*. at *21.

[375] *Id*. at *21 (quoting *S.E.C. v. W.J. Howey Co*., 328 U.S. 293, 296 (1946)).

[376] *See id*. at *22.

[377] *See* Rizzo, *supra* note 117. Accredited investors are high net worth individuals, knowledgeable finance industry employees, or others the SEC deems savvy enough to participate in risky investment schemes without the guardrails that exist for less sophisticated investors.

[378] *See id*.

[379] *See id*.

[380] *See id*.

would not mean that all NFT sales were suddenly subject to federal securities regulations, it would likely create widespread concern that they might be, which could curb the explosive growth the space has seen over the past couple of years.[381]

E. Criminal Cases

1. United States v. Chastain

Nathaniel Chastain was charged with wire fraud and money laundering in connection with his purchase and sale of NFTs on OpenSea.[382] A product manager for OpenSea, Chastain was responsible for selecting certain NFTs to be featured on OpenSea's homepage.[383] When an NFT is featured on a platform's homepage, the values of that NFT and NFTs by the same artist tend to increase as a result of the added visibility.[384] The government alleged that Chastain purchased dozens of NFTs shortly before OpenSea featured them or NFTs by the same artist on its homepage, and then quickly sold them at a profit.[385] The government charged Chastain with misappropriating OpenSea's confidential business information regarding which NFTs were due to be featured on OpenSea's homepage, thereby committing wire fraud to the tune of $50,000.[386] The government also charged Chastain with money laundering for concealing his scheme by transferring funds through anonymous Ethereum blockchain accounts and new Ethereum accounts with no prior history.[387] Though his conduct did not implicate classic insider trading under section 10(b) of the Securities Exchange Act,[388] the US Attorney's Office referred to the case as the "first ever digital asset insider trading scheme" to be prosecuted.[389]

At trial, Chastain argued that OpenSea did not treat knowledge which NFTs would be featured on its homepage as confidential information, but the jury was

[381] *See id.*

[382] *See United States v. Chastain*, No. 22-CR-305 (JMF), 2022 WL 13833637, at *1 (S.D.N.Y. Oct. 21, 2022).

[383] *See id.*

[384] *See id.*

[385] *See id.*

[386] *See id.*

[387] *See id.*

[388] *See* 15 U.S.C. § 78j(b).

[389] Press Release, *Former Employee of NFT Marketplace Charged In First Ever Digital Asset Insider Trading Scheme*, U.S. ATTORNEY'S OFFICE, SOUTHERN DISTRICT OF NEW YORK (June 1, 2023), https://www.justice.gov/usao-sdny/pr/former-employee-nft-marketplace-charged-first-ever-digital-asset-insider-trading-scheme [https://perma.cc/Q24H-XJQH].

not convinced by this argument.[390] Chastain was convicted by a jury in May of 2023.[391]

2. United States v. Nguyen and Llacuna

Federal prosecutors also arrested and charged two twenty-year-old men, Ethan Vinh Nguyen and Andre Marcus Quiddaoen Llacuna, with orchestrating a $1.1 million scam involving NFTs depicting cuddly, anthropomorphized scoops of ice cream.[392] In 2022, Nguyen and Llacuna launched an 8,888-NFT collection called Frosties that sold out within an hour of being listed on OpenSea for roughly $130 in Ethereum each.[393] Nguyen and Llacuna promised investors in the project early access to perks like a special metaverse game and the ability to "breed" new Frosties from existing characters.[394] Frosties come in different colors.[395] Some are dressed up like wizards or chefs or sharks.[396] Some are bespectacled.[397] Some sport crimson lips.[398] Others are drooling.[399] Buyers were told they would be able to propagate new Frosties with new combinations of these traits.[400] Once the collection sold out, however, Nguyen and Llacuna abandoned the project almost immediately.[401] Because cryptocurrency transactions are publicly recorded on the blockchain, certain Frosties purchasers noticed that all of the Frosties proceeds were transferred to a new wallet at approximately the same time the Frosties Website and related social media accounts were deactivated.[402] There were grumblings on social media about a suspected rug

[390] Luc Cohen, *Ex-OpenSea Manager Convicted in NFT Insider Trading Case*, REUTERS (May 3, 2023, EDT 5:46 PM), https://www.reuters.com/legal/ex-opensea-manager-convicted-nft-insider-trading-case-2023-05-03/ [https://perma.cc/LM4N-JWYN].

[391] *See id.*

[392] Press Release, *Two Defendants Charged in Non-Fungible Token ("NFT") Fraud and Money Laundering Scheme*, U.S. ATTORNEY'S OFFICE, SOUTHERN DISTRICT OF NEW YORK (Mar. 24, 2022), https://www.justice.gov/usao-sdny/pr/two-defendants-charged-non-fungible-token-nft-fraud-and-money-laundering-scheme-0 [https://perma.cc/48MP-29RD].

[393] Sarah Cascone, *Police Arrest Two 20-Year-Olds for Allegedly Conning Collectors Out of $1 Million—With Ice Cream-Themed NFT Artworks*, ARTNET (Mar. 28, 2022), https://news.artnet.com/market/frosties-nft-arrest-2090659 [https://perma.cc/8CNN-Z4NR].

[394] *See id.*

[395] *See* Frosties NFT, OPENSEA, https://opensea.io/collection/frosties-nft.

[396] *See id.*

[397] *See id.*

[398] *See id.*

[399] *See id.*

[400] Cascone, supra note 394.

[401] *See* Adi Robertson, Two Men Arrested For $1.1 Million NFT 'Rug Pull' Scam, THE VERGE (Mar. 24, 2022, EDT 5:10 PM), https://www.theverge.com/2022/3/24/22995107/us-arrest-charges-crypto-nft-rug-pull-frosties-ethan-nguyen-andre-llacuna.

[402] *See* Criminal Complaint at 10, *United States v. Nguyen and Llacuna*, https://www.justice.gov/usao-sdny/press-release/file/1486816/download [https://perma.cc/4T5K-82SS].

pull.[403] Shortly thereafter, a screenshot of a Discord message from Nguyen began circulating on Twitter.[404] The message read, in part, "I know this is shocking, but this project is coming to an end. I never intended to keep the project going, and I don't have a plan for anything in the future."[405] The message was interpreted as a confession.[406] In the criminal complaint, prosecutors alleged that Nguyen and Llacuna were planning to strike again with a follow-up NFT series called Embers.[407] The men were charged with wire fraud and conspiracy to commit money laundering.[408]

F. Service of Process Issues

Because so much of the crypto industry only exists online, and because so many who are drawn to the industry favor anonymity, it can sometimes be challenging to identify and locate defendants upon commencement of a lawsuit.[409] Frustrated plaintiffs have turned to NFTs as a way to effectuate legal process on parties in cyberspace who would otherwise remain elusive, and courts have begun to endorse this novel method of service.[410]

---

[403] *See id.*

[404] *See id.*

[405] *See id.*

[406] *See* Robertson, supra note 402.

[407] *See id.* The 5,555-piece Embers project was advertised as including a $50,000 donation to the Red Cross and a community-controlled wallet. It was expected to bring in an additional $1.5 billion.

[408] *See id.*

[409] *See* David Yaffe-Bellany, *Millions for Crypto Start-Ups, No Real Names Necessary*, N.Y. TIMES (Mar. 2, 2023), https://www.nytimes.com/2022/03/02/technology/cryptocurrency-anonymity-alarm.html. Anonymity has been important to the crypto industry from the beginning. Satoshi Nakamoto, the creator of Bitcoin, used a pseudonym and many crypto entrepreneurs go so far as to use voice-altering software on calls. Those who support anonymity argue that it levels the playing field, but many have embraced the anonymity of crypto as a way to avoid punishment for criminal activity conducted using the blockchain.

[410] At least one state court appears to have confronted requests to permit service via the blockchain before any federal courts were asked to opine on the issue. *See LCX AG v. John Doe Nos. 1-25*, No. 154644/2022 (Sup. Ct. N.Y. Co.), available at https://cases.justia.com/new-york/other-courts/2022-2022-ny-slip-op-32834-u.pdf?ts=1661548633 [https://perma.cc/5EDM-KSMT]. In *LCX AG v. John Does*, the plaintiff was a virtual asset service provider in Liechtenstein. It alleged that approximately $8 million in the provider's Ethereum-based virtual assets were stolen and sought permission to serve the defendants using cryptocurrency. Plaintiff proposed delivering a "special-purpose Ethereum-based token" to the defendants' crypto wallets. The token would contain a hyperlink to a website created by the plaintiff's law firm, and the website would publish the relevant filings. The hyperlink would include a mechanism to track when it was clicked. The court granted permission for service via the blockchain because "[c]ommunication through the account using the Service Token is effectively the digital terrain favored by the Doe Defendants. . . . Indeed, using a blockchain transaction to communicate with the Doe Defendants is the only available manner of communication." *See also* Kayla Joyce, Andrew Balthazor, and Jose Casal, *'NFT-y'*

An example of this can be seen in *Bandyopadhyay v. Defendant 1*. Plaintiff Rangan Bandyopadhyay filed a Complaint in the Southern District of Florida alleging a sophisticated global online cryptocurrency fraud scheme.[411] Bandyopadhyay alleged violations of the Racketeer Influenced and Corrupt Organizations Act ("RICO"), conversion, unjust enrichment, and conspiracy arising out of the defendants' theft of nearly $1 million in cryptocurrency from Bandyopadhyay.[412] According to Bandyopadhyay, the anonymous defendants were residents of the People's Republic of China and the most reliable way of communicating with them was via the blockchain.[413]

Bandyopadhyay created an NFT containing a notice of the action with summons language and hyperlinks to his website and a service website. His website also contained a notice of the action, with hyperlinks to the summons, complaint, and all filings and orders in the case.[414] Bandyopadhyay moved for leave to serve defendants by sending his NFT to the blockchain addresses of defendants' crypto wallets.[415]

Analyzing the issue under Federal Rule of Procedure 4, the court saw fit to permit service via NFT. Rule 4(f)(3) allows a district court to order an alternate method for service upon foreign defendants provided that the method is not proscribed by international agreement and is "reasonably calculated to give notice to the defendants."[416] Because service by NFT transfer and via posting on a designated website was not specifically proscribed under any international agreement between China and the United States, the court concluded that this method of service was appropriate.[417] Service by NFT, the court said, was reasonably calculated to give notice to the defendants, bringing Bandyopadhyay's proposal in line with the requirements of Rule 4.[418]

Service: Service of Process via NFT, 16 INSOLVENCY & RESTRUCTURING INT'L 24 (2022) (discussing the implications of *LCX AG v. John Does*).

[411] *Bandoyopadhyay v. Defendant 1, et al.*, No. 22-cv-22907 (S.D. Fl. 2022), 2022 WL 17176849. Miami has actively sought to position itself as the crypto capital of the United States, advancing a range of policies designed to make the city a friendly destination for crypto startups. *See* Andrew Ross Sorkin, Jason Karaian, Michael J. de la Merced, Ephrat Livni, and Sarah Kessler, *Miami Wants to Be the Hub for Bitcoin*, N.Y. TIMES (Mar. 23, 2021).

[412] *See id.*

[413] *See id.*

[414] *See id.*

[415] *See id.*

[416] *Id.*; *see also* Fed. R. Civ. P. 4.

[417] *See id.*

[418] *See id.* at *3; *see also Ohlin v. Defendant 1*, No. 3:23CV8856-TKW-HTC 2023 WL 4084523, at *1 (N.D. Fla. June 8, 2023) (granting permission for plaintiff to serve defendant via NFT); *but see De Ford v. Koutoulas*, No. 6:22-CV-652-PGB-DCI, 2022 WL 17823868, at *4 (M.D. Fla. Dec. 12, 2022) (denying permission for plaintiff to serve defendant via NFT in dispute over meme cryptocurrency LGBCoin).

CONCLUSION

Whether NFTs become a ubiquitous and durable feature of contemporary life, as some predict they will,[419] or disappear entirely from the cultural landscape, they will not be the last technology to catch consumers, courts, and lawmakers off guard. Early litigation involving NFTs illustrates the risks of operating in an emergent industry, especially one as irresistibly attractive to snake oil salesmen as crypto. But by understanding the mistakes made by early adopters, innovators can position themselves to take more calculated risks with crypto today, artificial intelligence tomorrow, or whatever the next Big Thing on the horizon turns out to be.

It is also instructive to examine the ways in which the courts are meeting (and failing to meet) the needs of litigants in the context of NFTs because, as the pace of technological change accelerates, we will find ourselves operating in these zones of legal and social uncertainty with increasing frequency. Disruption is lucrative, at least for the disruptors, and the improbable ascent of the NFT suggests that no monetizable aspect of human experience is entirely immune from "improvement." Blockchain technology may become obsolete, and arguments over the details of a license for an image of a computer-generated monkey may soon seem quaint or look like the product of pandemic-era collective hallucination. As our lives become more and more virtual, however, bodies of law dealing with analog reality may be the ones that come to seem quaint or quirky. There is no indication that we are losing interest in online structures of communication, community, and exchange, and these evolving structures will continue to challenge settled assumptions about art, ownership, and value.

[419] *See* LEE, *supra* note 2 at 293 (likening the invention of the NFT to the Wright brothers achieving the dream of human flight).

NOTE

CONSUMER PROTECTION OF GENETIC DATA: THE CALIFORNIA MODEL

JANE MURPHY

CONTENTS

INTRODUCTION

As the field of genetics grows and streamlines itself, so too does the ease of public access to it. For-profit companies such as 23andMe and Ancestry.com are making it easier than ever for consumers to procure genetic tests of their own volition.[1] While this can have beneficial uses, such as the identification of genetic predispositions towards certain health issues or the ability to trace ones' ancestry, it also raises a number of concerns for consumers.[2] Direct-to-consumer genetic testing companies often utilize user data and genetic samples for purposes such as their own research, marketing, and perhaps most troubling of all, third-party sales.[3] Unlike with genetic testing conducted by a physician or through a medical office, it is up to consumers to carefully review the disclosures given by the genetic testing company, and in many cases these disclosures are buried within lengthy legal documents the average consumer is not equipped to parse.[4] Beyond this, there is the risk that samples used for the above-stated purposes might be insufficiently disguised, and therefore lead to the identification of sources who did not consent to such exposure.[5]

Genetic data is a singularly sensitive type of health information, in that it serves as a unique marker for each of us.[6] This quality positions it as something that lawmakers have a particular interest in protecting from disclosure in any form without explicit consent.[7] This is especially true when that data belongs to commercial consumers and not to medical patients, as the machinery of medical confidentiality offers significantly less protection to those seeking direct-to-consumer tests.[8] This interest held by lawmakers is evidenced by genetic data's partial inclusion within federal laws such as the Health Insurance Portability and

---

[1] *See* Kevin C. Gilligan, Note, *Protecting Consumers and Regulating Data: The Need for Comprehensive Federal Oversight of the Direct-to-Consumer Genetic Testing Industry*, 14 DREXEL L. REV. 207, 209-10 (2022).

[2] *See* Janessa Mladucky, Bonnie Baty, Jeffrey Botkin & Rebecca Anderson, *Secondary Data Usage in Direct-to-Consumer Genetic Testing: To What Extent Are Customers Aware and Concerned?*, 24 PUB. HEALTH GENOMICS 199, 200 (2021).

[3] *Id.*

[4] *See* Andelka M. Phillips, *Only a Click Away — DTC Genetics for Ancestry, Health, Love…and More: A View of the Business and Regulatory Landscape*, 8 APPLIED & TRANSLATIONAL GENOMICS 16, 16 (2016).

[5] *See* Mladucky et al., *supra* note 2, at 200 (describing several reidentification risk scenarios).

[6] *See* Gilligan, *supra* note 1, at 210; Tim Newman, *What Is DNA and How Does It Impact Health?*, MED. NEWS TODAY, https://www.medicalnewstoday.com/articles/319818 [https://perma.cc/542H-VHEP] (last updated Feb. 14, 2023).

[7] *See* Aaron Shaffer, *Hacks of Genetic Firms Pose Risk to Patients, Experts Say*, WASH. POST (July 21, 2022, 7:16 AM), https://www.washingtonpost.com/politics/2022/07/21/hacks-genetic-firms-pose-risk-patients-experts-say/ [https://perma.cc/NH39-D2XR].

[8] *See* Reinaldo Franqui Machin, *Stop Looking at My Genes!: Direct-to-Consumer Genetic Testing and the Illusion of Privacy and Consent*, 61 REVISTA DE DERECHO P.R. 233, 234 (2022).

Accountability Act ("HIPAA") and the Genetic Information Nondiscrimination Act ("GINA"), as well as individual state efforts at consumer protection of genetic information.[9] However, no federal law or agency offers blanket protection for consumers tailored to genetic privacy, and while several promising state laws have made an appearance in the past few years, they are just that: state laws.[10] They offer no protection to those living in areas that have not yet managed to erect comparable protections of their own.

Given the pressing need for robust protection in this area, the current law is too much of a patchwork to be effective in protecting consumers against private testing companies.[11] Rather than the existing scattered efforts at providing protection, more success might be found in introducing one federal genetic data privacy law based on the fledgling efforts of states to craft a state-level version of the same. Part I of this Note provides background on the current law in this area, addressing prominent federal laws and regulatory actions (HIPAA, GINA, and the Federal Trade Commission ("FTC")), a sampling of some of the more relevant state laws, and one law that has found success abroad (the EU's General Data Protection Regulation ("GDPR")). Part II will then detail some of the issues that these laws face which prevent them from effectively guarding against misuse of consumer genetic data. These include HIPAA's limited scope regarding which entities are prevented from sharing patients' health data, GINA's failure to protect against disclosures, and the practices employed by direct-to-consumer genetic testing companies that allow them to distribute some data without the consent of customers. Finally, Part III will analyze which elements of the state laws seem most promising or have proved successful in practice, and then propose a policy for how these might fit together to provide robust protection against genetic data exploitation.

I. BACKGROUND

A. Direct-to-consumer genetic testing: the basics

Direct-to-consumer genetic testing first entered the market in the early 2000s as an alternative to more formal testing performed by a medical professional.[12] Originally a costly option at around $1,000 a test, the market has since grown and diversified to the point that a test costs as little as $99.[13] These tests can be purchased online or in a store, and typically gather DNA by means of a saliva

[9] *See id*. at 237-38; Benjamin T. Van Meter, Note, *Demanding Trust in the Private Genetic Data Market*, 105 CORNELL L. REV. 1527, 1536-37 (2020).

[10] *See* Gilligan, *supra* note 1, at 227; Van Meter, *supra* note 9, at 1536-37.

[11] *See* Gilligan, *supra* note 1, at 227.

[12] Haley J. Guion, *Inconclusive Results*, 108 ILL. BAR J. 32, 32 (2020).

[13] *Id*.

sample, which is sent by mail to the testing company.[14] The company then provides the results of the tests to the consumer via the internet.[15] The variety of tests offered is wide: nutrigenomic tests, pharmacogenomic tests, disease susceptibility tests, and ancestry tests, among others.[16] Most companies use genotyping to gather the information from these tests, which is "the process by which an individual's DNA is sequenced and then specific locations throughout the sequence are analyzed to identify variants."[17] By comparing the consumer's DNA sequences against existing samples and looking for patterns, the company can provide information such as the consumer's physical traits and ancestry.[18]

B. Uses of direct-to-consumer genetic testing and related data

Direct-to-consumer genetic testing can serve a number of purposes for consumers. One of the most common purposes is to provide the consumer with the type of health information that can be gleaned from ones' genes.[19] For example, this health information can reveal whether the consumer is a carrier of a gene associated with a particular illness, for the purposes of understanding risks to themselves or to their children.[20] Health information can also be used to determine how the body processes different nutrients.[21] The other most common use for this type of genetic testing is to provide the consumer with information about their ancestry.[22] This includes information about geographic and ethnic origin, as well as the ability to trace living relatives.[23] An offshoot of this particular use is genetic-relatedness, often for the purposes of testing paternity.[24]

The data produced by these tests also serves a purpose for the companies providing the testing. Companies use data for, among other things, "internal research, quality control, marketing, and third-party sales."[25] For example, data might be used to develop new products, or be sold to pharmaceutical companies conducting research.[26] There are in fact a number of benefits associated with the sharing and use of this data. The sheer volume of genetic data has greatly sped

[14] *See* Jacqueline Moran, *Privacy Perspectives on Direct-to-Consumer Genetic Testing in the Era of Big Data: Role of Blockchain Technology in Genomics*, 22 TUL. J. TECH. & INTELL. PROP. 185, 191 (2020).

[15] *Id*.

[16] *Id*.

[17] Juan Pablo Sarmiento Rojas, *Direct-to-Consumer Genetic Testing: Rethinking Privacy Laws in the United States*, 14 HEALTH L. & POL'Y BRIEF 21, 24 (2020).

[18] *Id*. at 24-25.

[19] Phillips, *supra* note 4, at 17.

[20] *Id*.

[21] Moran, *supra* note 14, at 191.

[22] *See* Phillips, *supra* note 4, at 18.

[23] *Id*.

[24] *Id*. at 19.

[25] Mladucky, *supra* note 2, at 200.

[26] *Id*.

up some types of medical research, allowing researchers to accomplish such goals as identifying risk factors for Alzheimer's disease.[27] Because of the legitimate uses of direct-to-consumer testing and the genetic data it produces, both in terms of personal benefits to the customer and to society as a whole, it is important to strike a balance that allows this testing to continue in a way that retains these benefits while also protecting consumers.

C. Privacy concerns generated by direct-to-consumer genetic testing

Because of the sensitive nature of genetic data and the as-yet not fully regulated privacy practices of direct-to-consumer genetic testing companies, the field raises a number of potential privacy concerns.[28] The basis of much of this concern is that while consent generally must be obtained to sell, lease, or rent out data that renders the consumer identifiable, when that same data is grouped with the data of other consumers and stripped of identifying information (or "de-identified") it can be distributed without consent.[29] There is also the threat that this genetic data can be re-identified – that the individual who provided the sample can be identified by information still present in de-identified data.[30] This can occur in a few different ways, but the most prominent is that the data is insufficiently de-identified to begin with. Because genetic data is unique to each individual, it is difficult to render it fully incapable of tracing back to its source.[31] Information such as postal area codes can also be left appended to data, which poses a similar risk of allowing the sample to be followed back to the subject that provided it.[32]

The risks associated with reidentification are varied. If data is obtained after distribution to a third party and reidentified, it could be used for purposes such as paternity suits, criminal investigations, insurance discrimination, national security or immigration cases, or unwanted disclosure of the existence or status of relatives.[33]

D. Current Federal Law

As previously indicated, there has already been some effort to use federal law as a method of protecting genetic data. HIPAA is one such law, passed by Congress in 1996 with the goal of preventing unauthorized disclosure of sensitive health information.[34] HIPAA's Privacy Rule creates standards for use and disclosure of protected health information ("PHI") by certain covered entities

[27] Machin, *supra* note 8, at 236.

[28] *See* Kristi Harbord, *Genetic Data Privacy Solutions in the GDPR*, 7 TEX. A&M L. REV. 269, 278 (2019); Sarmiento Rojas, *supra* note 17, at 23.

[29] Sarmiento Rojas, *supra* note 17, at 26.

[30] Gilligan, *supra* note 1, at 225.

[31] *Id*. at 226.

[32] *Id*.

[33] *See* Mladucky, *supra* note 2, at 200.

[34] *See* Sarmiento Rojas, *supra* note 17, at 30.

(namely health plans), the majority of health care providers, health care clearinghouses, and business associates of other covered entities.[35] PHI consists of information included in a medical record, conversations about treatment, information contained in a health insurer's system, billing information, and other health information possessed by covered entities (in other words, identifiable health information).[36]

HIPAA's Security Rule protects a narrower strip of information, limited to PHI that "a covered entity creates, receives, maintains, or transmits in electronic form," otherwise known as electronic protected health information ("e-PHI").[37] These entities must maintain reasonable "administrative, technical, and physical safeguards" for e-PHI to be compliant with the Rule.[38]

Finally, the Breach Notification Rule requires covered entities to notify affected parties after a breach of PHI or e-PHI.[39] A breach is defined as any unauthorized use or disclosure, with some limited exceptions.[40] As identifiable health information, genetic data falls under the definition of PHI, and is therefore subject to HIPAA.[41] Specifically under the Act, genetic data cannot be used to determine coverage, set premiums, or act as evidence of a pre-existing condition if held by a covered entity.[42] However because the definition of covered entities is a narrow one, direct-to-consumer genetic testing companies are likely not included.[43]

GINA is another, slightly more pointed, federal law dealing with genetic data security. GINA was enacted by Congress in 2008 in response to the increasing availability of genetic data, and with the specific purpose of preventing its discriminatory use by employers and health insurance companies.[44] Genetic information in the context of this law refers to information about an individual's genetic tests or those of family members; family medical history, requests or receipts for genetic services related to an individual or their family; and

[35] *Health Insurance Portability and Accountability Act of 1996 (HIPAA)*, CTRS. FOR DISEASE CONTROL AND PREVENTION (June 27, 2022), https://www.cdc.gov/phlp/publications/topic/hipaa.html [https://perma.cc/3QKX-RM29]; *Your Rights Under HIPAA*, U.S. DEP'T HEALTH AND HUM. SERVS. (Jan. 19, 2022), https://www.hhs.gov/hipaa/for-individuals/guidance-materials-for-consumers/index.html [https://perma.cc/3SYE-W6VG]; *see also* 45 C.F.R. § 164.105 (2013).

[36] *See* U.S. DEP'T HEALTH AND HUM. SERVS., *supra* note 35.

[37] CTRS. FOR DISEASE CONTROL AND PREVENTION, *supra* note 35; *see also* 45 C.F.R. § 164.105.

[38] Sarmiento Rojas, *supra* note 17, at 31.

[39] *Id*. at 32.

[40] *Id*.

[41] *See id*. at 33.

[42] Claire M. Amodio, *23andme: Attack of the Clones and Other Concerns*, 31 FORDHAM INTELL. PROP., MEDIA & ENT. L.J. 926, 941 (2021).

[43] Sarmiento Rojas, *supra* note 17, at 33.

[44] *See* Michael R. Dohn, *Personal Genomics and Genetic Discrimination: Is Increased Access A Good Thing?*, 45 W. STATE L. REV. 107, 122 (2018).

information about a fetus or embryo belonging to an individual or their family.[45] Employers cannot use genetic data to make hiring, firing, or career advancement decisions, nor can they allow it to influence compensation, privileges, or terms of employment.[46] In fact, they are not permitted to acquire this genetic information at all, with some very narrow exceptions.[47]

Health insurance companies face similar restrictions, as they are prevented from using genetic information to establish eligibility, adjust premiums or determine the cost of coverage based on predictive genetic data.[48] Health insurers, like employers, are prohibited from purchasing an individual's genetic information, or requiring that they or their family members take any kind of genetic test (again, with limited exceptions).[49] GINA is also the reason that genetic information is classified as PHI under HIPAA; GINA amended HIPAA to require that genetic information be treated as health information for purposes of the Act, affording it the protections thereto.[50] Because GINA deals with potential end users rather than holders of genetic data, any data produced through direct-to-consumer genetic testing companies is in fact covered under the Act.[51]

E. Federal Regulatory Agencies

The only federal regulatory agency to really touch on direct-to-consumer genetic testing as it relates to company privacy and disclosure policies is the Federal Trade Commission. The purpose of the Commission is to protect consumers from unfair trade practices, which it accomplishes through enforcing laws and regulations.[52] The Commission defines unfair trade practices as those that "cause[] or [are] likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[53] The FTC can go after companies for being deceptive if they fail to follow their own stated privacy practices or are otherwise deceptively inadequate in their protection of consumer privacy.[54] Although it has not officially released a compliance guide for direct-to-consumer testing companies, the FTC has issued informal advice on best practices in an unofficial statement, including advice on adequate disclosure and the

[45] Amodio, *supra* note 42, at 939; *Genetic Information Discrimination*, U.S. EQUAL EMP. OPPORTUNITY COMM'N, https://www.eeoc.gov/genetic-information-discrimination [https://perma.cc/NZ8D-EFMA].

[46] Amodio, *supra* note 42, at 939; U.S. EQUAL EMP. OPPORTUNITY COMM'N, *supra* note 45.

[47] Amodio, *supra* note 42, at 939; U.S. EQUAL EMP. OPPORTUNITY COMM'N, *supra* note 45.

[48] Sarmiento Rojas, *supra* note 17, at 29; Dohn, *supra* note 44, at 123.

[49] Dohn, *supra* note 44, at 123.

[50] *Id*.

[51] *See* 42 U.S.C. § 300gg-53 (2008).

[52] *See* Harbord, *supra* note 28, at 284.

[53] 15 U.S.C. § 45(n) (2006).

[54] Harbord, *supra* note 28, at 284.

suggestion that companies include a "one-stop-shop" option for expunging genetic information.[55]

F. Current State Law

There is no uniform approach among the states to regulating and protecting genetic data against unpermitted disclosure or use. As is often the case in state law, some states take a stricter approach and offer greater protection while others choose to remain more hands-off. However, as of 2019, every state, with the exception of Mississippi, has at last *some* law touching on the topic.[56]

California is among the more protective states, with both the Genetic Information Privacy Act ("GIPA") and the California Consumer Privacy Act ("CCPA").[57] In short, GIPA requires direct-to-consumer genetic testing companies to meet certain standards of transparency about their data collection and disclosure practices, and to obtain consent from individuals before their data is used.[58] It broadly defines the term "genetic testing companies" to provide as wide a range of protection as possible, with financial penalties if companies fail to abide by its requirements.[59]

The CCPA is not a targeted statute but applies to personal information overall. It defines personal information as any "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household."[60] This includes genetic data, as it is an inherent identifier of the individual from which it was gathered.[61] Under the CCPA, businesses that collect this personal information are required to inform the consumer that they are doing so and what

---

[55] *See* Elisa Jillson, *Selling Genetic Testing Kits? Read On.*, FED. TRADE COMM'N: BUS. BLOG (March 21, 2019), https://www.ftc.gov/business-guidance/blog/2019/03/selling-genetic-testing-kits-read [https://perma.cc/HG4V-WPVF]; Linda Malek, Jason Johnson, and Khaled Mowad, *Genetic Testing is on FTC's Radar*, LAW360 (April 18, 2019, 3:10 PM), https://www.law360.com/articles/1151143/genetic-testing-is-on-ftc-s-radar [https://perma.cc/26FZ-BH8B].

[56] *See* JUSTICE MING W. CHIN, ET AL., FORENSIC DNA EVIDENCE: SCIENCE AND THE LAW § 13:13 (The Rutter Group, 2023).

[57] *See* Harbord, *supra* note 28, at 286; Korey Clark, *State Lawmakers Find Success with Genetic Privacy*, LEXISNEXIS: INSIGHTS (June 17, 2022), https://www.lexisnexis.com/community/insights/legal/capitol-journal/b/state-net/posts/state-lawmakers-find-success-with-genetic-privacy#:~:text=The%20federal%20Health%20Insurance%20Portability,tests%20didn't%20even%20exist [https://perma.cc/6AGC-X6KX].

[58] *See* Jill McKeon, *Growing Number of States Enact New Genetic Data Privacy Laws*, HEALTH IT SECURITY: PATIENT PRIV. NEWS (Oct. 27, 2021), https://healthitsecurity.com/news/growing-number-of-states-enact-new-genetic-data-privacy-laws [https://perma.cc/6A73-MQK7].

[59] *Id.*

[60] California Consumer Privacy Act, CAL. CIV. CODE § 1798.140(v) (effective Jan. 1, 2020).

[61] Harbord, *supra* note 28, at 286.

the purpose of the collection is.[62] Consumers also have the right to opt out of the sale of their personal information by the collecting company.[63]

As of 2022, there are four states that have joined California in enacting comprehensive consumer privacy laws, including: Colorado, Connecticut, Utah, and Virginia.[64] Privacy laws dealing solely with consumer genetic information are starting to gain traction as well, with bills proposed in nine states and enacted in seven in 2021.[65] Arizona, Florida, Utah, Kentucky, Maryland, and Wyoming are some of the states that have enacted targeted genetic privacy laws.[66] A common thread among them seems to be transparency requirements for companies providing testing, so as to ensure consumers are aware of the possibility of disclosures and what the company intends to use the samples for.[67] In addition, some states have added consent as a requirement before data can be distributed to outside parties.[68]

G. Current Foreign Law

In May 2018, the European Union adopted the General Data Protection Regulation.[69] This is one of, if not the most, comprehensive pieces of data privacy legislation ever enacted.[70] The purpose of the regulation is to standardize data privacy laws across all EU member states, as well as to create stricter rules on how personally identifiable data is processed and handled.[71] The rules of the GDPR apply to any organization that collects or processes the data of citizens of an EU member state.[72] This applies regardless of whether the organization itself is based in the EU. The penalty for violation of the GDPR is a large fine, which caps at $22 million.[73] Anyone "processing," or coming into contact with, personally identifying data must have a legal basis for doing so, and collection and

[62] *GIPA: The Genetic Information Privacy Act*, CLARIP, https://www.clarip.com/data-privacy/the-genetic-information-privacy-act/#:~:text=The%20Genetic%20Information%20Privacy%20Act%20(GIPA)%20was%20signed%20into%20law,also%20focused%20on%20consumer%20privacy [https://perma.cc/5LLH-K5BA].

[63] *Id*.

[64] Pam Greenberg, *2022 Consumer Privacy Legislation*, NCSL (June 10, 2022), https://www.ncsl.org/about-state-legislatures/2022-consumer-privacy-legislation#:~:text=At%20least%2034%20states%20and,and%20the%20District%20of%20Columbia [https://perma.cc/9MXV-KL6K].

[65] Clark, *supra* note 57.

[66] McKeon, *supra* note 58; Greenberg, *supra* note 64.

[67] Greenberg, *supra* note 64.

[68] *Id*.

[69] Sarmiento Rojas, *supra* note 17, at 36.

[70] *See id*.

[71] *See* Harbord, *supra* note 28, at 287.

[72] Sarmiento Rojas, *supra* note 17, at 36.

[73] Harbord, *supra* note 28, at 287.

storage of data is limited to what is absolutely necessary.[74] In addition, there must be a high level of transparency related to the processing of data.[75] Individuals can also require that organizations erase identifiable information held about them.[76]

In addition to the above-stated protections, the GDPR prohibits the processing of sensitive data such as "racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and . . . genetic data . . ."[77] Genetic data for purposes of this legislation is defined broadly, amounting to basically any genetic characteristics that are personally identifiable that result from a biological sample.[78] There are some limited exceptions to this prohibition, namely use aligning with public policy purposes and explicit consent.[79]

While the GDPR does not apply to anonymized data, the regulation does take into account the possibility of methods capable of re-identifying this data. Data can only be considered anonymous if that "information is kept separately and is subject to technical and organizational measures to ensure that the personal data are not attributed to an identified or identifiable natural person."[80] Under this formulation of anonymization, the results of genetic tests such as those distributed by direct-to-consumer genetic testing companies are likely to be considered non-anonymized, and therefore they would be generally prohibited from storage or use.[81]

II. ISSUES WITH CURRENT LEGISLATION

A. HIPAA

Perhaps because it was enacted before the rise of the direct-to-consumer genetic test, HIPAA offers very limited protection of genetic information as a whole and almost none regarding private genetic testing companies.[82] HIPAA fails to stop insurance companies from requesting genetic information from those that they insure or from using this information in the underwriting process.[83] It also permits insurance companies to get around the ban on charging an individual more because of genetic status by instead charging everyone in their

[74] Sarmiento Rojas, *supra* note 17, at 36.

[75] *Id*. at 37.

[76] *Id*.

[77] *See id*.; Regulation (EU) 2016/679, of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data and Repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, art. 9 [hereinafter GDPR].

[78] Harbord, *supra* note 28 at 289; GDPR, *supra* note 77, art. 4, ¶ 13.

[79] Harbord, *supra* note 28, at 289; GDPR, *supra* note 77, art. 9, ¶ 2.

[80] GDPR, *supra* note 77, art. 4, ¶ 5.

[81] *See* Harbord, *supra* note 28, at 290.

[82] *See* Amodio, *supra* note 42, at 941.

[83] *Id*. at 941-42.

group plan more.[84] Additionally, HIPAA is silent on whether it is permissible for third parties to disclose genetic data to insurance companies.[85] Insurance companies are not barred from using genetic data produced through direct-to-consumer tests as the basis for charging an entire group a higher rate, and inversely direct-to-consumer testing companies are not barred from providing this information to insurance companies.[86]

Furthermore, while HIPAA requires medical records to be de-identified, the standards under the Act are not enough to solve the issues with de- and re-identification listed above.[87] While elements like name, address, and contact information are usually removed from records, other traits such as health, medical conditions, diseases, and lifestyle are retained to facilitate the research process.[88] This is sometimes enough to trace genetic data back to the source, a fact which HIPAA does not address and therefore does not offer adequate protection against.

Finally, HIPAA only applies to covered entities (namely health plans, health care providers, and business associates), and within those entities there are a number of disclosure exceptions.[89] These include "'treatment, payment, and routine health care operations'; public health; 'specialized government functions, including national security and intelligence operations'; law enforcement; and 'judicial and administrative proceedings.'"[90] Covered entities are defined narrowly, and as such it is unlikely that direct-to-consumer genetic testing companies fall within the statute at all.[91]

B. GINA

GINA, while more targeted towards misuse of genetic data than HIPAA, has its own issues that render it insufficient as a means of regulating direct-to-consumer genetic testing. To begin, the Act is not directed towards the blanket prevention of unauthorized disclosure and does not require that the proposed use be explained, or consent be sought.[92] Additionally, it only covers health insurance – this means that "life, long-term care, [and] disability insurance providers" are not covered.[93] GINA also "does not apply to employers with less than fifteen employees, military, or Indian Health Services." [94] While the Act does prevent discrimination from an insurer in the event that genetic tests reveal a

[84] *Id*. at 942.

[85] *Id*.

[86] *Id*.

[87] *See* Dohn, *supra* note 44, at 119-20.

[88] *Id*.

[89] Harbord, *supra* note 28, at 282-83; Sarmiento Rojas, *supra* note 17, at 30.

[90] Harbord, *supra* note 28, at 282-83.

[91] Sarmiento Rojas, *supra* note 17, at 33.

[92] Gilligan, *supra* note 1, at 240.

[93] Amodio, *supra* note 42, at 939-40.

[94] Harbord, *supra* note 28, at 283.

predisposition to a particular illness, once you begin to exhibit symptoms you are no longer protected.[95] This is true even where the diagnosis came about because of a genetic test.[96] Finally, GINA makes no mention of direct-to-consumer genetic testing companies.[97] Direct-to-consumer genetic testing companies disclose aggregate data to many third parties who have nothing to do with insurance or employment, leaving GINA with little impact on genetic consumer protection.[98]

C. FTC

The Federal Trade Commission is also not entirely adequate as a form of consumer protection against direct-to-consumer genetic disclosures. The FTC can only enforce standards that companies have already put in place for themselves.[99] Therefore, if the genetic testing companies have particularly loose standards regarding disclosure and privacy, there is nothing the FTC can do to change that fact. They are not empowered to mandate reform of a company's policy and must work within the framework that already exists.[100] Additionally, if a company openly discloses that it intends to share user data, relying on the fact that many consumers are unlikely to do the research into whether or not this is the case, the FTC cannot discipline them for this.[101]

D. GDPR

Although the GDPR is not a US-based attempt at protecting genetic data privacy, it is worthwhile as an academic exercise to point out some issues the regulation has with protecting consumer genetic data to aid this analysis and policy proposal. Because of how broad and comprehensive this regulation is, there are fewer snags to deal with than GINA or HIPAA, but they do exist. One such concern is that there is a fairly broad research exemption to the prohibition on use of sensitive data such as genetic information.[102] This might pave the way for distribution of genetic data from direct-to-consumer tests to third parties so long as it is for the purposes of scientific or medical research.[103] In addition to this, there is no standardization on what "reasonably likely to be used" means in terms of the method of re-identification of data.[104] Because cost, technology available, and time required are all variables, and these can vary wildly between the parties

[95] *Id.* at 284.
[96] *Id.*
[97] Gilligan, *supra* note 1, at 241.
[98] *See id.*
[99] *See* Harbord, *supra* note 28, at 285.
[100] *Id.*
[101] *Id.*
[102] Sarmiento Rojas, *supra* note 17, at 38.
[103] *See id.*
[104] *See id.*

attempting the re-identification process, it is possible that certain types of genetic data, including direct-to-consumer test results, might slip under the GDPR's radar.[105]

E. Direct-to-Consumer Contracts and Disclosures

Finally, the contracts and disclosures provided by the direct-to-consumer genetic testing companies themselves are far from adequate at protecting against their own organizations' use and sale of genetic data. While the necessity of written consent and the standards of transparency vary from state to state, most companies have consent-to-use documents and privacy policies in place which disclose information about the potential purposes and risks of genetic data.[106] The most obvious complaint here is that the average consumer is not at all prepared to read and process a complicated contract; it would be difficult for someone not versed in contract law to understand which provisions might be harmful to their genetic data privacy, or what rights they might be signing away regarding their personally identifying information.[107] And even if they had a sophisticated enough understanding of contracts to object to certain provisions and clauses, most consumers don't bother to read these types of contracts at all because of their length and the density of language they use.[108] According to data gathered by Deloitte, out of a sample of 2,000 consumers, 91% of people accept terms and conditions without actually taking the time to read them, a number which increases to 97% when looking at young adults between eighteen and thirty-four.[109] Although one might argue this inability or unwillingness to engage with contracts is the fault of the consumer (which is not a particularly *fair* argument considering it takes three to four months of law school education to even get the basics down), this trend still prevents consent contracts from serving as an effective means of consumer protection.

In addition to this, the documents themselves might be drafted in such a way as to grant the issuing companies broad rights to use and disclose consumers' genetic data without alerting the consumer. For example, important provisions such as what types of research the data may permissibly be used for or what risks can arise from genetic data disclosure can be buried deep in the contract in a

[105] *See id*.

[106] *See* Eric Rosenbaum, *5 Biggest Risks of Sharing Your DNA with Consumer Genetic-Testing Companies*, CNBC (June 16, 2018), https://www.cnbc.com/2018/06/16/5-biggest-risks-of-sharing-dna-with-consumer-genetic-testing-companies.html [https://perma.cc/3UY5-UPX8].

[107] *See* Amodio, *supra* note 42, at 961-63.

[108] *See* Amodio, *supra* note 42, at 962.

[109] *Id*.; Caroline Cakebread, *You're Not Alone, No One Reads Terms of Service Agreements*, BUS. INSIDER (Nov. 15, 2017, 7:30 AM), https://www.businessinsider.com/deloitte-study-91-percent-agree-terms-of-service-without-reading-2017-11 [https://perma.cc/6PJB-EB63].

location where it does not obviously stand out.[110] This is the case with 23andMe's consent agreement, which contains the former provision halfway through a ten-page document, and the latter on page seven.[111] 23andMe also contains a "key points" section at the beginning of the document; notably, certain key points are missing from this section, including notification of data use in pharmaceutical research.[112] Because the key points section is presented as containing a summary of the important information in the contract, this type of drafting is likely to fool some consumers into thinking there are no further risks or concerns they should be aware of.[113] This in turn means that consumers are not consenting with full knowledge of where their data might go or be used for, and whether there are any potential risks associated with its use.[114]

Another area of significant concern with these self-imposed privacy policies and consent standards is that they are just that: self-imposed. Companies can amend their own policies, meaning protection afforded by well-put-together privacy policies might not be permanent.[115] There is also the fact that these privacy policies and consent standards do not tend to extend to de-identified data, so potentially identifying pieces of genetic information are not covered by the company's own consumer protection efforts.[116] This information is not as readily shared in the privacy and disclosure statements as information related to the purpose of identified data. In fact, data suggests that 40% of donors did not know that companies like 23andMe sold their data at all.[117]

III. POLICY PROPOSAL: FROM STATE TO FEDERAL LAW

As illustrated above, there are sizable issues with the current system we have in place to protect consumers from direct-to-consumer genetic testing companies. HIPAA was not crafted with genetic data in mind, GINA was not crafted with disclosures in mind, and the FTC can do little to force these companies to alter their behavior outside of punishing individual instances of deceptive practice.[118] The effectiveness of state law can vary, and even the most promising of state initiatives really only apply to that state.[119] Similarly, while a promising

[110] *See* Amodio, *supra* note 42, at 953.

[111] *Id*.

[112] *Id*. at 956.

[113] *See id*.

[114] *See id*.

[115] Rosenbaum, *supra* note 106.

[116] Machin, *supra* note 8, at 241.

[117] *Id*.

[118] *See* CTRS. FOR DISEASE CONTROL AND PREVENTION, *supra* note 35; U.S. EQUAL EMP. OPPORTUNITY COMM'N, *supra* note 45; *see* Malek, *supra* note 55.

[119] *See* Clark, *supra* note 57.

method of consumer protection, the GDPR is not United States law.[120] And companies cannot be trusted to monitor themselves.[121]

It is impractical that what protection we do have is scattered between these different laws and regulatory bodies. Rather than this cobbled together attempt at protecting consumers, which still contains significant gaps in coverage, there should be a singular federal "blanket" statute aimed specifically at genetic data privacy and offering comprehensive protection. The easiest way to achieve this is to do what is so often done when crafting federal law: to turn to the experimentation of states as a guide. The strictest United States privacy laws belong to California, which has also recently passed legislation aimed specifically at regulating direct-to-consumer genetic testing companies.[122] In addition to this, several other states have made impressive headway in their own versions of genetic data-specific laws.[123] The following section therefore proposes the use of California's Genetic Information Privacy Act as a template for a federal act, while also drawing elements from other relevant state laws.

A. Genetic Information Privacy Act ("GIPA")

California's GIPA was signed into law on October 6, 2021, and took effect on January 1, 2022.[124] GIPA applies specifically to direct-to-consumer genetic testing companies, as opposed to existing federal laws such as HIPAA and GINA. The Act defines these companies as any entity that does one or more of the following:

(A) Sells, markets, interprets, or otherwise offers consumer-initiated genetic testing products or services directly to consumers.

(B) Analyzes genetic data obtained from a consumer, except to the extent that the analysis is performed by a person licensed in the healing arts for diagnosis or treatment of a medical condition.

(C) Collects, uses, maintains, or discloses genetic data collected or derived from a direct-to-consumer genetic testing product or service, or is directly provided by a consumer.[125]

Section (A) makes clear that, by definition, this Act is specifically targeting those companies that offer direct-to-consumer genetic testing.

The Act then imposes a number of requirements on companies to safeguard the "privacy, confidentiality, security, and integrity of a consumer's genetic

[120] *See* Sarmiento Rojas, *supra* note 17, at 36.

[121] *See* Rosenbaum, *supra* note 106.

[122] Gilligan, *supra* note 1, at 235; *Genetic Information Privacy Act (California)*, PRIVACYRIGHTS.ORG (Feb. 1, 2022), https://privacyrights.org/resources/genetic-information-privacy-act-california#:~:text=The%20Genetic%20Information%20Privacy%20Act,with%20access%20and%20deletion%20rights [https://perma.cc/933L-QWJ5].

[123] *See* Clark, *supra* note 57.

[124] Genetic Information Privacy Act (California), *supra* note 122 (providing a brief history of GIPA).

[125] CAL. CIV. CODE § 56.181 (2022).

data."[126] The first of these is to provide certain clear and complete disclosures to consumers.[127] One such disclosure is "[a] summary of its privacy practices, written in plain language, that includes information about the company's collection, use, maintenance, and disclosure, as applicable, of genetic data."[128] This is likely designed to resolve the problem of so-called "legalese" in the privacy policies put forward by direct-to-consumer testing companies, as the phrasing "plain language" signals.[129] The next such disclosure is

A prominent and easily accessible privacy notice that includes, at a minimum, complete information about the company's data collection, consent, use, access, disclosure, maintenance, transfer, security, and retention and deletion practices, and information that clearly describes how to file a complaint alleging a violation of this chapter . . .[130]

This too is seemingly written to combat the issue of inaccessible and strategically drafted company disclosure documents.[131] It also provides a specific list of what consumers need to know that covers the full life of their genetic data from collection to potential destruction, with virtually no room for companies to wiggle out of the responsibility of disclosing inconvenient or unappealing portions of their practices. Additionally, it forces companies to make sure consumers know there is a redress mechanism in the event of abuse, and where to find it. The final disclosure is "[a] notice that the consumer's deidentified genetic or phenotypic information may be shared with or disclosed to third parties for research purposes . . ."[132] This solves one of the more pervasive issues in company self-enforcement, which is the tendency to withhold any warning about the distribution of de-identified data on the grounds that consent is not required for said distribution.[133] Overall, the disclosure requirement forces companies' hands in terms of revealing the less convenient truths about what they do with genetic information, while at the same time ensuring that these revelations come in a form that is easy for consumers to understand.

The next action the Act forces direct-to-consumer genetic testing companies to perform as a safeguard for consumers is to obtain "express consent for collection, use, and disclosure of the consumer's genetic data . . ."[134] At a minimum it requires "separate and express" consent for a list of five individual data handling practices.[135] Briefly summarized, these include:

[126] *Id*. at § 56.181(a).
[127] *Id*. at § 56.181(a)(1).
[128] *Id*. at § 56.181(a)(1)(A).
[129] Amodio, *supra* note 42, at 962.
[130] CAL. CIV. CODE § 56.181(a)(1)(B).
[131] *See* Amodio, *supra* note 42, at 953, 962.
[132] CAL CIV. CODE § 56.181(a)(1)(C).
[133] *See* Machin, *supra* note 8, at 241.
[134] CAL CIV. CODE § 56.181(a)(2).
[135] *Id*.

The use of the genetic data collected through the company's product or service;

The storage of the consumer's biological sample(s);

Every use of the genetic data or biological sample beyond the original product or service;

Every transfer or disclosure of the genetic data or biological sample to a third party, including the identity of that third party; and

The marketing or "facilitation of marketing" directed towards a consumer based on their genetic data on the part of the company, or the same actions based on their having sought and used a genetic test on the part of a third party.[136]

Like the disclosure requirement related to the potential life cycle of genetic data, these provisions of the Act require consent at basically every major point of data use or movement. This solves the problem of one blanket (potentially flawed) consent contract being used by companies as justification for essentially doing whatever they want with a user's genetic data, regardless of whether the user might find it objectionable. Under the Act, consumers will be able to evaluate and decide whether they agree with each use or transfer of their sensitive genetic information.[137]

It should be noted there are some exceptions to point E above. A company is not required to seek express consent to market to the consumer on their own website or app based on their demonstrated interest in the product; however, this marketing cannot rely on the contents of the consumer's actual genetic information.[138] If express consent is obtained for a third-party to advertise to the consumer, these ads must be clearly marked and there must be a disclaimer that the claims of the ad have not been vetted and the ad itself is not endorsed by the direct-to-consumer genetic testing company.[139] There is also a further exception in which the use of "third party" in this context does not include post-secondary educational institutions which plan to or are using the genetic data or biological samples for research or educational purposes.[140]

The next section requires that direct-to-consumer genetic testing companies also provide effective mechanisms for the consumer to revoke their consent and specifies that there must not be unnecessary steps in this process.[141] This gives consumers even more ownership over how their genetic data is used because it provides a certain amount of flexibility to their decision-making. This revocation must be honored "as soon as practicable," with an absolute cap of thirty days

[136] CAL CIV. CODE § 56.181(a)(2)(A)-(a)(2)(E).

[137] *Id*. at § 56.181(a)(2).

[138] *Id*. at § 56.181(a)(2)(E).

[139] *Id*. at § 56.181(a)(2)(E)(iii).

[140] *Id*. at § 56.181(a)(2)(F).

[141] CAL. CIV. CODE § 56.181(b).

after it is given.[142] If this revocation is regarding the storage of the biological sample, the company has thirty days to destroy it.[143]

After this, the Act requires that the company "[i]mplement and maintain reasonable security procedures and practices to protect a consumer's genetic data against unauthorized access, destruction, use, modification, or disclosure."[144] It also requires that the company develop procedures and practices that allow the consumer to easily access their genetic data, delete both their account and their genetic data, and have their biological sample destroyed.[145]

The Act preemptively addresses the potential for discrimination based on the consumer's choice to exercise any of the rights listed in the Act.[146] This includes a prohibition on denying goods, services, or benefits to the consumer; charging different prices for goods or services; providing a different quality or level of goods or services; or suggesting that any of the above will occur.[147] It also prohibits considering the exercise of any of the consumer's rights under the Act as grounds for suspecting them of anything unlawful.[148] This last provision seems drafted to address the social fallout of a recent trend in law enforcement, wherein officers use the data from direct-to-consumer genetic tests as evidence in investigating or trying criminal conduct.[149]

The Act then steps somewhat into the shoes of GINA by prohibiting disclosure of a consumer's genetic data to a number of insurance entities, including health insurance, life insurance, long-term care insurance, and disability insurance.[150] This solves a significant problem present in GINA—that protection only extends to health insurance and leaves consumers vulnerable to discrimination from other entities in the field.[151] The Act also prohibits disclosure to employers, or any entity that provides advice to an insurance or employment organization.[152] This conforms to the mandate set forth by GINA, but also skirts around the potential issue of listed entities still getting genetic information from third-parties. There are three exceptions to these prohibitions, but they essentially boil down to disclosure being permissible only if the party is in no way capable of making or effecting either insurance or employment decisions.[153]

[142] *Id*. at § 56.181(c).

[143] *Id*. at § 56.181(c)(2).

[144] *Id*. at § 56.181(d)(1).

[145] *Id*. at § 56.181(d)(2).

[146] *Id*. at § 56.181(e).

[147] *Id*. at § 56.181(e)(1)-(4).

[148] *Id*. at § 56.181(e)(5).

[149] *See* Rafil Kroll-Zaidi, *Your DNA Test Could Send a Relative to Jail*, THE NEW YORK TIMES (Dec. 27, 2021) https://www.nytimes.com/2021/12/27/magazine/dna-test-crime-identification-genome.html [https://perma.cc/KU39-UFS6].

[150] CAL. CIV. CODE § 56.181(f).

[151] *See* Amodio, *supra* note 42, at 939-940.

[152] CAL. CIV. CODE § 56.181(f)(1).

[153] *See id*. at § 56.181(f)(2).

The one downside to the Act is that in terms of remedies, the consequences of disclosure are fairly light. The penalties are all monetary, and the highest they can go is $10,000 plus any court costs determined by the judge.[154] However, each violation is a separate and actionable offense, so multiple failures with even a single set of genetic data could be potentially costly.[155]

Overall, GIPA is a comprehensive law that addresses and remedies many of the deficiencies in existing methods of regulation. In particular, it expands on GINA and the existing privacy practices of direct-to-consumer genetic testing companies, while affording the consumer greater agency over their genetic information than any common law or federal equivalent. However, before trying to shape the helpful aspects of GIPA into a model framework for our proposed federal law, it would be helpful to look to other state laws to see if there are provisions we can scavenge.

B. Other applicable State laws: comprehensive data privacy legislation

First off, while not specifically targeted at genetic data privacy, it could be beneficial to look through the five states that have enacted comprehensive data privacy laws similar to the GDPR to see if there is anything that GIPA missed.

The first of the five is Colorado, which passed its Colorado Privacy Act ("CPA") on July 7, 2021.[156] Enforcement of the CPA began in July of 2023.[157] Rather than requiring express consent, as in GIPA, the CPA functions on a universal opt-out system that provides consumers with the right to opt out of targeted advertising, the sale of personal data, and some types of profiling based on that data.[158] Like GIPA, consumers have the right to request the destruction of their personal data, although the time period permitted for companies to avoid doing so is longer under the CPA at forty-five days.[159] The CPA also requires that before engaging in processing that presents a heightened risk of harm, organizations controlling data must "conduct and document data protection assessments." This essentially amounts to weighing the possibility of harm to the consumer against benefits to the organization itself, the consumer, other stakeholders, and the public at large.[160] The ideas of a universal opt-out option and a risk analysis requirement seem like potentially transferable and beneficial concepts for our model.

---

[154] CAL. CIV. CODE § 56.182 (b).

[155] *Id*. at § 56.182 (f).

[156] *Colorado Privacy Act Resource Center*, HUSCHBLACKWELL, https://www.huschblackwell.com/industries_services/colorado-privacy-act#:~:text=The%20Colorado%20Privacy%20Act%20provides,for%20targeted%20advertising%20and%20sales [https://perma.cc/NAX3-TGL5].

[157] *Colorado Privacy Act (CPA) Rulemaking*, COLORADO ATTORNEY GENERAL, https://coag.gov/resources/colorado-privacy-act/ [https://perma.cc/QK49-UELJ].

[158] Colorado Privacy Act Resource Center, *supra* note 156.

[159] *Id*.

[160] *Id*.

The next state is Connecticut, which is in a similar position to Colorado in that it passed the Connecticut Data Privacy Act ("CDPA") on May 10, 2022, and also went into effect in July of 2023.[161] Like Colorado, there is a universal opt-out option as well as individual opt-outs for the sale, processing for targeted advertising, and profiling of personal data.[162] Consumers are also afforded the right to delete data, and controllers are obligated to provide notice about what type of data is being collected, its uses, and consumer's rights in relation to it.[163] Additionally, there is a data protection assessment provision in situations of heightened risk.[164] As with Colorado, the universal opt-out and risk assessment seem like beneficial takeaways for our purposes.

Utah enacted its Utah Consumer Privacy Act ("UCPA") on March 24, 2022, and went into effect on December 31, 2023.[165] It is similar in most respects to the two preceding laws, including opt-out provisions, the right to confirm whether a company is in possession of data, the right to avoid discrimination for exercising rights, and the right to delete data.[166] It also mandates the distribution to consumers of a "reasonably accessible and clear privacy notice," and disclosure of any sale of information to a third party.[167] There is nothing particularly new here, just reinforcement of the right to delete and the notice requirements found in GIPA.

The fourth state is Virginia, which enacted the Virginia Consumer Data Protection Act ("VCDPA") on March 2, 2021.[168] The VCDPA went into effect on January 1, 2023.[169] Virginia appears to be the model for the preceding three states, which closely resemble it.[170] Because it is the model for much of the other three laws, there is not much that stands out here. However, the language regarding the data protection assessment seems to mandate that individual assessments

[161] *The Connecticut Data Privacy Act*, CT.GOV: THE OFFICE OF THE ATTORNEY GENERAL WILLIAM TONG, https://portal.ct.gov/AG/Sections/Privacy/The-Connecticut-Data-Privacy-Act#:~:text=When%20Does%20the%20Act%20take,controllers%20that%20process%20personal%20data [https://perma.cc/NT4J-RSDE].

[162] *Id*.

[163] *Id*.

[164] *Id*.

[165] *Utah Consumer Privacy Act*, SULLIVAN & CROMWELL LLP (Apr. 27, 2022), https://www.sullcrom.com/SullivanCromwell/_Assets/PDFs/Memos/sc-publication-utah-becomes-fourth-us-state-to-enact-comprehensive-privacy-law.pdf [https://perma.cc/44TF-A5JE].

[166] *Id*.

[167] *Id*.

[168] *Virginia Consumer Data Protection Act (VCDPA) Amendments and Clarifications*, BLOOMBERG LAW (May 3, 2023), (https://pro.bloomberglaw.com/brief/virginia-consumer-data-protection-act-vcdpa-amendments-and-clarifications/) [https://perma.cc/949U-BMDX].

[169] *Virginia Consumer Data Protection Act (VCDPA)*, BLOOMBERG LAW (Dec. 8, 2022), (https://pro.bloomberglaw.com/brief/virginia-consumer-data-protection-act-vcdpa/#:~:text=CCPAVCDPAAmbiguities-,What) [https://perma.cc/6KXT-CKDP].

[170] *Id*.

be conducted for each of the three types of data usage: targeted advertising, sale, and profiling.[171] This required assessment of each action taken is an appealing one, and something to keep in mind for our model.

The final state is California, which enacted the California Consumer Privacy Act in 2018, well before any other states began enacting similar laws.[172] Again, this Act is not much different. However, there is a right to limit use of personal information that seems promising, in that consumers can direct businesses to only use sensitive personal information for specific purposes, thereby maintaining the ability to choose who they want their data shared with, without cutting it off entirely.[173]

Overall, though certainly less stringent than the type of law we are attempting to create here, there are some valuable pieces of drafting legislation that can be carved from these comprehensive data privacy laws for our purposes.

C. Other applicable State laws: genetic data privacy laws

As other states' genetic data privacy laws are obviously more analogous to our own GIPA-based model, we should analyze a selection to look for helpful tips.

Arizona is a notable example, as it signed its Genetic Information Privacy Act into law on April 20, 2021.[174] Similar to GIPA in many ways, part of the disclosure requirement is a basic description of the security program in place to protect genetic data, a description of how long the company will retain that data, and a description of the method that will be used to destroy the data at the end of the retention period.[175] The remedy can also include actual damages suffered by consumers, rather than simply a financial penalty per infraction.[176] These could serve as helpful additions to our model.

Another example is Florida, whose Protecting DNA Privacy Act went into effect on October 1, 2021.[177] The most significant difference here from other examples of state genetic privacy laws is that Florida enforces criminal, not civil,

---

[171] VA. CODE § 59.1-577 (2023).

[172] *California Consumer Privacy Act (CCPA)*, STATE OF CAL. DEP'T OF JUST.: OFF. OF ATT'Y GEN., https://oag.ca.gov/privacy/ccpa#:~:text=This%20landmark%20law%20secures%20new,them%20(with%20some%20exceptions)%3B [https://perma.cc/AC3Z-RFJ7] (last updated May 10, 2023).

[173] *Id*.

[174] Wangari Thuo, *Arizona: Genetic Testing Law Enters into Effect*, ONETRUST DATAGUIDANCE (Sept. 2021), https://www.dataguidance.com/opinion/arizona-genetic-testing-law-enters-effect [perma.cc/9UTW-P9DK].

[175] *Id*.

[176] *Id*.

[177] Fay Shaulson, *How Florida is Protecting the DNA Privacy Rights You Didn't Know Need Protection*, U. MIA. L. REV. (Nov. 28, 2021), https://lawreview.law.miami.edu/florida-protecting-dna-privacy-rights-didnt-protection/ [https://perma.cc/E6HU-FGSP].

penalties for violations of the Act.[178] In fact, under Florida's Act, unlawful use of an individual's DNA is a potential felony, meaning there is the possibility of jail time for violations of genetic data privacy.[179] This might be the case because the law is not targeted specifically at direct-to-consumer genetic testing companies, but rather anyone who provides testing or otherwise produces genetic data (meaning individual physicians as well).[180] Although the classification as a felony may seem a little out of proportion to individual violations, and also difficult to enforce given the inevitable question of whom in a testing company should be held responsible, the idea of imposing criminal liability might be a more powerful deterrent than what currently exists in GIPA.

Utah is our final example; its Genetic Information Privacy Act (also known as "GIPA") went into effect May of 2021.[181] It reads as a pared down version of California's GIPA, with less extensive guidance on disclosures, and fewer required consents.[182] However, unlike those of the previous two states, this Act specifically targets direct-to-consumer genetic testing companies and, like California's GIPA, it offers its own expanded take on GINA.[183] While similar in many respects to the privacy laws of other states, it is a strong indicator of the importance of expanding GINA within the model.

Overall, because the states seem to be somewhat following one another's lead on this front, there is not a huge amount of variation in genetic data privacy laws. However, there are a few helpful pieces to be gleaned, as well as some confirmation of what portions of the legislation states find important.

D. Bringing it together: our final federal model

Now that we have gathered our base legislative model as well as additional relevant provisions, we can bring it all together into our hypothetical federal statute. We should start with GIPA's specific application to direct-to-consumer genetic testing companies, and their definition of those companies as entities that:

(A) offer consumer-initiated genetic testing services directly to the public;

(B) analyze consumer genetic data (with the exception of medical professionals for diagnostic/treatment purposes); and

(C) collect, use, maintain, or disclose consumer genetic data from a direct-to-consumer testing service.

This ensures that there are no loopholes that genetic testing companies can employ to avoid applicability of the statute to their business model, and keeps the purpose of the statute succinct and easy to interpret in future civil proceedings.

[178] *Id.*

[179] *Id.*

[180] *Id.*

[181] McKeon, *supra* note 58.

[182] *See* UTAH CODE § 13-60-104 (2023).

[183] McKeon, *supra* note 58; UTAH CODE § 13-60-105 (2023).

In addition, our statute should carry over the package of safeguards for the "privacy, confidentiality, security, and integrity"[184] of customers' genetic data. This would include the mandated list of disclosures from the company, including:

(A) a plainly written summary of privacy practices, including collection, use, maintenance, and disclosure of genetic data;

(B) a privacy notice that includes a baseline amount of information about the company's data collection, consent, use, access, disclosure, transfer security, retention, and deletion practices as well as how to file a complaint; and

(C) notice of potential disclosure to third parties of de-identified data.

This ensures that consumers are fully aware of all potentially necessary information to protect themselves and evaluate whether they are willing to put their genetic information in the hands of specific companies based on what they state they will do with it.

Next, we come to the consent portion of the statute. One option is to go with GIPA's five individual consents, which would be thorough and demonstrably protective. However, due to the ongoing nature of some of these consents (notably transfer and use beyond the original service), obtaining them may at times be prohibitively difficult or costly to the company. Therefore, this is a good area to look to the guidance of other states to determine if there is an easier way to provide a similar level of protection to the consumer. By synthesizing Colorado and Connecticut's universal opt-out with consumers' right to direct use of data for specific purposes in California, we arrive at a workable solution. Rather than having to obtain express consent for all five data handling practices, companies would only need to seek a one-time consent for the use of the genetic data collected through the company's service. This leaves four remaining practices:

(A) the storage of biological samples;

(B) any additional uses of the sample beyond the original service;

(C) every transfer of genetic data or biological sample to a third party; and

(D) any marketing directed towards the consumer based on their genetic data.

For these, consumers would automatically be opted out with the ability to choose to opt-in on any of the four. Thereafter, they would have the option to opt-in and -out at their discretion and would be informed in that choice by the disclosures noted above, as well as information on the specific third parties the company plans to distribute their data to. In effect, each data handling practice would have one consent, but that consent could be turned off and on by the consumer whenever they wished. By handing control of consent over to the consumer (presumably via companies' online portals for ease of access) the burden is removed from the company while still allowing a fully informed individual to decide what uses their data may be put to.

We then come to the section mandating that companies provide effective mechanisms for consumers to revoke their consent for the use of their genetic data, which is the foundational consent for all others in the statute. The

[184] CAL. CIV. CODE § 56.181(a).

mechanism itself should probably be up to the company to determine, but GIPA's 30-day limit on enacting the revocation is reasonable. In addition, it should include the destruction of any stored biological samples if the consumer has previously consented to allow this storage.

Like GIPA, the statute should also require the company to "[i]mplement and maintain reasonable security procedures and practices to protect a consumer's genetic data against unauthorized access, destruction, use, modification, or disclosure."[185] This is where Colorado, Connecticut, and Virginia's risk analysis requirements come in. In addition to security measures, companies should conduct data protection assessments weighing potential harm to consumers and the public against potential benefit when a particular use of data presents a heightened risk of injury. They should only be permitted to go forward with this higher risk use if the benefits significantly outweigh the costs.

The final set of requirements based on GIPA should be aimed at preventing discrimination against the consumer based on genetic data produced through the companies' services. The first will be a prohibition on discrimination based on the consumer's choice to exercise their rights pursuant to the statute, including a prohibition on:

(A) denying goods, services, or benefits to the consumer;

(B) providing differing qualities of goods and services;

(C) suggesting A or B will occur; and

(D) using the consumer's choice to exercise their rights under the statute as a basis for suspecting them of violating the law.

The statute will also include GIPA's GINA-like prohibition on providing genetic data to certain entities, including:

(A) health insurance;

(B) life insurance;

(C) long-term care insurance;

(D) disability insurance;

(E) employers; and

(F) providers of advice or counseling to any of the above entities.

These provisions will prevent retaliation against consumers looking to protect themselves, while also ensuring that their genetic data cannot be used to discriminate against them in a health or employment context.

The final component to consider is the remedy available to individuals under the statute. Here, GIPA may not provide the best example, as its flat monetary penalty per infraction cannot adjust to differing levels of harm. We will turn instead to Arizona's decision to use actual damages, which provides a more discretionary measure that can adjust up or down depending on how bad the harm to the consumer was. This provides a method of redress that is fairer to both consumers and the companies themselves.

What we are left with after constructing our model statute is a comprehensive and targeted protection against the potential misuse of genetic data by direct-to-

[185] *Id*. at § 56.181(d)(1).

consumer testing companies. It sets a base level of disclosure required to provide genetic testing to the public, a system of consents and opt-outs that prevent companies from taking advantage of the uninformed, and security guidelines ensuring appropriate protections are in place. It also steps into the shoes of federal laws like HIPAA and GINA to fill the gaps in preventing distribution of data to potentially discriminatory third parties.

CONCLUSION

As the direct-to-consumer genetic testing industry continues to flourish, we will have to square more decisively with the potential concerns it represents.[186] Our genetic data is some of the most sensitive health information we have, and it is therefore imperative that lawmakers take steps to keep it safe.[187] The current collection of law and policy available is insufficient for this purpose.[188] We must therefore turn to the states to provide us with a model of how we can comprehensively and specifically protect against this emerging threat to our privacy by adopting pieces of their genetic data privacy statutes. Our GIPA-based model serves as a starting point for federal legislators to craft their own statute, one that will provide at least a minimum level of protection to all in a manner that fills the gaps left by the laws that came before it. Hopefully, as we move forward, we can balance access to our own genetic data, the ability to provide access to that data to researchers if we so choose, and the ability of these companies to operate in an ethical manner.

[186] *See* Mladucky et al., *supra* note 2, at 200.

[187] *See* Gilligan, *supra* note 1, at 210.

[188] *See id*. at 227.

NOTE

THE SUBSTAN-DARD SIMILARITY TEST: THE SUBSTANTIAL SIMILARITY TEST APPLIED TO MUSICAL WORKS AND SOUND RECORDINGS

*Benjamin Silvers**

CONTENTS

* J.D. 2024, Boston University School of Law; B.S. in Music, Northeastern University, 2021. Thank you to Professor Jessica Silbey for her never ending guidance on this Note and beyond; to Professor Rebekah Moore for introducing me to the world of research, scholarship, and academia; to Joanna Allison and Sofya Nadgorny for their mentorship and advocacy; to the editors of Boston University's Journal of Science and Technology Law for their hard work getting this Note into shape; and to Matt, Chris, Kris, Hannah, Kaela, and Alex for their continuous support.

INTRODUCTION

Johann Helgason, despite having composed "Söknuður," the best-selling Icelandic song ever, has not gained critical acclaim in the worldwide music industry.[1] According to Helgason, his 1977 melody entered the canon of power ballads everywhere through the voice of Josh Groban.[2] In 2001, Rolf Lovland's band Secret Garden recorded a song titled "You Raise Me Up," of which Josh Groban recorded a version a couple of years later.[3] Helgason sued Lovland for copyright infringement, claiming that "You Raise Me Up" copied the melody of "Söknuður."[4] Using the extrinsic/intrinsic test, the Ninth Circuit held that "You Raise Me Up" and "Söknuður" are not substantially similar works, and therefore Lovland did not infringe Helgason's copyright.[5]

Johannsongs-Publishing Ltd. v. Lovland is only one case amidst a surge of high-profile copyright cases in the past few years.[6] Although the Second and Ninth Circuits hear most of the country's copyright cases, they apply different tests to determine whether a party has infringed another's copyright.[7] Furthermore, the other Federal Circuit Courts of Appeals are divided—some aligning themselves with the Second or Ninth Circuit and others applying an entirely distinct test.[8] Given the recent surge of copyright cases and the Courts of Appeals' circuit split regarding which test to apply when deciding issues of substantial similarity, copyright litigants and lawyers are facing a greater quantity of

[1] *Helgason*, DISCOGS, https://www.discogs.com/artist/1117410-J%C3%B3hann-Helgason?filter_anv=1&anv=Helgason [https://perma.cc/QT73-TKW6].

[2] Johannsongs-Publishing Ltd. v. Lovland, No. 20-55759, 2021 WL 5564626, at *1 (9th Cir. Nov. 29, 2022), *cert. denied*, 142 S. Ct. 2650 (2022) (mem.).

[3] *Id.*

[4] *Id.*

[5] *Id.*

[6] Rachel Hall, *'Music Is So Different Now': Copyright Laws Need to Change, Says Legal Expert*, THE GUARDIAN (Mar. 13, 2022), https://www.theguardian.com/music/2022/mar/13/music-is-so-different-now-copyright-laws-need-to-change-says-legal-expert [https://perma.cc/PQ83-VU6E]; *see, e.g.*, Gray v. Hudson, 28 F.4th 87 (9th Cir. 2022); Williams v. Gaye, 895 F.3d 1106 (9th Cir. 2018); Copeland v. Bieber, No. 2:13cv246, 2016 WL 11784720 (E.D. Va. Nov. 14, 2016).

[7] Daryl Lim, *Saving Substantial Similarity*, 73 FLA. L. REV. 591, 601, 603 (2021) (citing Skidmore v. Led Zeppelin, where the Ninth Circuit clarified relationship between inverse ratio rule and substantial similarity, and Arnstein v. Porter, establishing roots for ordinary observer test).

[8] *Id.* at 602-03 ("Courts employ three main tests or some combination thereof: the ordinary observer test, the extrinsic/extrinsic test, and the abstraction/filtration/comparison test. Most either adopt the Second Circuit's ordinary observer test or the Ninth Circuit's extrinsic/intrinsic test.").

disputes with a greater diversity of outcomes.[9] Furthermore, courts struggle to apply the substantial similarity tests to music because of music's distinguishable features: deep emotional connection to sounds, Western music's predisposition to use a limited number of chord progressions, pervasive industry-wide subconscious copying, and widely varied ways of hearing and interpreting music.[10]

The Supreme Court could have clarified the substantial similarity test in *Johannsongs* but instead denied the Plaintiff's petition for writ of certiorari.[11] So, the question remains: Which substantial similarity test is best for judging copyright infringement of musical works and sound recordings, and whose interests are best served by unifying the different tests across circuits? Copyright scholars have debated these normative questions at length,[12] but I propose in this note that the Supreme Court or Congress should consider the effects of a unified substantial similarity test upon four distinct interests. This Note will weigh the prevailing substantial similarity tests, as well as a few original tests or additions proposed by other scholarly articles, against the following interests: (1) the court's interest in creating a standard rather than a rule, thereby allowing judges to make decisions based on each case's individual facts; (2) litigants' interest in predictability; (3) the public's interest in the wide dissemination of music; and (4) the public's interest in minimizing the disparate impacts that copyright infringement claims have on marginalized musicians, specifically Black musicians. The Supreme Court or Congress should use this discrete list of interests to guide its approach to unifying substantial similarity analyses for musical work and sound recording copyright infringement cases among the Federal Circuits. Ultimately, this Note argues that the "ordinary observer" test, combined with a consideration of a musician's creative process and an analysis of the composition or recording itself, would best address these interests in light of the current state of copyright law and the music industry.

I. BACKGROUND

A. Constitutional underpinnings of copyright law

Congress receives the power to promulgate intellectual property laws, such as copyright and patent laws, from Article 1, Section 8, Clause 8 of the United

[9] Daryl Lim, *Substantial Similarity's Silent Death*, 48 PEPP. L. REV. 713, 735 (2021); Clark D. Asay, *An Empirical Study of Copyright's Substantial Similarity Test*, 13 U.C. IRVINE L. REV. 35, 81 (2022) (finding the substantial similarity test's application among different courts to be "characterized by significant heterogeneity").

[10] Liesl Alyse Eschbach, *Do You Hear What I Hear?: The Inequities in Substantial Similarity Tests for Musical Copyright Infringement Cases*, 11 BERKELEY J. ENT. & SPORTS L. 71, 92-93 (2022).

[11] Johannsongs-Publishing Ltd. v. Peermusic Ltd., 142 S. Ct. 2650 (2022).

[12] Lim, *supra* note 7, at 623.

States Constitution.[13] Although the original text of the Constitution grants this power in order to "promote the Progress of Science and useful Arts," intellectual property is widely viewed as protecting creators—such as inventors and artists—or contributing to economic growth, rather than bolstering society's compendium of knowledge.[14] Some copyright scholars have suggested that intellectual property actually stifles "progress," if within its conception of "progress," the Constitution considers the promotion of fundamental values like equality, privacy, and distributive justice.[15] The music copyright litigation that pervades today's legal landscape might seem far removed from these fundamental justifications for intellectual property. Properly calibrated, however, the standard for discerning the infringement of musical works and sound recordings may, in fact, incentivize musicians to produce more works, thereby promoting the progress of music. Congress's most recent comprehensive approach to protecting creative works is the Copyright Act of 1976, which provides copyright owners a cause of action against "[a]nyone who violates any of the exclusive rights of the copyright owner."[16] Absent from the Copyright Act's text, however, is guidance on determining when someone has violated an exclusive right. The result of this ambiguity is a body of judge-made law that guides copyright infringement analysis.

B. Copyright protection of musical works & sound recordings

Music copyright has two categories: musical works and sound recordings.[17] A musical work is "music (melody, rhythm, and/or harmony expressed in a system of musical notation) and accompanying words (lyrics)" whereas a sound recording is a "fixation of a series of sounds (e.g., a particular performance)."[18] Musical work owners have the exclusive right to (1) reproduce their work, (2) prepare derivative works based upon their work, (3) distribute their work to the public, (4) perform their work publicly, and (5) display their work publicly.[19] Sound recording owners have the exclusive right to (1) reproduce their work, (2) prepare derivative works based upon their work, (3) distribute their work to the public, and (4) perform their work publicly by means of digital audio

[13] "To promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and Discoveries." U.S. CONST. art. I, § 8, cl. 8.

[14] *See* Simone A. Rose, *The Supreme Court and Patents: Moving Toward a Postmodern Vision of "Progress"?*, 23 FORDHAM INTELL. PROP., MEDIA & ENT. L.J. 1197, 1215-16 (2013).

[15] *See* JESSICA SILBEY, AGAINST PROGRESS: INTELLECTUAL PROPERTY AND FUNDAMENTAL VALUES IN THE INTERNET AGE, 21-24 (2022).

[16] Copyright Act of 1976, 17 U.S.C. § 501(a).

[17] *See* U.S. COPYRIGHT OFF., CIRCULAR 56A, COPYRIGHT REGISTRATION OF MUSICAL COMPOSITIONS AND SOUND RECORDINGS (2021).

[18] *Id.*

[19] 17 U.S.C. § 106.

transmission.[20] A famous example of how these copyrights are distinct is Whitney Houston's sound recording of Dolly Parton's musical work "I Will Always Love You."[21] There, as the songwriter, Dolly Parton owns the underlying musical work copyright, whereas Whitney Houston's record label owns the sound recording copyright of Houston's specific performance of the song.[22] United States copyright law long predates sound recording technology, so in order to understand the current system of copyright protection, an overview of copyright law's evolution is helpful.

The Copyright Act of 1790 afforded no protection for musical works or sound recordings, only including maps, charts, and books within its scope.[23] Musical works first became protected in the Copyright Act of 1831, which included a series of formalities necessary to effectively protect a work under copyright, such as depositing "a printed copy of the title of such . . . musical composition . . . in the clerk's office of the district court of the district wherein the author . . . shall reside."[24] The Copyright Act of 1909 added significant protections for musical works, including the exclusive rights to publicly perform a composition for profit and "make any arrangement or setting" of the musical work, as well as introducing a compulsory mechanical license, which allowed non-authors to make use of the copyrighted work by creating "mechanical reproductions" – copies of musical works played by and recorded by people other than the author.[25] Finally, the Copyright Act of 1976 included sound recordings among its list of protected subject matter.[26] The sound recording right under the 1976 Act is limited, in that public performances of sound recordings are only protected if performed "by means of a digital audio transmission," and that sound-alike recordings are not infringements of the sound recording copyright, even if they "imitate or simulate those in the copyrighted sound recording."[27] The advent and increased accessibility of sound recording technology prompted the inclusion of

[20] *Id*.

[21] WHITNEY HOUSTON, I WILL ALWAYS LOVE YOU (Arista 1992); DOLLY PARTON, I WILL ALWAYS LOVE YOU (RCA Studio B 1974).

[22] WHITNEY HOUSTON, I WILL ALWAYS LOVE YOU (Arista 1992); Until recently, standard practice in the music industry has been an exchange between a record label and a recording artist in which the record label provides the recording artist an advance (recoupable by the label against the artist's royalties) in exchange for the recording artist assigning their sound recording copyright to the label, usually for the entire copyright term. AWAL, *Why Owning Your Master Recordings Means Everything* (Sept. 19, 2018), https://www.awal.com/blog/maintaining-ownership-rights-as-an-artist/ [https://perma.cc/ZK2H-235T].

[23] Copyright Act of 1790, Pub. L. No. 1-15, 1 Stat. 124.

[24] Copyright Act of 1831, ch. 16, 4 Stat. 436, 437.

[25] Copyright Act of 1909, Pub. L. No. 60-349, 35 Stat. 1075, 1075-76.

[26] 17 U.S.C. § 102(a) (1976). Along with this addition, the Act removed the formalities required under the 1831 Act, only requiring a work to be "original" and "fixed in any tangible medium of expression" to acquire protection.

[27] 17 U.S.C. § 106(6) (2002); 17 U.S.C. § 114(b) (2020).

sound recordings in the Copyright Act, but it took nearly 120 years from the first sound recording device's creation for U.S. copyright law to recognize sound recordings among copyrightable subject matter.[28] If it took this long for copyright law to respond to sound recording technology, one can imagine the difficulty the law would experience once copyrighted works began being copied and distributed via the Internet.

The music industry adapted to the complex structure of music copyright and the various rights it protects by introducing entities that streamline the licensing process for both musical works and sound recordings. Although section 115 of the Copyright Act provides a process for obtaining mechanical licenses from musical work owners, the Harry Fox Agency emerged in 1927 as a mechanical rights management company which contracts with music publishers to administer mechanical licenses to users of musical works and collect mechanical royalties on behalf of publishers and songwriters.[29] In 2018, Congress passed the Music Modernization Act, which offers blanket mechanical licenses to online streaming services and collects mechanical royalties on publishers' and songwriters' behalf.[30] Performance rights organizations, such as BMI and ASCAP, emerged in the early twentieth century to administer performance licenses on behalf of songwriters and publishers.[31] In 2003, SoundExchange was formed to administer compulsory licenses for the digital performance of sound recordings.[32] Although these entities created methods for obtaining licenses from musical work and sound recording owners, music copyright litigation persists.[33] These licensing entities cover some, but not all, of a music copyright owner's exclusive rights. For example, none of these entities administers licenses for the section 106(2) right to "prepare derivative works based upon the copyrighted work," meaning derivative work licenses must be negotiated directly with the owner of the musical work or sound recording.[34] This complex licensing scheme, combined with a general lack of public understanding of what

[28] *See* Talk of the Nation, *1860 'Phonautograph' Is Earliest Known Recording*, NPR (Apr. 4, 2008, 10:00 AM), https://www.npr.org/templates/story/story.php?storyId=89380697 [https://perma.cc/G6ZQ-CNSL].

[29] *History of HFA*, HARRY FOX AGENCY, https://www.harryfox.com/history [https://perma.cc/CWE4-568S].

[30] Orrin G. Hatch–Bob Goodlatte Music Modernization Act, Pub. L. No. 115-264, 132 Stat. 3676 (2018); *see About the MLC*, MECHANICAL LICENSING COLLECTIVE, https://www.themlc.com/our-story [https://perma.cc/4MA5-VXJG].

[31] *About Us*, AMERICAN SOCIETY OF COMPOSERS, AUTHORS, AND PUBLISHERS, https://www.ascap.com/about-us [https://perma.cc/2EK3-6593]; *About*, BROADCAST MUSIC, INC., https://www.bmi.com/about [https://perma.cc/8QVL-LL49].

[32] *Who We Are*, SOUNDEXCHANGE, https://www.soundexchange.com/who-we-are/#about-us [https://perma.cc/93SE-ZYSL].

[33] *See* Asay, *supra* note 9, at 53 (finding 6,368 cases available on Westlaw discussing substantial similarity in copyright infringement matters between 1978 and 2020).

[34] 17 U.S.C. § 106(2).

constitutes copyright infringement, might help to explain the persistence of music copyright infringement litigation.

C. Substantial similarity

When a plaintiff brings a copyright infringement action against a defendant, one of the analyses that the court can undertake is the "substantial similarity" test to determine whether the defendant's alleged copying amounts to misappropriation.[35] Although the "substantial similarity" test is not part of any copyright statute, it has been a common law feature of copyright law for nearly 100 years.[36] After determining that the plaintiff did, in fact, copy the defendant's work, the court asks whether the copying that took place amounted to misappropriation– in other words, whether the plaintiff's work is substantially similar to the defendant's.[37] How courts apply this test, however, varies depending on the circuit in which copyright litigants bring their case.[38] Although copyright protection extends to works in categories as disparate as literary works, musical works, motion pictures, and even pantomimes, each circuit applies its own "substantial similarity" test to all copyrightable works regardless of their artistic form.[39]

Applying the "substantial similarity" test specifically to music, when it was devised for creative works more broadly, presents a host of issues.[40] Western music is generally confined to the use of twelve musical notes, and the arrangement of these notes is usually dictated by a limited set of chord progressions.[41] Given the limited number of notes and chords, it is likely that one song will sound similar to another, even when the songs' artists had never heard the other's work.[42] Furthermore, the "substantial similarity" test's emphasis on the lay-observer means that similarity is to be judged from the perspective of a non-

[35] Arnstein v. Porter, 154 F.2d 464, 468 (2d. Cir. 1946) (applying the "ordinary observer" substantial similarity test to determine whether misappropriation had occurred); Steinberg v. Columbia Pictures Indus., Inc., 663 F. Supp. 706, 711 (S.D.N.Y. 1987) ("[T]he sole issue . . . is whether there is such substantial similarity between the copyrighted and accused works as to establish a violation of plaintiff's copyright."); *see* Nichols v. Universal Pictures Corp., 45 F.2d 119, 121 (2d. Cir. 1930) ("[T]he right cannot be limited literally to the text, else a plagiarist would escape by immaterial variations . . . the questions is whether the part so taken is substantial.").

[36] *See Nichols*, 45 F.2d at 121 (citing Marks v. Leo Feist, Inc., 290 F. 959, 960 (2d. Cir. 1923)).

[37] *Arnstein*, 154 F.2d at 468.

[38] *Id*. (defining the Second Circuit's test: "[T]he test is the response of the ordinary lay hearer."); Sid & Marty Krofft Television Prods., Inc. v. McDonald's Corp., 562 F.2d 1157, 1165 (9th Cir. 1977) (defining the Ninth Circuit's test: "We analyze this distinction in terms both of the elements involved—idea and expression—and of the tests to be used—extrinsic and intrinsic—in an effort to clarify the issues involved.").

[39] Eschbach, *supra* note 10, at 92.

[40] *Id*.

[41] *Id*.

[42] *Id*. at 93.

musician who is less likely to perceive significant differences between two musical works or sound recordings.[43] The current "substantial similarity" regime does not appropriately account for the unique aspects of musical works and sound recordings; thus, the Supreme Court or Congress should consider those aspects when unifying the "substantial similarity" test.

II. ANALYSIS

Given copyright law's lack of a uniform "substantial similarity" test, I will propose certain interests that the Supreme Court or Congress should consider when adopting such a test. I will also analyze the Second, Ninth, and Sixth Circuits' approaches to the "substantial similarity" test, as well as some innovative approaches to "substantial similarity" proposed by copyright scholarship.

A. Interests to consider

1. Court's interest in creating a standard rather than a rule

A uniform "substantial similarity" test promulgated by the Supreme Court or Congress would most obviously affect lower courts, guiding judges in their analysis of copyright infringement cases. When creating a uniform test, however, it is within the Supreme Court's or Congress's purview to create a rule-like test or a standard-like test. Louis Kaplow's explanation of rules and standards in an economic context is helpful to understand how a rule or standard might affect lower courts that implement such a test.[44] A rule-like test will determine the legality of an action before that action takes place whereas a standard-like test will determine the legality of an action after that action takes place.[45] For example, a speed limit is a rule because drivers know exactly what driving speed conforms to that law.[46] On the other hand, a regulation that required drivers to drive at a "reasonable" speed would be a standard.[47] Generally, actions that happen often and uniformly (e.g., driving at a speed greater than the speed limit) are conducive to being regulated by rules, and actions that happen less frequently and are more nuanced (e.g., intentional torts or negligence) are better regulated by standards.[48]

Although both Kaplow and Nachbar view the incentives for creating either rules or standards to concern individual litigants, in the copyright context, courts tasked with deciding infringement lawsuits with complicated facts may prefer to work with a standard rather than a rule. Having a standard-like test would allow

[43] *Id*.

[44] Louis Kaplow, *Rules Versus Standards: An Economic Analysis*, 42 DUKE L.J. 557, 559-62 (1992).

[45] *See id*.; Thomas B. Nachbar, *Rules and Standards in Copyright*, 52 HOUS. L. REV. 583, 594 (2014).

[46] Nachbar, *supra* note 45, at 594.

[47] *Id*.

[48] Nachbar, *supra* note 45, at 595.

courts to make individualized judgments based on the nuanced facts of a particular copyright case.[49] A standard-like test might also partially alleviate the difficulty that courts currently have in applying the "substantial similarity" test to copyright cases involving music.[50] Of course, it may be suggested that the overburdened court may have an interest in an easy-to-apply rule-like test and would not take on the extra burden of applying a standard-like test, given that the cost of implementing standards is higher than that of rules.[51] Working under the assumption that courts prioritize justice over ease of decision-making, however, this Note's analysis considers a standard-like "substantial similarity" test preferable to a rule-like test for purposes of analyzing the court's interest.

2. Litigants' interest in predictability

Contrary to the court's interest in creating a flexible standard, costs for copyright litigants and advocates, including the cost of hiring legal experts to understand the test, are lower if a uniform "substantial similarity" test is rule-like.[52] Many copyright scholars have offered suggestions detailing how the "substantial similarity" test could be more rule-like. One such suggestion, specific to the music context, is that courts "should adopt a precise definition of a musical idea, making uniform the application of the substantial similarity test in all music copyright actions."[53] Another suggests an injury-based test, in which substantial similarity "should be decided by asking whether the similarities are such as to result in substantial harm to the plaintiff," thereby increasing the predictability of litigation outcomes by grounding the misappropriation aspect of substantial similarity in a discrete list of harms: "economic harm, harm to reputation, loss of privacy, [or] loss of artistic control."[54]

3. Public's interest in dissemination of music

At the heart of United States copyright law is the proposition that protecting creative works through copyright incentivizes the production of new creative works. While some empirical studies support this proposition,[55] others argue that

[49] *Id*. at 594-95; *see* Kaplow, *supra* note 44, at 560-62.

[50] *See, e.g.,* Eschbach, *supra* note 10, at 92.

[51] *See* Kaplow, *supra* note 44, at 562-63.

[52] *See id*.

[53] Stephanie J. Jones, *Music Copyright in Theory and Practice: An Improved Approach for Determining Substantial Similarity*, 31 DUQ. L. REV. 277, 279 (1993).

[54] Laura G. Lape, *The Metaphysics of the Law: Bringing Substantial Similarity Down to Earth*, 98 DICK. L. REV. 181, 202 (1994).

[55] *See* Michela Giorcelli & Petra Moser, *Copyrights and Creativity: Evidence from Italian Operas*, 128 J. POL. ECON. 4163, 4166, 4206 (2020); Rahul Telang & Joel Waldfogel, *Piracy and New Product Creation: A Bollywood Story*, 43 INFO. ECON. & POL'Y 1, 10 (2018).

copyright law has endangered entire creative industries, such as the sampling-reliant genre of hip-hop.[56]

Despite the growing number of music copyright infringement cases, musicians continue to produce compositions and sound recordings, and music sales (both on subscription-based services and in physical formats) continue to rise.[57] As more music is created and more technologies arise that enable our listening to music, musical borrowing and influence have become more pervasive than ever before.[58] Given the constant growth in sales of musical works and sound recordings and the public's interest in the dissemination of music, it remains unclear whether the "substantial similarity" test needs to be made more protective of authors or not. But certainly, any revision to the "substantial similarity" test should consider that the scope of copyright protection affects follow-on musicians as well as legacy musicians. Because subconscious copying is no defense to copyright infringement,[59] a strict "substantial similarity" test has the potential to stifle musical creativity by incentivizing copyright owners to target musicians whose compositions are similar to their own and had access to their work. Instead, the Supreme Court or Congress could propose a "substantial similarity" test that promotes music dissemination by accounting for the vast exposure each individual has to music every day, which would strike a balance between protecting original work and enabling follow-on music to be produced.[60]

4. Public's interest in minimizing the disparate impacts that copyright infringement claims have on marginalized musicians, specifically Black musicians

Black musicians have influenced pop culture in enormous ways that have often not been recognized by the white music consumers who enjoyed the product of their influence.[61] Blues, jazz, rock and roll, rap, hip-hop, and pop music all

[56] KEMBREW MCLEOD & PETER DICOLA, CREATIVE LICENSE: THE LAW AND CULTURE OF DIGITAL SAMPLING, 204-09 (2011) (finding that acquiring licensees for the samples used on Public Enemy's FEAR OF A BLACK PLANET and Beastie Boys' PAUL'S BOUTIQUE would have resulted in a net loss of $6.8 million and $19.8 million, respectively).

[57] Joshua P. Friedlander & Matthew Bass, *Mid-Year 2022 RIAA Revenue Statistics*, RIAA (2022), https://www.riaa.com/wp-content/uploads/2022/09/Mid-Year-2022-RIAA-Music-Revenue-Report-1.pdf [https://perma.cc/2TW2-P2JT].

[58] J. Michael Keyes, *Musical Musings: The Case for Rethinking Music Copyright Protection*, 10 MICH. TELECOMM. & TECH. L. REV. 407, 425-26 (2004).

[59] Bright Tunes Music Corp. v. Harrisongs Music, Ltd., 420 F. Supp. 177, 180-81 (S.D.N.Y. 1976); Fred Fisher, Inc., v. Dillingham, 298 F. 145, 147-48 (S.D.N.Y. 1924).

[60] *See* Keyes, *supra* note 58, at 426 ("Music is disseminated through a vast reservoir of media. Because of this, music bombards individuals on a systemic and daily basis. The law should anticipate and expect that the responses to this incredible music infiltration will be varied and abundant and it should encourage such responses.").

[61] K.J. Greene, *Copyright, Culture & Black Music: A Legacy of Unequal Protection*, 21 HASTINGS COMMC'NS & ENT. L.J. 339, 364-67 (1998).

owe their origin to Black musicians.[62] Historically, the law has benefitted white musicians and devalued the work of Black musicians.[63] An early innovation in copyright law, the compulsory mechanical license, exacerbated this industry practice by allowing recording artists to record "cover" versions of songs without obtaining the permission of the songwriter.[64] The harm to Black musicians from mechanical licenses was concretely demonstrated in the 1950 watershed district court decision *Supreme Records, Inc. v. Decca Records, Inc.*, which held that any musical elements added by a performer during the recording process that were not "of a distinct kind" were not protected under copyright, and thus could be freely copied by others.[65] This holding was convenient for white recording artists, given that the white music industry had implemented a business model based on re-recording successful songs originally recorded by Black musicians.[66] These "mirror" recordings by white musicians sold much more because of segregated music charts and racism, depressing the value and exclusivity of the Black musicians' performances of the original musical work.[67]

Nowadays, copyright law impacts Black musicians even more directly by heavily disincentivizing (and in some circuits, completely prohibiting) digital sampling, a musical practice that is core to the hip-hop genre.[68] In *Grand Upright*, the Second Circuit compared music sampling to stealing by opening the opinion with the Biblical quote "Thou shalt not steal."[69] By doing so, the Second Circuit "effectively legitimized a hierarchy of cultural production in which digital sampling (within hip-hop specifically) is on the bottom."[70] The Sixth Circuit in *Bridgeport* held that the *de minimis* defense can never be applied to sampling a sound recording.[71] In doing so, the Sixth Circuit threatened copyright law's longstanding non-discrimination principle by effectively deciding which sort of

[62] *Id.* at 364.

[63] *Id.* at 365-67.

[64] 17 U.S.C. § 115 (2018).

[65] Supreme Records, Inc., v. Decca Records, Inc., 90 F. Supp. 904, 912-13 (S.D. Cal. 1950).

[66] Greene, *supra* note 61, at 373. Professor Greene refers to this industry practice as the "Bo Diddley pattern. Bo Diddley authored a number of hit tunes, but found that white performers 'covering' his work eliminated his opportunity to become a hit-maker himself." *Id.*

[67] Greene, *supra* note 61, at 367-371; Robert Brauneis, *Copyright, Music, and Race: The Case of Mirror Cover Recordings* 7-9 (Geo. Wash. Univ. L. Sch. Pub. L. Rsch. Paper, Paper No. 2020-56, 2020), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3591113.

[68] 17 U.S.C. § 114(b); *see* Grand Upright Music Ltd. v. Warner Bros. Recs., Inc., 780 F. Supp. 182, 183-85 (S.D.N.Y. 1991); Bridgeport Music, Inc. v. Dimension Films, 410 F.3d 792, 799-802 (6th Cir. 2005).

[69] *Grand Upright*, 780 F. Supp. at 183.

[70] Note, *Not in Court 'Cause I Stole a Beat: The Digital Music Sampling Debate's Discourse on Race and Culture, and the Need for Test Case Litigation*, 2012 U. ILL. J.L., TECH. & POL'Y 141, 152 (2012).

[71] *Bridgeport*, 410 F.3d at 801.

art is worthy of existence.[72] In *VMG Salsoul v. Ciccone*, the Ninth Circuit applied the *de minimis* doctrine to a sound recording sample and ruled in favor of the defendant.[73] The Ninth Circuit also determined that Congress intended to maintain the *de minimis* doctrine for sound recordings, contradicting the Sixth Circuit's interpretation of the Copyright Act.[74] Notably, the defendants who the court ruled against in *Grand Upright* and *Bridgeport* were Black rapper Biz Markie and Black hip-hop group N.W.A., respectively.[75] The defendant in *Salsoul* with whom the court sided was white popstar Madonna.[76]

A new "substantial similarity" test could help address these inequities by invalidating the circuit court decisions that have perpetuated them.[77] A test that explicitly allowed *de minimis* copying or provided a more nuanced approach to analyzing sound recording copying might erode or completely eliminate *Grand Upright* and *Bridgeport* and give lower courts another chance to interpret "substantial similarity" in a way that promotes and supports Black musicians.

There is a tension, however, between the strict application of copyright law in the "mirror recording" cases and those in the sound recording sampling cases. In the case of "mirror recordings," giving more rights to sound recording artists protects the interests of Black musicians, even if those rights only encompass small changes that a cover artist makes during recording.[78] On the other hand, in the cases of sound recording sampling, giving more rights to sound recording artists *harms* the interests of Black hip-hop musicians because even a *de minimis* taking of a prior work would be considered infringement.[79] An equitable "substantial similarity" test would creatively account for this dichotomy and balance the interests of protecting original recording artists with promoting the creation of musical works and sound recordings.

B. Different approaches to the "Substantial Similarity" test

1. Second Circuit's "Ordinary Observer" test

The Second Circuit introduced its "ordinary observer" or "average lay observer" test for determining substantial similarity in *Arnstein v. Porter*.[80] The court identified the central question as "whether defendant took from plaintiff's

[72] *See* Bleistein v. Donaldson Lithographing Co., 188 U.S. 239, 251 (1903) (reversing and remanding order by Sixth Circuit preventing recovery of copyright infringement by stating that "[i]t would be a dangerous undertaking for persons trained only to the law to constitute themselves final judges of the worth of pictorial illustrations").

[73] VMG Salsoul, LLC v. Ciccone, 824 F.3d 871 (9th Cir. 2016).

[74] *Id*. at 880-87; 17 U.S.C. § 114(b).

[75] *Grand Upright*, 780 F. Supp. at 183; *Bridgeport*, 410 F.3d. at 805.

[76] *Salsoul*, 824 F.3d. at 874.

[77] *See Grand Upright*, 780 F. Supp. at 183; *Bridgeport*, 410 F.3d. at 801.

[78] *See* Brauneis, *supra* note 67, at 20-27.

[79] *Bridgeport*, 410 F.3d. at 801.

[80] Arnstein v. Porter, 154 F.2d 464, 468 (2nd Cir. 1946).

works so much of what is pleasing to the ears of lay listeners, who comprise the audience for whom such popular music is composed, that defendant wrongfully appropriated something which belongs to the plaintiff."[81] Additionally, the *Arnstein* court offered its opinion regarding the unimportance of expert testimony in a substantial similarity analysis: "The impression made on the refined ears of musical experts or their views as to the musical excellence of plaintiff's or defendant's works are utterly immaterial on the issue of misappropriation."[82] The Fourth Circuit, in a case involving an African American spiritual, qualified the "ordinary observer" test by requiring district courts to "consider the nature of the intended audience of the plaintiff's work."[83] The Fourth Circuit clarified that "if the intended audience is more narrow in that it possesses specialized expertise, relevant to the purchasing decision, that lay people would lack, the court's inquiry should focus on whether a member of the intended audience would find the two works to be substantially similar."[84] The Second Circuit explained another addition to the "ordinary observer" test in *Boisson v. Banian, Ltd.* – the "more discerning" ordinary observer test.[85] When approaching substantial similarity analyses involving creative works that incorporate a lot of elements from the public domain, the "ordinary observer" must be "more discerning" in order to determine whether the protectible elements of the defendant's work are substantially similar to the protectible elements of the plaintiff's work while disregarding the unprotectible elements in both.[86]

The Second Circuit's "ordinary observer" test functions more as a standard than a rule.[87] Since the test hinges upon a jury's understanding of "wrongful appropriation," the legality of the defendant's use of the plaintiff's work is determined *after* the use takes place.[88] The classification of the "ordinary lay observer" test as a standard aligns with the common-sense understanding of which kinds of actions are better regulated by rules rather than standards – most instances of copyright infringement are unique and nuanced; thus, copyright infringement is better regulated by standards.[89] The Fourth Circuit's "intended audience" qualification and the Second Circuit's "more discerning observer" test attempt to restrict the broad discretion a jury has when determining issues of substantial similarity.[90] Overall, however, the Second Circuit's "ordinary observer" test promotes the court's interest in creating a standard for substantial similarity rather than a rule.

---

[81] *Id.* at 473.

[82] *Id.*

[83] Dawson v. Hinshaw Music, Inc., 905 F.2d 731, 736 (4th Cir. 1990).

[84] *Id.*

[85] Boisson v. Banian, Ltd., 273 F.3d 262, 272 (2d Cir. 2001).

[86] *Id.*

[87] *See* Kaplow, *supra* note 44, at 559-62.

[88] *See id.*; Nachbar, *supra* note 45, at 594.

[89] *See* Nachbar, *supra* note 45, at 595.

[90] *See Dawson*, 905 F.2d at 736; *see also Boisson*, 273 F.3d at 272.

The "ordinary observer" test frustrates litigants' interest in predictability because the "wrongful appropriation" standard is broad and minimally defined.[91] Additionally, because expert testimony is "utterly immaterial on the issue of misappropriation," litigants are less likely to predict outcomes by consulting with experts before litigation.[92] The "more discerning observer" variation of the Second Circuit's test decreases the likelihood of finding infringement by acknowledging when there is public domain material included.[93] The "ordinary observer" test's "wrongful appropriation" standard, prohibition of expert testimony, and "more discerning observer" variation all weigh against litigants' interest in predictability.

The "ordinary observer" test can be seen as protecting original work, which, if the economic incentive theory of copyright is to be believed, promotes the dissemination of more musical works and sound recordings.[94] It can also be seen as unfairly prohibiting the work of follow-on artists, like hip-hop artists who sample from previous works.[95] Without a working knowledge of different musical genres and what would be considered "wrongful appropriation" in each one, juries might be confused regarding how to apply the "ordinary observer" test to works in different genres.[96] It is unclear whether this confusion would lead to juries finding copyright infringement more often or less often; given this uncertainty, the "ordinary observer" test is likely neutral regarding the public's interest in the dissemination of music.

Given the Second Circuit's decision in *Grand Upright*, it is obvious that the "ordinary observer" test allows for the disparate impacts that copyright infringement claims have on marginalized musicians.[97] In fact, the same "wrongful appropriation" standard whose broadness gives juries the ability to consider customs from multiple genres also allows courts to impose their outdated racist views upon copyright infringement analyses.[98] The Fourth Circuit's "intended audience" consideration shows promise, in that maybe the "intended audience" of a follow-on artist's work could be considered different than the lay observer; however, the Fourth Circuit has explained that the "intended audience" consideration should be narrowly construed, given the detriments of introducing expert

[91] *See* Jones, *supra* note 53, at 287.

[92] *See id*. at 287, 289-290 (explaining that courts after Arnstein would either "lump[] the two tests together completely, or strictly bifurcat[e] them so that experts play[ed] no part in the layperson analysis").

[93] *See Boisson*, 273 F.3d at 272.

[94] *See* Giorcelli & Moser, *supra* note 55, at 4166; Telang & Waldfogel, *supra* note 55, at 18-19.

[95] *See* McLeod & DiCola, *supra* note 56, at 204-09.

[96] *See* Ani Khachatryan, *The Stairway to Fairness: Copyright and Creativity in the Digital Age*, 25 U. DEN. SPORTS & ENT. L.J. 23, 64-65 (2021).

[97] *Grand Upright*, 780 F. Supp. 182; *see Not in Court*, *supra* note 71, at 152.

[98] *See Not in Court*, *supra* note 71, at 152 (finding that the only authority cited in the entire *Grand Upright* decision was from the Bible, "Thou shalt not steal.").

testimony in substantial similarity analysis and the general difficulty of applying the test.[99] It is not likely that a court would determine that the intended audience of a hip-hop record possesses "specialized expertise," which the *Dawson* court identified as the threshold for abandoning the "ordinary lay observer" test.[100] Overall, the "ordinary observer" test does nothing to prevent the perpetuation of unfavorable copyright infringement outcomes for marginalized musicians and musicians that create within "follow-on" genres such as hip-hop and rap.

2. Ninth Circuit's "Extrinsic/Intrinsic" test

The Ninth Circuit introduced its "extrinsic/intrinsic" test in *Sid & Marty Krofft v. McDonald's*.[101] The Ninth Circuit bifurcated its test into analyses of (1) "specific criteria which can be listed and analyzed . . . [such as] the type of artwork involved, the materials used, the subject matter, and the setting for the subject" and (2) "the observations and impressions of the average reasonable reader and spectator."[102] Essentially, the first step of the test dissects the plaintiff's and defendant's works into protectible and unprotectible elements.[103] The second step of the test compares, from an "ordinary reasonable person's" perspective, the protectible elements of the two works.[104] Moreover, the Ninth Circuit specified that in the extrinsic part of the test, expert testimony is allowed; however, in the intrinsic part of the test, "analytic dissection and expert testimony are not appropriate."[105] Although the Ninth Circuit seemed confident in its introduction of a new substantial similarity test in *Krofft*, the Ninth Circuit itself, along with copyright scholars, has since acknowledged that the "extrinsic/intrinsic" test is difficult to apply across subject matter.[106]

---

[99] *Dawson*, 905 F.2d at 737 ("[I]n any given case, a court should be hesitant to find that the lay public does not fairly represent a work's intended audience. In our opinion, departure from the lay characterization is warranted only where the intended audience possesses 'specialized expertise.'").

[100] *Id.*

[101] Sid & Marty Krofft Television Prods., Inc. v. McDonald's Corp., 562 F.2d 1157, 1164-65 (9th Cir. 1977).

[102] *Id.* at 1164 (citing Twentieth Century-Fox Film Corp. v. Stonesifer, 140 F.2d 579, 582 (9th Cir. 1944)).

[103] *Id.*

[104] *Id.*

[105] *Id.*

[106] *See* Swirsky v. Carey, 376 F.3d 841, 848 (9th Cir. 2004) (noting that "the application of the extrinsic test . . . to musical compositions is a somewhat unnatural task, guided by relatively little precedent. Music is an art form that 'produces sounds and expresses moods,' . . . but it does not necessarily communicate separately identifiable ideas. The extrinsic test provides an awkward framework to apply to copyrighted works like music or art objects, which lack distinct elements of idea and expression.") (citing Debra Presti Brent, *The Successful Musical Copyright Infringement Suit: The Impossible Dream*, 7 U. MIAMI ENT. & SPORTS L. REV. 229, 244 (1990)).

Compared to the "ordinary observer" test, while the "extrinsic/intrinsic" test functions more like a rule, it is nonetheless a standard.[107] The extrinsic analysis, dividing the work at issue into protectible and unprotectible elements, involves "specific criteria which can be listed and analyzed," and expert testimony is appropriate during extrinsic analysis.[108] With enough precedent, the extrinsic analysis may evolve into a more rule-like test as more cases define these specific criteria.[109] As the Ninth Circuit observed about the intrinsic part of the test in *Krofft*, "[t]he determination of when there is substantial similarity between the forms of expression is necessarily more subtle and complex."[110] The Ninth Circuit adopted the "total concept and feel" standard to determine the intrinsic part of the test, which is likely just as broad as the Second Circuit's "wrongful appropriation" standard.[111] Overall, the "extrinsic/intrinsic" test functions as a standard, albeit to a slightly lesser degree than the "ordinary observer" test, promoting the court's interest in having a substantial similarity test that is a standard rather than a rule.

The "extrinsic/intrinsic" test allows for greater predictability of outcomes, but only within the extrinsic prong and only regarding certain subject matters.[112] For example, within the literary context, a court applying the extrinsic part of the test will compare "the individual features of the works to find specific similarities between the plot, theme, dialogue, mood, setting, pace, characters, and sequence of events."[113] However, in the music context, "there is no uniform set of factors to be used."[114] Potential copyright infringement litigants will likely struggle to predict their likelihood of success given the "extrinsic/intrinsic" test's ambiguities, and therefore the "extrinsic/intrinsic" test weighs against litigants' interest in predictability.[115]

Like the "ordinary observer" test, the "extrinsic/intrinsic" test functions to protect original work and therefore may promote the dissemination of more musical works and sound recordings.[116] However, some argue that, by deliberately

[107] *See* Kaplow, *supra* note 44, at 559-62.

[108] *Krofft*, 562 F.2d at 1164.

[109] *See* Nachbar, *supra* note 45, at 594 (discussing distinctions between legal rules and standards generally).

[110] *Krofft*, 562 F.2d at 1164.

[111] *Id*. at 1167.

[112] *See* Shaw v. Lindheim, 919 F.2d 1353, 1357-1358 (9th Cir. 1990).

[113] *Id*. at 1362 (quoting Berkic v. Crichton, 761 F.2d 1289, 1292 (9th Cir. 1985)).

[114] Goldberg v. Cameron, 787 F. Supp. 2d 1013, 1021 (N.D. Cal. 2011) (listing among the elements of a musical work its "idea, lyrics, rhythm, pitch, tempo, melody, harmony, structure, chord progressions, dissonance, and new technological sounds").

[115] *See* Jones, *supra* note 53, at 295-296 (discussing the likelihood of expert testimony confusing jurors and creating unpredictable outcomes in musical copyright suits).

[116] *See generally* Giorcelli & Moser, *supra* note 55, at 3 (discussing correlation between copyright law creation and increased number of Italian operas); Telang & Waldfogel, *supra* note 55, at 9-10 (discussing correlation between enforcement of Indian copyright law and increasing number of Bollywood movies).

separating the protectible/unprotectible analysis from the misappropriation analysis, the Ninth Circuit—unlike the Second Circuit—can find for the defendant on summary judgment and preempt long, unnecessary jury trials on the issue of misappropriation, again leading to the dissemination of more works.[117] One might expect that an increase in grants of motions for summary judgment would accompany a decrease in cases brought, given that litigants expecting a full jury trial would lose the incentive to bring a claim for copyright infringement. However, the Ninth Circuit hears the most copyright infringement cases of any circuit court.[118] Additionally, given the extrinsic part of the test's ambiguity when it comes to the elements of music that are to be compared, more music cases might pass through the extrinsic analysis and garner a full jury trial on the issue of misappropriation.[119] Overall, the "extrinsic/intrinsic" test is likely neutral regarding the public's interest in the dissemination of music.

The "extrinsic/intrinsic" test explicitly allows the court to determine, as a matter of law, which elements of a creative work are protectible under copyright and which are unprotectible.[120] Like the "intended audience" test, this feature of the "extrinsic/intrinsic" test has the potential to prevent unfavorable copyright infringement outcomes for marginalized musicians, for example, by determining that certain aspects of a hip-hop record, such as a short sound recording sample, are not protectible.[121] However, given its conception of the unprotectable elements of a work, the Ninth Circuit would be unlikely to consider an original sound recording sample unprotectable.[122] Overall, the Ninth Circuit's approach to substantial similarity analysis does not fare much better than the Second Circuit's regarding copyright infringement outcomes for marginalized musicians in "follow-on" genres.

3. Circuits that don't follow either approach

The Tenth Circuit uses the "abstraction/filtration/comparison" test for a wide range of cases.[123] The Tenth Circuit articulated the test:

[117] *See* Shaw, 919 F.2d at 1358-60 (discussing how parties must show triable issues of fact in extrinsic test to survive summary judgment motion).

[118] Asay, *supra* note 9, at 58.

[119] *Id.* at 95 (showing that experts are used more often in music cases than any other type of copyright infringement case).

[120] *Krofft*, 562 F.2d at 1165.

[121] *See id.*

[122] *See* Cavalier v. Random House, Inc., 297 F.3d 815, 822-23 (9th Cir. 2002) (finding the unprotectable elements of a work to be "primarily ideas and concepts, material in the public domain, and scènes à faire").

[123] *See* Country Kids 'N City Slicks, Inc. v. Sheen, 77 F.3d 1280, 1284-85 n.5 (10th Cir. 1996). The abstraction/filtration/comparison test was originally developed by the Second Circuit to determine whether one computer program infringes another. Comput. Assocs. Int'l, Inc. v. Altai, Inc., 982 F.2d 693, 706-11 (2d Cir. 1992).

At the abstraction step, we separate the ideas . . . which are not protectable, from the particular expression of the work. Then, we filter out the nonprotectable components of the product from the original expression. Finally, we compare the remaining protected elements to the allegedly copied work to determine if the two works are substantially similar.[124]

The Sixth and D.C. Circuits have adopted a similar test; however, they claim their test only has two steps: filtration and comparison.[125] In *Kohus*, the Sixth Circuit outlined which kinds of elements are filterable in the first part of the test: abstract ideas, elements dictated by efficiency, and *scènes à faire*.[126] Furthermore, the Sixth Circuit agreed with the Fourth Circuit's "intended audience" analysis and explained it would allow expert testimony in cases where the intended audience is not the lay public but rather an audience that possesses specialized expertise.[127]

Like the "ordinary observer" and "extrinsic/intrinsic" tests, the "abstraction/filtration/comparison" test functions more as a standard than a rule.[128] While adding yet another step to the substantial similarity test might seem to make it more formulaic, each component of the "abstraction/filtration/comparison" test is accompanied by its own ambiguity.[129] In the abstraction step, the court decides which types of expression present in the work are protectable.[130] Examples of unprotectable expression might be abstract ideas, elements dictated by efficiency, and *scènes à faire*; however, none of these categories presents a bright-line rule for protectability.[131] Once the court has decided which elements of the work are unprotectable, its decision regarding which elements to filter out of the analysis follows formulaically.[132] The comparison step of the test operates similarly to the "ordinary observer" test, in that the Tenth Circuit will consider "whether the accused work is so similar to the plaintiff's work that an ordinary reasonable person would conclude that the defendant unlawfully appropriated the plaintiff's protectible expression by taking material of substance and value."[133] Thus, the "abstraction/filtration/comparison" test as a whole promotes the court's interest in promulgating a standard rather than a rule.

---

[124] *Country Kids*, 77 F.3d at 1284-85.

[125] Kohus v. Mariol, 328 F.3d 848, 855-57 (6th Cir. 2003); Sturdza v. United Arab Emirates, 281 F.3d 1287, 1295-96 (D.C. Cir. 2002).

[126] *Kohus*, 328 F.3d at 855-56.

[127] *Id*. at 857.

[128] *See* Kaplow, *supra* note 44, at 559-62.

[129] *See Country Kids*, 77 F.3d at 1285 ("Because the idea/expression distinction is somewhat elusive, courts often adopt an ad hoc approach, eschewing the application of any bright line rule or any clear formula.").

[130] *Id*. at 1284-85.

[131] *Kohus*, 328 F.3d at 855-56.

[132] *Country Kids*, 77 F.3d at 1284-85.

[133] *Id*. at 1288 (citing Atari, Inc. v. N. Am. Philips Consumer Elec. Corp., 672 F.2d 607, 614 (7th Cir. 1982)).

By this point in the analysis, it is evident that there is an inverse relationship between the court's interest in creating a substantial similarity standard and litigants' interest in predictable litigation outcomes.[134] Further frustrating the prediction of litigation outcomes in the Tenth Circuit, the court has held that "not every case requires extensive analysis" and that "the appropriate test to be applied and the order in which its various components are to be applied . . . may vary depending upon the claims involved, the procedural posture of the suit, and the nature of the [works] at issue."[135] This holding suggests that the Tenth Circuit would consider applying an entirely different substantial similarity test, given a particular set of facts.[136] The ambiguity regarding which test to apply and how to apply said test stifles litigants' interest in predictability.

The "abstraction/filtration/comparison" test both protects original expression and gives judges broad discretion to permit copying that falls below the threshold of "wrongful appropriation."[137] Because the "abstraction/filtration/comparison" test was originally intended for use in computer software copyright cases, the application of the test to a music context might confuse jurors who are dealing with nebulous issues of fact such as "lyrics, rhythm, pitch, tempo, melody, harmony, structure, chord progressions, [and] dissonance."[138] However, whether this confusion might lead juries to find copyright infringement more or less often is unclear, and thus the "abstraction/filtration/comparison" test is likely neutral regarding the public's interest in the dissemination of music.

Given the Sixth Circuit's decision in *Bridgeport*, it is clear that even the existence of a precedential substantial similarity test does not prevent a court from applying a different test to a particular subject matter, in this case sound recordings.[139] Although part of the *Bridgeport* court's rationale for imposing a bright-line rule that prohibited bringing a *de minimis* defense against an allegation of sound recording copyright infringement was to promote judicial efficiency and general fairness, the decision actually "open[ed] the floodgates to more lawsuits."[140] Additionally, a strict "get a license or do not sample" rule increases the cost of samples because it makes the demand for sound recording licenses less economically elastic.[141] By implementing this "get a license or do not sample"

[134] *See* discussion *supra* Sections III.B.1, III.B.2.

[135] Jacobsen v. Deseret Book Co., 287 F.3d 936, 943 n.5 (10th Cir. 2002) (quoting Mitel, Inc. v. Iqtel, Inc., 124 F.3d 1366, 1372 (10th Cir. 1997) (internal citation omitted)).

[136] *Id*.

[137] *See Arnstein*, 154 F.2d at 473; *Country Kids*, 77 F.3d at 1288.

[138] *See Altai*, 982 F.2d at 706-11; *Goldberg*, 787 F. Supp. 2d at 1021.

[139] *Bridgeport*, 410 F.3d at 799-805.

[140] Jennifer R. R. Mueller, *All Mixed Up: Bridgeport Music v. Dimension Films and De Minimis Digital Sampling*, 81 IND. L.J. 435, 456 (2006).

[141] *Id*. (explaining that "a copyright is, *by definition*, a monopoly" and therefore market forces do not necessarily control the prices of music samples); *Bridgeport*, 410 F.3d at 801. In economics, the price elasticity of demand refers to "how responsive the quantity demanded is to a change in price." PRINCIPLES OF ECONOMICS § 5.1 (2011)

rule, the *Bridgeport* court essentially issued "a legally binding decree of what sort or art, and what sort of technology, society is willing to accept as valid."[142] Not only does this outcome conflict with copyright's long-standing "nondiscrimination" principle, it also opens the door even further for courts to consider their racist or otherwise discriminatory ideologies when deciding issues of copyright infringement under whichever substantial similarity test their circuit might apply.[143]

4. Suggested approaches from copyright literature

Copyright scholars have suggested many doctrinal, procedural, and institutional changes to the copyright system that they propose would significantly improve the outcome of copyright infringement cases.[144] In analyzing these changes against the interests described above, this Note will attempt to determine whether the changes could remedy the deficiencies of the existing substantial similarity tests.[145]

i. Using neutral expert testimony to educate jurors

Liesl Alyse Eschbach explains that many music copyright infringement cases turn into "battle[s] of the experts," in which both parties' musicologists argue about the "'correct' way to hear the songs at issue."[146] Eschbach's proposed solution is to appoint a neutral third-party expert musicologist who would explain to the jury basic musical concepts and answer the jury's questions about music before any evidence is presented.[147] Both parties would contribute money to hire the neutral expert, and the judge would select the neutral expert.[148]

Eschbach's neutral expert would affect litigants' interest in predictability and possibly the public's interest in minimizing disparate impacts of copyright litigation on marginalized communities.[149] The neutral expert would likely increase predictability for litigants in copyright infringement suits because it would provide the jury a uniform basis upon which to evaluate the plaintiff's and

[https://open.lib.umn.edu/principleseconomics/chapter/5-1-the-price-elasticity-of-demand/]. By requiring sound recording licenses in all instances, the *Bridgeport* court forces music users to buy a license, regardless of the price, incentivizing music owners to raise licensing fees unnecessarily.

[142] *Not In Court*, *supra* note 71, at 155.

[143] *Bleistein*, 188 U.S. at 251.

[144] *See* Eschbach, *supra* note 10; Lim, *supra* note 7; Patricia Rezac, *Take the © Train: Why a Musician's Creative Process Should Be Considered in Music Copyright Litigation*, 2021 B.C. INTELL. PROP. & TECH. F. 7-9; Khachatryan, *supra* note 97.

[145] *See supra* Section III.A.

[146] Eschbach, *supra* note 10, at 110.

[147] *Id*. at 111.

[148] *Id*.

[149] *See supra* Section III.A.2, 4.

defendant's experts' credibility.[150] Additionally, the jury's factual determinations would become more predictable with a neutral expert because most jurors do not begin a copyright infringement suit having a method of forming their own subjective opinion of the works in controversy.[151] A neutral expert would provide jurors with their own foundation upon which they could form their own opinions about the works before the plaintiff and defendant present their own experts.[152] However, using a neutral expert might introduce even more bias, given that a truly "neutral" party is unlikely to exist, and might contravene the adversarial system upon which the American court system relies. Eschbach acknowledges that "judges are likely to have as little musical training as jurors" and yet proposes that judges decide which neutral expert to select.[153] Although this approach might seem to present an objective method of educating jurors on musical issues, the selection of the neutral expert will likely be subject to the same biases that have historically created disparate impacts among marginalized musicians.[154] Additionally, the more experts that are required in copyright litigation, the higher litigant's costs will be – this increased cost could lead to not-well-funded litigants being unable to advocate on equal terms.

ii. Including a claim-like requirement in copyright registrations

Daryl Lim proposes a patent-like claim requirement in copyright registration.[155] Currently, copyright ownership exists without registration, and the only requirements for registration are an application, a fee, and a deposit of a copy of the work.[156] In this way, "neither plaintiffs nor defendants know the scope of the copyright for the work before a court's determination."[157] Lim's claim-like system would require copyright owners "to provide a simple description of what they claim to be copyrightable in the work" upon registering the work with the Copyright Office.[158]

Lim's claim-like requirement for copyright registrations would alter the substantial similarity test to function more as a rule than a standard, while also improving the predictability of copyright infringement outcomes.[159] Without a claim-like requirement, juries typically begin their substantial similarity analysis by distinguishing copyrightable expression from unprotectable material without

[150] Eschbach, *supra* note 10, at 114.

[151] *Id*. at 113.

[152] *Id*.

[153] *Id*. at 114.

[154] *See generally* Supreme Records, Inc. v. Decca Records, Inc., 90 F. Supp. 904 (S.D. Cal. 1950); Bridgeport Music, Inc. v. Dimension Films, 410 F.3d 792 (6th Cir. 2005); Grand Upright Music Ltd. v. Warner Bros. Recs., Inc., 780 F. Supp. 182 (S.D.N.Y. 1991).

[155] Lim, *supra* note 7, at 650.

[156] 17 U.S.C. §§ 102(a), 408(a)-(b).

[157] Lim, *supra* note 7, at 651.

[158] *Id*.

[159] *See supra* Section III.A.1-2.

reference to the text of the copyright application itself.[160] Lim's claim-like requirement, however, would help determine the scope of the work before litigation begins, making the impending substantial similarity test function more like a rule than a standard.[161] Lim argues that implementing a claim-like system for copyright registration would "clarify the claimed copyright scope of the work ahead of litigation," thereby helping courts more uniformly and predictably determine whether infringement occurred.[162] By including these claims in the publicly accessible Copyright Office database, the copyright registrant puts the public on notice of exactly what expressive elements they believe their copyright protects.[163] This notice not only bolsters the predictability of litigation outcomes but also serves to preempt infringement before it ever occurs.[164]

iii. Taking a genre-specific approach to substantial similarity in cases of music copyright infringement

Ani Khachatryan argues that "substantial similarity tests must be specific to the type of expression at issue," specifying that "[w]here the expression involves music, the most appropriate substantial similarity test requires a genre-specific approach."[165] Khachatryan points out that the *scènes à faire* doctrine itself, which describes elements of a work that are so customary to the genre that they do not garner copyright protection, requires a consideration of genre.[166] Additionally, a jurors' lack of familiarity with a specific music genre could impact their evaluation of an infringement claim.[167] Khachatryan proposes that courts should apply different tests to pop, rock, country, and R&B/hip-hop.[168]

Khachatryan's genre-specific approach to substantial similarity would likely decrease predictability for copyright infringement litigants and may also have a negative impact on marginalized musicians.[169] First, in order to apply a genre-specific substantial similarity test, someone would need to assign a genre to the works at issue.[170] Regardless of the genre-assigning entity, this assignment introduces an additional level of uncertainty and complication before the

[160] Lim, *supra* note 7, at 652.

[161] *Id*.; *see* Kaplow, *supra* note 44, at 559-62; Nachbar, *supra* note 45, at 594.

[162] Lim, *supra* note 7, at 652.

[163] *See id*. at 653.

[164] *See id*.

[165] Khachatryan, *supra* note 97, at 64.

[166] *Id*. at 64-65.

[167] *Id*. at 66.

[168] Khachatryan proposes using an extrinsic/intrinsic test for pop music, an extrinsic test for rock music, an extrinsic test for country music, and an abstraction/filtration/comparison test for R&B/hip-hop music. *Id*. at 67-79.

[169] *See supra* Sections III.A.2, III.A.4.

[170] *See generally* Khachatryan, *supra* note 97, at 64-65 (acknowledging that some genres are hard to evaluate).

substantial similarity analysis begins.[171] Additionally, using multiple variations of the substantial similarity test within each circuit for different genres of music would add even more unpredictability to copyright infringement suits, as each circuit would likely interpret each test in a different way.[172] Furthermore, the genre-specific approach to substantial similarity might exacerbate the inequities that marginalized musicians face by inappropriately categorizing all music produced by a certain group of people as one genre – for example, Khachatryan groups R&B and hip-hop in the same genre category and only explains why R&B belongs in that category, seemingly assuming that hip-hop follows the same patterns as R&B.[173]

iv. Considering a musician's creative process in copyright litigation

Patricia Rezac relies on the District Court for the Southern District of New York's opinion in *Tempo Music, Inc. v. Famous Music Corp.* and argues that it is important for courts to "examine the process by which a composer has created a piece of music" in copyright infringement cases.[174] The *Tempo* court noted that "[t]his emphasis on creative process rather than novel outcomes is consistent with the standard in other jurisdictions which emphasize creative inputs beyond mere technical changes any skilled musician could make."[175] Rezac argues that considering a musician's creative process partially obviates the need for experts to explain advanced technical musical concepts – rather, the jury can split its focus between technical components (such as the music theory contained in both parties' works) and non-technical ones (such as the creative process).[176]

Considering a musician's creative process in copyright litigation suits may increase predictability of copyright infringement outcomes as well as allow for greater dissemination of music.[177] Because "the general public often lacks a basic familiarity of musical terminology and compositional elements," attorneys must explain technical concepts to juries that might lead to more confusion than understanding.[178] If juries are allowed to consider a musician's creative process in copyright litigation suits, litigants may be more equipped to predict litigation outcomes – that is, litigants can rely on the predictability of the jury's non-technical analysis, rather than the relatively less predictable analysis of technical musical concepts.[179] Considering a musician's creative process might also lead to juries finding infringement less often and therefore allow more music to be

[171] *See id.*

[172] *See supra* Section II.C.

[173] Khachatryan, *supra* note 97, at 77-79.

[174] Rezac, *supra* note 145, at 6; Tempo Music, Inc. v. Famous Music Corp., 838 F. Supp. 162, 164 (S.D.N.Y. 1993).

[175] *Tempo*, 838 F. Supp at 169 n.11.

[176] Rezac, *supra* note 145, at 7-8.

[177] *See supra* Section III.A.2-3.

[178] Rezac, *supra* note 145, at 7.

[179] *See id.* at 6-7.

disseminated. Rezac explains three values of the use of creative process in a substantial similarity analysis: (1) courts will reach more well-informed decisions by "evaluating a musician's creative process as a non-technical criterion," (2) "examining a musician's creative process can lead to fair outcomes across genres," and (3) "a musician's creative process can also provide insight into copyright disputes among digital composers."[180] The second and third values tend to weigh in favor of the dissemination of music. First, musicians in some genres, like classical music, tend to have less compositional freedom; therefore, the standard for originality should be lower in those genres.[181] Second, a digital musician's process could reveal that their sounds are wholly original or that they used sounds produced by their software.[182] If the musician produced their own sounds, a jury would be more likely to find those sounds original.[183]

CONCLUSION

Given the interests discussed above, the Supreme Court or Congress should create a uniform substantial similarity test for musical works and sound records that combines the "ordinary observer" test with Patricia Rezac's addition of considering a musician's creative process during substantial similarity analysis.[184] The "ordinary observer" test promotes the court's interest in creating a standard rather than a rule, but it fails to increase predictability or minimize the disparate impact that copyright infringement claims have on marginalized musicians.[185] Rezac's suggestion partially remedies these failings by increasing predictability and promoting the dissemination of music to the public.[186] While neither the "ordinary observer" test nor the inclusion of a musician's creative process in substantial similarity analysis seem to influence the disparate impact that copyright infringement suits have on marginalized musicians, copyright law and the music industry itself seem to have "moved in the right direction" to address some of these concerns.[187] Musical works can now be fixed using a sound recording alone, the threshold for originality is now very low, and producers (or sound recording artists) are now encouraged to bargain for songwriting credit.[188] In this

[180] *Id*. at 7.

[181] *See id*. at 8-9.

[182] *Id*. at 9.

[183] *See id*.

[184] *See supra* Section III.B.1; Rezac, *supra* note 145, at 6-9.

[185] *See supra* Section III.B.1.

[186] *See supra* Section III.B.4.iii.

[187] Brauneis, *supra* note 67, at 27.

[188] *Id*. To continue "moving in the right direction," Brauneis suggests that (1) musical works contained within sound recordings should extend to aspects of the recording that cannot be, or would be hard to be, notated on a piece of sheet music; (2) the threshold for originality should not change – that is, it should remain low – for musical arrangements or derivative works; and (3) the music industry should implement infrastructure that educates "all

way, substantial similarity analysis has already been changed due to the realization that copyright law was not working equally well for everyone.[189]

When unifying the federal circuit courts' substantial similarity tests, the Supreme Court or Congress should consider the four interests discussed above, creating a test for musical works and sound recordings that balances (1) the court's interest in creating a standard rather than a rule, thereby allowing judges to make decisions based on each case's individual facts; (2) litigants' interest in predictability; (3) the public's interest in the wide dissemination of music; and (4) the public's interest in minimizing the disparate impacts that copyright infringement claims have on marginalized musicians, specifically Black musicians. Because the number of music copyright infringement suits has dramatically increased in recent years and applying copyright law to music is significantly different than applying copyright law to other subject matters, musical works and sound recordings require their own substantial similarity test that accomplishes copyright's goals while acknowledging the idiosyncratic issues that music presents to the courtroom.[190]

participants in the process of creating a sound recording" about bargaining for songwriting credit and/or royalties. *Id*.

[189] *See id*.

[190] *See* Hall, *supra* note 6; Eschbach, *supra* note 10.