OHIO STATE LAW JOURNAL

2018 – 2019

Editor in Chief
David Roper

Executive Editor
Maggie O'Shea

Chief Articles Editor
Madeline J. Rettig

Chief Note Editor
Aaron D. Rothey

Symposium Editor
Steven T. Darnell

Chief Online Editor
Alex A. Al-Doory

Managing Editors
Tyler G. Aust
Jordan Belcastro
Zachary P. Bowerman
Joseph M. Carrafello
Claudia Cash
Kathryn L. Caudill
Erica Duff
Timothy Gabel
Matthew D. Gutierrez
Sam Jones
Molly Komig
William J. Meadows
D. Anthony Merenda
Kenzie Nothnagel
Matthew R. Pettit
Ryan Steyer

Business Editor
Alexander J. Szaruga

Faculty Advisors
Deborah Jones Merritt
Anne E. Ralph
Christopher J. Walker

Events Editors
Jared Kriwinsky
Ethan W. Weber

Digital Editor
Sarah A. Rhodes

Online Editors
Gretchen Rutz
Rachel Stoneburger
Taylor R. Tremont

Note Editors
Caroline Eversman
Michael Rogers
Matthew W. Stevens

Managing Editors
Tyler G. Aust
Jordan Belcastro
Zachary P. Bowerman
Joseph M. Carrafello
Claudia Cash
Kathryn L. Caudill
Erica Duff
Timothy Gabel
Matthew D. Gutierrez
Sam Jones
Molly Komig
William J. Meadows
D. Anthony Merenda
Kenzie Nothnagel
Matthew R. Pettit
Ryan Steyer

Staff Editors
Matthew S. Hauer
Kelcie N. Hendren
Amanda G. Jones
Bethany Jones
Riley Kane
Rebecca E. Kanz
Adam C. Kennett
Kaela King
S. Matthew Krasnik
Julia Lauritzen
Zach Leciejewski
Samuel V. Lioi
Diane Long
Dustin M. Lorenzo
Zachary L. Marcum
Amanda C. Maxfield
Brandon J. McNeill
Spencer Meador
Tadd Minton
Donald B. Naiman
Hannah L. Nicholson
John Osinski
Evan Poole
Clairanne Porter

Benjamin J. Reeb
Alison Roth
Matthew Somogyi
Brittany Stevenson
Graeme S. T. Sua
Micaela Taylor
Katherine M. Toth
Jessica Van Ranken
Erica M. Van Heyde
Will White
Lindsey M. Woods

Published Six Times a Year by Students of The Ohio State University Moritz College of Law
OFFICERS OF ADMINISTRATION
Michael V. Drake, B.A., M.D., President of the University
Bruce A. McPherson, B.S., M.S., Ph.D., Executive Vice President and Provost of the University
Alan C. Michaels, A.B., J.D., Dean of the College and Edward M. Coxson Professor in Law

Daniel P. Tokajer, B.J.D., J.D., Assoc. Dean for Faculty, Charles W. Ebersold Ebersold Professor of Law, Senior Fellow of Election Law at Moritz
Kathy S. Northern, B.A., B.J.D., Assoc. Dean for Admissions, Director of Diversity and Inclusion, and Robert M. Duncan/Jones Day Designated Assoc. Prof. of Law
Paul Rose, B.A., J.D., Assoc. Dean for Academic Affairs, Robert J. Watkins/Procter & Gamble Professor of Law and Executive Director of Law, Finance and Governance Programs

Laura Fernandez, B.S., J.D., Assist. Dean for International and Graduate Affairs and Adjunct Prof.
Sara A. Sampson, B.S., M.S., J.D., Assist. Dean for Information Services, Director of Law Library, and Senior Lecturer
Darren Nealy, B.A., J.D., Assist. Dean for Academic Affairs and Adjunct Prof.
Michael States, B.A., J.D., Assist. Dean for Admissions & Financial Aid

FACULTY EMERITI
Mary Beth Beazley, B.A., J.D., Assoc. Prof. of Law
Michael Braunstein, B.A., J.D.
Sanford N. Caust-Elfenben, M.C.R.P., J.D.
Albert L. Clovis, B.A., M.A., LL.B.
Sharon L. Davies, B.A., J.D.
Gordon E. Gee
Laura Fernandez
John C. Elam/Vorys Sater Professor of Law

FACULTY
Anna Akbar, B.A., J.D., Assoc. Prof. of Law
Douglas A. Berman, A.B., J.D., Newton D. Baker-Baker & Hosteller Chair in Law
Michal Berman, B.A., J.D., Assoc. Prof. of Public Health and Law
Gregory A. Caldeira, B.A., A.M., Ph.D., Distinguished Univ. Prof., Ann and Darrell Dreher Chair in Pol. Commun. and Policy Thinking and Prof. of Law
Cinnamon P. Carlame, B.A., B.C.L., M.S., J.D., Alumnus Society Designated Professor of Law
Martha Chamallas, B.A., J.D., Robert Lyon Chair in Law
Bryan H. Chos, A.B., J.D., Assist. Prof. of Law and Engineering
Daniel C.K. Chou, B.A., J.D., Frank E. & Virginia H. Buzer Chair in Business Law
Hoppy Coat, B.A., J.D., Visiting Assist. Prof. of Law
Amy J. Cohen, B.A., J.D., John C. Elam/Vorys Sater Professor of Law
Sarah Rudolph Cole, B.A., J.D., John W. Bricker Professor of Law and Director of Program on Dispute Resolution
Ruth Colker, A.B., J.D., Distinguished Univ. Prof. and Grace Fern Heck Faust Chair in Constitutional Law
Owen Conway, B.A., J.D., Assist. Clinical Professor of Law
Elizabeth Igen Cooke, B.A., J.D., Clinical Professor of Law
Ellen E. Deison, B.A., M.S., J.D., Joanne W. Murphy/Classes of 1965 and 1973 Prof. of Law
Tern L. Erns, B.A., J.D., Clinical Prof. of Law, Senior Fellow of Election Law at Moritz
Katherine Hunt Federle, B.A., J.D., J.L.M., Joseph S. Platt-Porter Wright Morris & Arthur Professor of Law and Director of the Center for Interdisciplinary Law and Policy Studies
Edward B. Foley, B.A., J.D., Charles Ebersold & Florence Whitecomb Ebersold Chair in Constitutional Law and Director of Election Law at Moritz
William Froehlich, B.A., J.D., Langdon Fellow in Dispute Resolution
Larry T. Gauerin, B.A., B.S., M.S., J.D., Lavrentiev and Stanley Prof. of Law
Art Glogower, B.A., J.D., LL.M., Assoc. Prof. of Law
Arthur F. Greenbaum, B.A., J.D., James W. Shockeyness Prof. of Law
L. Camille Hébert, B.A., J.D., Carter C. Kessell Prof. of Law
Mohamed S. Helal, B.A., M.A., LL.B., LL.M., J.D., Assist. Prof. of Law
Dennis D. Hirsch, B.A., J.D., Prof. of Law, Director of Program on Data and Governance
Stephanie R. Hoffer, B.S., J.D., LL.M., Prof. of Law
Steven F. Huefner, A.B., J.D., C. William O'Neill Professor in Law and Judicial Administration, Senior Fellow of Election Law at Moritz and Director of Clinical Prof.
Cecelia Johnson, B.S., J.D., President's Club Prof. of Law
Kimberly Jordan, B.S., J.D., Clinical Prof. of Law and Director of Justice for Children Project
Katharine S. Kelly, B.A., J.D., Assoc. Clinical Prof. of Law and Director of Academic Support Program
Katherine J. Lee, B.A., J.D., Clinical Prof. of Law
Deborah Jones Merritt, A.B., J.D., John Deaver Drinko-Baker and Hosteller Chair in Law
Dale A. Osterlee, B.A., M.P.P., J.D., Gilbert Reese Chair in Contract Law
Efthimios Parasidis, B.A., M.B.E., J.D., Prof. of Law and Public Health
Anne Ralph, B.A., J.D., Clinical Prof. of Law
Courtney Roger-Jones, B.A., J.D., L.L.M., Assist. Prof. of Law
Guy A. Rub, B.A., LL.B., M.A., LL.M., J.D., Prof. of Law
Dakota Rudesill, B.A., J.D., Chief Justice Thomas J. Moyer Prof. for the Administration of Justice and the Rule of Law
Colleen Garrity Settineri, B.S., B.A., J.D., Assist. Clinical Professor of Law
Peter M. Shane, B.A., J.D., Jacob E. Davis & Jacob E. Davis II Chair in Law
Re Simmons, B.A., M.A., J.D., Chief Justice Thomas J. Moyer Prof. for the Administration of Justice and the Rule of Law
Marc S. Spindelblum, B.A., J.D., Isadore & Idie Togger Prof. of Law
Todd A. Stankor, B.A., M.B.A., J.D., Clinical Prof. of Law
David Stebenne, B.A., M.A., J.D., Prof. of History and Law
Joseph B. Stulberg, B.A., J.D., M.A., Ph.D., Michael E. Moritz Chair in Alternative Dispute Resolution
Christopher J. Walker, B.A., M.P.P., J.D., Assoc. Prof. of Law, Director of Washington D.C. Summer Program
Paige L. Wilson, B.A., J.D., Clinical Prof. of Law

ADJUNCT FACULTY
Karin Ali
Elizabeth L. Arstaeck
Stephen Anway
Susan Ayendy
David T. Ball
Jordan Berneman
Allison Binkley
Amy Bittner
Ben Bodnaruk
Joseph Boehmam
Edward Braum
Joseph M. Caliguri
Jeff Chilcoat
Ron C. Clay Cole Jr.
Daniel Conway
Matt Cooper
Lorenzo Cortez
Jonathan E. Coughlan
Nanette Dahman
Rick Daley
Scott E. Failer
Laura Fernandez
Benjamin Flowers
Tod Friedman
Cates Garrity-Rokous
Paul Gatz
Franz Geiger
Peter Glenn-Applegate
David W. Grauer
Gary Greenwald
Robb Henz
Hon. John E. Hoffman Jr.
Melissa Jackson
Daniel J. Kaye
Mary C. Kolman
James K.L. Lawrence
Sherry B. Lazear
George Limbert
Emma MacGaidwin
Hon. Allen L. Marley
Greg Mathews
Ingrid McCarthy
Hon. Stephen L. McIntosh
Richard M. Mascher
Robert J. Miller
Rebecca Monroe
Norman Nadoff
Ryan O’Rourke
Matt Palmer
Frank M. Placenti
Matt Richardson
Michael Robertson
Scott V. Sampson
Rob Solomon
Douglas Squares
Carter Stewart
Hon. Jeffrey S. Sutton
Austin Thompson
Kathryn Thompson
Hon. Chelsey M. Vascura
Hon. Michael H. Watson
Robert Weiler
Samantha Wuhrer
Geoff Wilcox

The Ohio State University Moritz College of Law
IN MEMORIAM

Dean James E. Meeks..................................................................................... 381

Articles

Toying with Privacy: Regulating the Internet of Toys
Eldar Haber ................................................................................................ 399

Freedom to Hack
Ido Kilovaty ................................................................................................. 455

Offshore Tax Enforcement and Divorce
Khrista McCarden ...................................................................................... 521

Notes

No Trespassing: A Lawmaker’s Guide to Protecting Property Rights in the Age of Augmented and Mixed Reality
Joseph Carrafiello ........................................................................................ 583

The Decontextualization of Music in Political Settings: An Argument for Moral Rights for Musical Works
Chance Johnson .......................................................................................... 619
IN MEMORIAM

Dean James E. Meeks................................................................. 381

Articles

Toying with Privacy: Regulating the Internet of Toys
  Eldar Haber .................................................................................. 399

Freedom to Hack
  Ido Kilovaty ............................................................................... 455

Offshore Tax Enforcement and Divorce
  Khrista McCarden ................................................................. 521

Notes

No Trespassing: A Lawmaker’s Guide to Protecting Property Rights in the Age of Augmented and Mixed Reality
  Joseph Carrafiello ..................................................................... 583

The Decontextualization of Music in Political Settings: An Argument for Moral Rights for Musical Works
  Chance Johnson ........................................................................ 619
In Memoriam
Dean James E. Meeks

TABLE OF CONTENTS
INTRODUCTION .....................................................................................381
PETER M. GERHART..............................................................................383
N. WILLIAM HINES ...............................................................................385

Introduction

This issue of the Ohio State Law Journal is dedicated to Dean James E. Meeks, who passed away on October 26, 2017.¹ This dedication is to honor his years of commitment to the Ohio State University. It is also to recognize his commitment to friends and family.

Dean Meeks was born on November 8, 1938. For his undergraduate degree, he attended Oberlin College. Dean Meeks graduated from Columbia Law School in 1963. During his time at Columbia, he served as an editor of the Columbia Law Review. After graduation, he clerked on the United States Court of Appeals for the District of Columbia Circuit for Judge Carl McGowan.

Dean Meeks began his teaching career at the University of Iowa Law School. From 1973 to 1976, he served as associate dean at Iowa. In 1978, he joined the Ohio State University College of Law. He served as dean until 1985 and returned to teaching.

In 1983, Dean Meeks was in a near-fatal automobile accident that left him in a coma for two weeks. He recovered with no memory of the accident. Dean Meeks used that experience to bring torts alive for his students. He also specialized in and taught antitrust law, legal writing, and public utilities. Dean Meeks was pivotal in establishing the Dispute Resolution Program and the Ohio State Law Journal on Dispute Resolution. After twenty-eight years of dedication to the law school, Dean Meeks retired in 2005.

Beyond the walls of Moritz, Dean Meeks also played a legal role throughout the Ohio State University. From 1988 to 1991, he served as a special assistant for legal affairs to the university president. In 1985, Dean Meeks helped investigate protocols of the university hospital. Ultimately, this investigation led to the prosecution of a physician guilty of committing homicides in hospitals around the world.

Dean Meeks was a staple of the Ohio State University community. Most importantly though, he was a family man married to the love of his life, Priscilla, for over forty-eight years. Dean Meeks is survived by his wife, two children,

¹ The Ohio State University Moritz College of Law Faculty, College Mourns Loss of Former Dean Meeks (Nov 7, 2017), https://moritzlaw.osu.edu/briefing-room/faculty/college-mourns-loss-of-former-dean-meeks/ [https://perma.cc/SK8H-YS6Z].
and many grandchildren. The In Memoria tributes that follow provide a glimpse of Dean Meeks as a mentor and cherished friend to so many.
The Measure of a Dean: A Tribute to Dean James E. Meeks

PETER M. GERHART *

Imagine the qualities that make a law school dean special. Then think of Dean James E. Meeks. The congruence is so great that the overlap between imagination and reality hardly leaves a shadow.

Law school deans ride the waves of fortune, buffeted by the whims of capricious state legislatures, a besieged central administration, an ambitious yet individualistic faculty, an eager but distracted alumni base, and a dream-filled student body. The law school dean faces this tempest alone, equipped with only the strength of character and the power of personal values that the dean brings to the task. James E. Meeks brought character and values aplenty to the Ohio State College of Law.

Jim arrived at the law school from the faculty of the University of Iowa (a birthplace of deans) in 1978, loaded with credentials and optimism. A graduate of Oberlin College and Columbia Law School, he had the perfect pedigree for the College of Law:

• Clerkship at the United States Court of Appeals for the District of Columbia (Judge McGowan).
• Successful teaching career at the University of Iowa.
• Author and authority on regulatory law and public policy.

Dean Meeks served as dean until 1985, six years of accomplishment and service. My sense is that he would have served even longer had an auto accident not robbed Jim of the fire that he knew was essential to doing the job at the level he wanted to sustain. That is because what Jim Meeks cared about the most was the well-being of the institution he led. He continually asked what sacrifices he could make for the institution, rather than what sacrifices the institution would make for him.

Dean Meeks cared deeply about the law school, the people who made it great, and the potential it had to make great people. He was not a person who wanted glory for his own sake; he wanted glory for the institution and its people. His ambition was great but it was a quiet ambition, radiating outward rather than inward, and radiating without fanfare or fluff. It was the ambition of substance, not form; the ambition of getting the job done well, rather than the ambition of appearing to have done the job well.

Jim knew that a successful dean builds the right culture among the faculty and staff, working to bring unity out of individuality and a common sense of shared destiny out of disparate faculty agendas. He and Priscilla hosted faculty

* The John Homer Kapp Professor of Law at the Case Western Reserve School of Law. Professor Gerhart served as Associate Dean under Dean Meeks at the Ohio State University from 1983 until Dean Meeks resigned as dean in 1985, and served as Interim Dean while Dean Meeks recuperated from an automobile accident in the 1983–84 school year.
parties in their home; Jim hosted faculty retreats at various state parks to build a stronger, more unified faculty; by inviting outside speakers, he sought to bring the spark of outside ideas to ignite the flames of faculty creativity.

He was a good listener, sympathetic and empathetic. He processed what he heard and was candid in stating his disagreement, while appreciating the advice he had been given. He cared about the well-being of his faculty and staff, and was sensitive to their interests, goals, and personal issues. He was never judgmental of the person, nor even of ideas that did not resonate with him. He accepted human foibles as an inevitable part of living together in a community.

Dean Meeks led with courage and conviction. He was not afraid of personal failure; his only fear was that the institution would not reach its potential. He found no task too daunting and no challenge too unpleasant. My fondest memory of Jim focuses on an early morning meeting when a small group of us gathered at 7:30 AM in his office to consider where to make university-mandated budget cuts. A thousand small cuts take their toll on an institution, but Jim faced the budget-cutting predicament with characteristic resolve and commitment, confident that he could make the required cuts without hitting any arteries. He listened patiently to the various suggestions of the assembled group and then acted decisively, avoiding either the self-pity that could accompany the resulting losses or the outward show of frustration that would dispirit the faculty. As always, it is courage under pressure that defines leadership. Few faculty fully understand the pressures a dean faces, the cross-current menu of choices to be made, or the time that robs a dean of that most rare resource: reflection. Through it all, Jim displayed confidence and optimism, trusting in his own leadership and never showing the disappointments that were an inevitable part of the job.

The impact on the law school was formidable. If you dusted for fingerprints at The Ohio State College of Law you would find those of Dean James E. Meeks wherever you looked, in the library, the legal clinic, in faculty offices, and in the classroom. The legacy of a law school dean is not in the institution’s outward garb but in the institution’s inner culture and spirit. That made Dean Meeks a very successful dean.
Jim Meeks, 1938–2017:
Remembering a Fifty-Year Friendship

N. WILLIAM HINES*

Most of the papers in this commemorative issue of the Ohio State Law Journal will focus on various aspects of Jim’s splendid academic career and his many professional accomplishments, and properly so. I intend to do something different. I want to tell you about Jim the person, his wonderful wife Priscilla for almost fifty years, his family, and some of the many fun things we did together during a friendship that stretched over half a century. There may be an excess of fishing stories in this tribute, but that is because Jim and I did a whole lot of fishing together.

James Edward Meeks was born in 1938 and he was raised in a loving, middle class household in central Ohio. His father, Voras (who understandably went by Jeff), was on the road a lot, selling school books and academic texts for Harcourt-Brace Publishing. His mother, Frankie, was a traditional stay-at-home mom who devoted all of her considerable energy to raising Jim and his two sisters, Betty and Nancy. Both Jim’s father and mother were well-educated parents who kept up with national events. They inspired Jim to become alert to what has happening around him and to become a voracious reader. They also encouraged his developing interest in the arts, including opera. Jim graduated from high school in Columbus in 1956, and attended Oberlin College where he played lacrosse, graduating in 1960. Jim was then accepted at Columbia University School of Law, where he established an outstanding academic record and served as an Editor of the Columbia Law Review. After graduating from

*Professor Emeritus and Dean Emeritus, University of Iowa College of Law.
Columbia in 1963, Jim passed the Ohio Bar Examination, and served as a Law Clerk to Judge Carl McGowan of the U. S. Court of Appeals for the D.C. Circuit during the 1963–1964 term of court. It was at this point in his career that Jim entered what would be a fifty-plus-year tenure as a law professor.

I first became aware of Jim’s existence in November of 1962 when his name came up as a teaching candidate in an Iowa law faculty meeting. I had only recently joined the Iowa faculty as an assistant professor the prior May, having been hired by Iowa’s legendary law dean, Mason Ladd. When I say Dean Ladd hired me, I am not using a euphemism; these were the days in law teaching when deans hand-picked their faculty members, subject to rubber-stamp approval after the fact by the tenured law faculty. The first time I met any member of the Iowa law faculty was when I showed up at the law school to start teaching my first summer school class.

Dean Ladd was in the habit of making annual pilgrimages east to what he regarded as the citadels of higher law learning (Yale, Harvard, and Columbia) to search for faculty talent. I was a graduate teaching fellow at Harvard when I was recruited by Dean Ladd in 1961; Jim Meeks was a senior law student at Columbia, editing the Columbia Law Review in 1962, when Dean Ladd came calling to offer him a teaching position at Iowa. Dean Ladd’s practice was to carefully select his favorite teaching candidates and then present them at a law faculty meeting for a vote of approval, reciting their credentials and explaining his reasons for selecting them. I vividly recall the faculty meeting when Dean Ladd recommended the appointment of Jim Meeks as an assistant professor. Things were going smoothly until I politely raised my hand to ask whether it was such a good idea to hire so young a candidate who was still in law school, regardless of how strong the dean thought his scholarly potential was. Shouldn’t we at least wait to see if he passed a bar exam somewhere? I was all of twenty-five years old at the time and had served less than six months on the faculty, but I was pretty sure of myself.

A senior colleague, Professor Sam Fahr, immediately spoke up to support the Dean’s recommendation. Sam said, “This young fellow Meeks looks impressive to me on paper, and the one thing about which we can be confident is that he will definitely grow older.” After the laughter subsided, Dean Ladd went on to explain that Jim had already accepted a prestigious federal clerkship with Judge Carl McGowan on the D.C. Circuit, so he would not enter law teaching until the fall of 1964. With this slight delay in Jim availability made clear, the faculty voted unanimously to approve the Dean’s recommendation, and Jim officially became an Iowan. Professor Fahr’s prediction was right; Jim did indeed grow older for the next fifty-three years. There is more than a little bit of irony in the fact that as the only person to raise a question about Jim’s appointment, we quickly became great friends once he was in Iowa City, a friendship that continued for the rest of Jim’s lifetime.
I. JIM’S TIME AS A PROFESSOR IN IOWA CITY

Jim enjoyed rapid success at Iowa, quickly climbing the rungs of the academic ladder to earn tenure and advancement to Full Professor. Jim was a popular teacher and colleague, and soon after arriving he began serving as faculty advisor to the Iowa Law Review. Although he regularly taught Torts, his early scholarly interests were in Anti-Trust law and Regulated Industries. As part of Iowa’s relatively radical curriculum reform in the late 1960s, Jim and I collaborated to create a new required first-year course that we both commenced teaching. We called the new course “Resource Planning.” This innovative course combined private arrangements affecting real property rights with public regulation of land use (think zoning), and also included emerging environmental law topics. We still teach this course at Iowa as an elective. Jim also teamed up with his law colleague Professor Dan Ellis, along with professors from engineering, geography, and business to create Iowa’s first interdisciplinary course in “Energy Law” in the early 1970s. After playing several leadership roles on the faculty, Jim served ably for two years as Associate Dean for Academic Affairs under my decanal predecessor, Dean Larry Blades.

Jim and his family left Iowa in 1978 when he was appointed the Dean at the Ohio State University College of Law. Jim’s colleagues, students, and friends at Ohio State know much more than I do about Jim’s contributions to Ohio State and his activities in Columbus. Because we were fellow deans throughout his Ohio State deanship, I know that he served with notable success as Dean for seven years. When he stepped down as Dean, he joined the faculty as a beloved teacher, mentor of students and colleagues, and a valued scholar in his specialty subjects. In recognition of his professional accomplishments, Jim was named the Joseph E. Davis Distinguished Professor. Besides teaching and writing, Jim provided important advisory services to the law school and to the university for a number of years, both officially and unofficially. Jim formally retired in 2006, but he continued to teach one or another of his specialty courses until his deteriorating health condition prevented him from continuing in the classroom.

In October of 2017, I was a guest at the 50th Reunion Dinner of the Iowa Law Class of 1967. The members of this class were the first Iowa students Jim taught, instructing them in Torts in the fall of 1964. I knew Jim considered the 1967 class his favorite Iowa class, so it was not surprising that Jim had many admirers and a number of close friends in the class. Several of them present at this reunion noted his absence to me and inquired about him. They were saddened to learn that the progress of Jim’s Parkinson’s disease made it impossible for him to travel to the reunion, much as he wished he could have attended it. As often happens at these reunion events, the 1967 class members began exchanging tales about their old professors. Jim’s name came up much
more than anyone else’s, and most of the recollections concerned some memorable thing Jim had said in class or some kind deed Jim had done to help an alum when he or she was a student or later in their professional careers. One class member recounted how Jim had generously tutored him in Advanced Anti-Trust law for a semester to prepare him to join the U.S. Justice Department’s Anti-Trust Division.

In a different vein, one 1967 class member reminded this classmates that law school in the 1960s was a high stakes venture that occasionally caused student resentments to run high. He specifically remembered rallying classmates to Jim’s defense in a dark parking lot after a Phi Delta Phi party, when Jim was about to be accosted by a drunken student who had flunked Jim’s Torts course. Those were the days when law schools admitted many more first-year students than they intended to graduate, and only two-thirds or less of the entering class ever completed law school. Our colleague, Professor Sam Fahr, who taught first-year Criminal Law, often boasted that he was the Admissions Director for the second year of the law school. At the end of these alumni reminiscences, we all raised a toast to the formative role Jim had played in so many Iowa grads’ lives and to his good health, none of us knowing Jim’s condition had become so dire and that he would pass away less than a month later.

II. Jim’s Personal Life in Iowa City

Let me share with you some recollections about my wife, Jean, and my time with Jim, Priscilla, and their family during the fourteen years Jim taught at Iowa and since. In those early years at Iowa, Jim spent a lot of time with me, Jean and our three girls, bonding as well with my parents and my three siblings, to the point where we soon regarded Jim as an honorary member of the Hines family. Jim’s close relationship with my family continued long after he moved to Columbus, mostly because of our fishing trips together, our joint travels, and our long-time connection to Star Island, our cherished summer paradise in northern Minnesota. In 1990, Jim and Priscilla joined members of my family and some of our college friends on a glorious two-week visit to Greece, enjoying an educational land tour followed by a fabulous cruise around the Greek Islands.
Early on, Jim also became well acquainted with what we called the Baker Eight. This close knit group was composed of Jean and me, and three other couples, Larry and Janie Wilson, Asheville, N.C., Tom and Kathy Keefe, Denver, and John and Shari Layle, Kansas City. All three other couples were Jean’s or my former college roommates at Baker University. They all married shortly after college and we have remained very close friends for nearly sixty years, often visiting each other around the country and travelling together on vacation trips. During their time in Iowa City, Jim and Priscilla became ex officio members of the Baker Eight, and renewed acquaintances with them every summer for over 40 years on Star Island in Cass Lake, Minnesota, where Jim and Priscilla have had a summer cottage since the 1980s. Three of the Baker Eight couples have long owned cabins on Star Island and the fourth visits regularly for weeks every summer.

Jim was a bachelor when he arrived in Iowa, which was rare on the Iowa faculty. Iowa City is the quintessential “college town” in “fly over” land, short on the amenities of larger metropolitan areas, but a safe place with great public schools; and an ideal place to raise children. Dean Ladd strongly preferred to recruit teaching prospects who had already formed their own families, believing they were much more likely to stay at the law school than bachelors. (I could say bachelorettes as well, but when Jim joined the Iowa faculty, it would be another ten years before Iowa hired its first female law teacher.)

Early in Jim’s time in Iowa City, Jean and I resolved that Jim needed to sink deeper roots in Iowa. To us this meant that Jim should find a satisfactory life partner, get married and start his own family, so we set out to become matchmakers. After a couple of false starts, including the younger sister of our next door neighbor, Jean met Miss Priscilla Lohr at a kindergarten roundup. Priscilla was a U. of I. elementary education grad from Churdan, Iowa. She was roughly Jim’s age, attractive, bright, sweet, and most importantly single and seemingly without a serious boyfriend in her life. Jean decided on the spot that Priscilla was a prime prospect to become Jim’s wife. Shortly thereafter, she introduced Jim to Priscilla and thankfully the two of them clicked immediately. Jim and Priscilla soon became a couple, joining with us and other young law faculty couples in various parties and adventures.

During Jim’s courtship of Priscilla, he lived for a year in Chicago where he taught as visiting professor at Northwestern Law School. (Later during his long career Jim also visited as a professor at the University of Virginia and at Boston University.) More than once that year, we travelled to Chicago to spend a weekend doing the town with Jim and Priscilla. Jim lived in a brand new luxury apartment located high in a apartment building overlooking Lake Michigan. Part of the attraction of visiting Jim in Chicago was just spending time in such a beautiful place gazing out over the lake. One of our most memorable outings with Jim and Priscilla in Chicago occurred when the four of us attended a dinner/theatre event at the Drake Hotel featuring the popular singer Peggy Lee. Every time I hear Ms. Lee’s fabulous recording of the song “Fever” on TV or
radio, I flash back to sitting in the dark in the Drake dining room watching her amazing performance of her signature number.

Jim and Priscilla’s engagement in 1968 was celebrated in Iowa City by a party in a private room at the University Athletic Club with four other young law faculty couples (Jean and I, Ron and Mary Carlson, Meade and Deborah Emory, and Gary and Gracie Goodpasture). You have no doubt heard the expression “drinking someone under the table.” At this engagement party, most of the attendees spent time under the table at one point or another. Eventually, the party became too rowdy and the management asked us to leave. Fortunately, there were no later repercussions because the fog of drink made the party an evening few, if any, of us could remember with much clarity the next day.

Another memorable outing during Jim and Priscilla’s engagement was a trip to Star Island on Cass Lake in North Central, Minnesota with our mutual friends, Ron and Mary Carlson. Officially, this trip was a further celebration of Jim and Priscilla’s engagement, but the unofficial purpose was to see how Priscilla stood up to the rustic simplicity of Star Island, to which Jim had already formed a firm bond. The challenge lay in the primitive nature of my parents’ North Woods cabin, with no running water, thus no hot shower, no indoor plumbing, only an outhouse, plus the cabin’s resident bats, mice, and its mildewed bedding. Priscilla ended up sleeping on a sun porch, perched on a stack of four ancient mattresses. She made no complaint, and unlike the Princess and the Pea, she claimed she slept in complete comfort. As was predictable from her small-town Iowa background, Priscilla passed the Star Island test with flying colors. Soon thereafter in the summer of 1969, she and Jim were married and started their own family. I served as Jim’s Best Man, and all three of our young daughters, then ages eight, six, and four, attended their first ever wedding courtesy of Jim and Priscilla. Our girls were so impressed it was all they could talk about for weeks before and after.

After three years of living in an Iowa City home a couple of blocks from us, in 1972, Jim and Priscilla settled into a new home in a rural residential subdivision five miles from town. The expansion of their family started with the birth of Kathy (1972) and then Jeff (1974). We saw less of them as child-raising consumed their time, but we still caught up with them regularly at law school events, Hawkeye sports competitions, and during annual summer vacations on Star Island. We also travelled in the same social circles related to the university. For example, we helped start a Gourmet Dinner Group in Iowa City with a number of young couples from other University Departments. The Gourmet Group met at a different couple’s home, and each member brought an assigned part of the planned ethnic meal, Italian, Spanish, Asian, Polynesian, or some other ethnicity. Jim did little cooking, but in recognition of his expertise with wines, he excelled as the wine sommelier for the group, selecting just the right wines to serve with every type of exotic meal. Occasionally, the alcohol flowed too freely, and the parties sometimes got a little wild for a group of staid professors, but everyone always made it home safely and all the marriages endured.
III. SUSTAINING OUR FRIENDSHIP AFTER MEEKS LEFT IOWA CITY

The Meeks family moved to Columbus in 1978 when Jim was appointed Ohio State Law Dean. Jean and I stayed in fairly close touch with the Meeks after they left Iowa City. I continued to see Jim regularly at ABA Deans Meetings and various AALS events. We always exchanged newsy Christmas cards, and we saw the Meeks family during their occasional visits back to Iowa, during our occasional visits to Columbus, and for the past twenty years every March we got together in Florida. In the late 1990s, Jim and Priscilla began renting a gulf-side condo unit for a month on Marco Island, Florida, where they entertained visiting family members and friends from Ohio and Minnesota. Coincidently, about the same time Jean and I started renting our own water-side place on Sanibel Island, about forty miles north of Marco. Every March the four of us would meet once or twice somewhere in the area for lunch or some other adventure. But it was the quality time we spent with the Meeks every summer on Star Island for over thirty years that most sustained our friendship.

Let me tell you a little more about Star Island, a magical place for both the Hines and the Meeks families. Star Island is located off the West Shore of Cass Lake, the ninth largest lake in Minnesota. Cass Lake is the second biggest lake in the chain of lakes that form the headwaters of the Mississippi River. The river flows into the west side of Cass Lake and flows out seven miles away on its east side. Not surprisingly, Star Island is in the shape of a star with four points; and it contains about 1500 acres of heavily forested land, with lots of mature white pine and red pine trees. The island is part of the Chippewa National Forest, and has the highest population of eagles in the lower forty-eight states. In the eighteenth century, the northeast tip of the island was home to a small tribe of Ojibway Indians. The first summer cabin on the island was built over a century
ago in 1910 and it housed the local Forest Ranger. This cabin still stands, but is now privately owned. Today, there are eighty-four summer residences on the island. One third of the summer homes are privately owned; the other two thirds are on land leased from the U.S. Forest Service. The island is interlaced with miles of hiking trails and features an abundance of interesting flora and fauna.

Star Island is somewhat unique because a beautiful 200-acre wilderness lake, Lake Windigo, lies in the interior of the island – a lake in the center of an island in a lake. Lest you doubt its uniqueness, Lake Windigo was once featured as a “geological wonder” in a “Ripley’s Believe It Or Not” book. Jim first accompanied me to Star Island in late spring of 1967. We drove up to the lake to meet my dad for a long weekend of fishing and male bonding. Jim was immediately captivated by the special character of Star Island. He was already familiar with this part of Minnesota, having visited relatives who lived on nearby Leech Lake several times in his youth. Jim made many summer visits to Star Island over the next ten years, first by himself joining us at our cottage, and later with his family. For several summers, Jim’s family rented a unit at Hooks Landing, an old-fashioned fishing resort two miles across the lake from our summer cabin. During those visits, besides fishing together while the kids played on our beach, we enjoyed shared evening meals almost every night.

Ultimately, in 1979, Jim and Priscilla purchased their own Star Island cottage on a sandy south shore beach, investing a small inheritance Priscilla had received from her Aunt Mary. Starting in 1980, they spent a month or more there every summer. Soon summer activities on Star Island became deeply imbedded in the rhythms of their family life. Jim’s leadership skills were put to use as Commodore of the Star Island Yacht Club, which raced small family sailboats around the island, and later as President of the Star Island Protective League, a non-profit organization that was the closest thing to local government on the island. Over the years, we were fortunate to enjoy many wonderful times doing fun things with the Meeks on Star Island, until Jim’s disability prevented his traveling there the last two years of his life.

IV. Jim was a Resilient Survivor

It is still hard to believe that his Parkinson’s disease finally got the best of Jim. So many other health conditions that would overwhelm other people barely phased Jim. Of all the people I knew with bothersome health conditions, Jim was the most resilient at bouncing back from life-threatening accidents, bad falls, Crone’s Disease, Diabetes, a heart attack, and multiple joint replacements. (Jim was the real Bionic Man.)

I still vividly remember my shock in August of 1983 when I received the phone call from one of Jim’s Ohio State faculty colleagues advising me that Jim and his family had experienced a devastating traffic accident on their way home from Star Island. The Meeks’ minivan was towing a boat trailer full of furniture when it ran off the road, ending up in a steep roadside ditch. Jim was in critical condition in a hospital in Danville, Illinois and it was not certain whether he
would survive his massive injuries. Priscilla was also injured badly with several broken bones. Thankfully, Kathy and Jeff had walked away from the accident with only minor injuries.

At the time of the accident, Jim was asleep in the back seat without a seat belt, and he was ejected from the van, which then landed on him. Besides a number of injuries to his limbs, Jim suffered severe damage to his abdomen, resulting in some life-threatening internal injuries. Surgeons removed Jim’s spleen and did major repairs to his liver and other internal organs. If you ever noticed the ugly scar down the middle of Jim’s abdomen, you would appreciate the seriousness of these injuries. Obviously, Jim did survive, and as soon as he was stable, he was transported to a top hospital in Columbus, where we visited him a few days later. Jim being Jim, he was already in recovery mode, making light of his injuries, praising his doctors and nurses, and already planning his return to the classroom.

Like many people, I dread going to a hospital for any reason. Jim, on the other hand, appeared to actually enjoy much of his time in hospitals, and he spent a great deal of time there over the years. Hospitals were almost his second home, and I never heard a discouraging word from him about them or the care he received. On our last Ozark fishing trip together, one night as Jim bent over to untie his shoes before getting into bed he dislocated his artificial left hip. He was in great pain, but refused any pain killers offered by the first responders. Jim was transported by ambulance fifty miles over winding mountain roads to the nearest hospital in Springfield, Missouri. When I picked him up from the hospital the next morning his hip was back in place and it was as if nothing unusual had happened. He was amazingly cheerful, and he was anxious to get back to the fishing. His only mention of the incident was an apology for costing me a half day on the lake to come get him.

Another scene relating to Jim’s medical conditions stands out in my memory. It occurred on one of our last Ozark fishing trips together. Our fishing gang was having a leisurely lunch in a local restaurant. Jim was complaining to Dr. John Layle, then a practicing Internist, about how he disliked the severe dietary limits he had to observe owing to his active Crone’s Disease and an advancing diabetes condition. He was telling John about these troubling health problems as he wolfed down a huge double cheeseburger, followed by a gigantic piece of strawberry-rhubarb pie ala mode, washed down by a large glass of sweet tea. (Jim never met a piece of pie for which he did not lust.) Dr. Layle could only roll his eyes, but I could tell what he was thinking: “Severe dietary limitations, my foot. Jim’s Crone’s and diabetes must be the most amazingly mild cases in medical history.”

V. FISHING WITH JIM FOR OVER FIFTY YEARS

Until Parkinson’s disease slowed him down, Jim was my most consistent fishing buddy, and we fished a lot. Jim and I went fishing together literally hundreds of times all over the United States and Canada. We fished together for
bass in farm ponds around Iowa City and in the Ozarks on Table Rock Lake, for trout in mountain streams in the front range of the Rockies, for snook and sea trout off sandy beaches of Southwest Florida, and for muskies in the Crowe River chain of lakes in Eastern Ontario. Most of our fishing, however, was concentrated in three venues: Table Rock Law in Southwest Missouri, Cass Lake in North Central Minnesota, and Lake of the Woods in Western Ontario, Canada.

The very first spring he lived in Iowa City, I took Jim on a fishing trip to my favorite Ozark impoundment, Table Rock Lake. Table Rock Lake was then a brand new Corps of Engineers reservoir in the Missouri Ozarks, impounded just a few years earlier but already developing a reputation as a “hot spot” for bass fishing. Table Rock is a huge lake with 15,000 miles of shoreline flooding three river systems famous for float trips before the lake came along. Jim was familiar with trout fishing from seasonal visits to the family “Camp,” near Tallmansville, West Virginia, where as a boy he enjoyed outdoor activities with his mother’s adult relatives and several young cousins. But Jim was a neophyte bass fisherman. Considerable time was therefore spent in preparation for this outing, just learning how to cast a level-wind casting reel without creating a maddening backlash was a challenge. Jim never completely mastered this art, however, so he was affectionately known among our fishing friends as “Mr. Backlash.” Because his casting accuracy was always suspect, Jim developed one fishing skill the rest of us genuinely admired. He became a master at retrieving seemingly lost fishing lures from where they landed high in shoreline trees.

Wouldn’t you know, on his first day with me on Table Rock Lake Jim caught a 9.5 lb. bass, a much bigger fish than I ever caught in a lifetime of bass fishing. That bass was mounted and still holds a place of honor on the wall of the Meeks’ Star Island cabin. I immediately informed Jim that it was rookie luck; he just happened to be in the right place when that ancient fish decided to commit suicide. Later in the day, I warned Jim that if he caught another lunker like his first big bass, he might never be invited to go fishing with me again. This was obviously an insincere threat as Jim became my regular fishing buddy for countless hours on the water over the next fifty years.

On that first trip to the Ozarks in March 1965, we camped out in my leaky old canvas army tent. After two cold and wet nights in the tent, we went to the Marina café for a hot breakfast. We were so bedraggled that Mrs. Null, who ran the restaurant, took pity on us and kindly offered to let us take a free hot shower at the Shad Rack Resort, which she owned just up the road. After gratefully accepting her offer and enjoying the luxury of hot shower, we returned to thank her and inquire how much the room rates were at her resort. March was off-season and the room rate was $12, or only $6 apiece. On hearing this price, even though we were then poorly paid young teachers, we just looked at each other, nodded agreement, immediately broke camp and moved to the resort. We resolved then and there never to camp out again when a dry room with a hot shower and all the amenities was available so cheaply, and that was our last camping experience together. Jim and I ended up patronizing the Shad Rack
Resort every Table Rock trip for the next forty years, so Mrs. Null made a smart business decision in offering a hot shower to a couple of chilled campers.

Until he was no longer able to travel, Jim and I made one or two fishing trips to Table Rock Lake together every year. Often we were joined by former law students and an occasional law faculty member. Later, several members of the Baker gang became regulars on the annual Ozark adventure. More than once, we organized fishing groups of six or more fisherman for Table Rock trips. The quality of fishing in Table Rock Lake varied a great deal from year to year, depending on the lake level, climatic factors and whether the bass were cooperative, but we always caught enough fish for one or two sumptuous fried fish dinners. Measured by the good fun and fellowship enjoyed by all, the Ozark trips were always a great success. Jim last made the Table Rock trip in the spring of 2014, and except for the one night spent in a local hospital to correct a dislocated hip, he participated fully and caught his share of bass and crappie.

When Jim first visited Star Island in 1967, my family and I fished Lake Windigo exclusively because we were intimidated by the size of the main body of water in Cass Lake (15,000 acres) and we knew we could catch lots of bass and pan fish in the interior lake. On one of our early fishing adventures on Lake Windigo, we were accompanied by our former law student, John Rashke, who later joined us on many fishing trips, and by our friend Larry Wilson, another frequent fishing buddy. On this May trip, the four of us enjoyed one fabulous fishing day of bass fishing on Lake Windigo. The photo showing off the impressive stringer of big bass we caught and later released that day records one of our most treasured fishing memories. After a number of years, we finally began to master fishing in the main lake, which boasts one of the finest walleye fisheries in all of Minnesota. Now, with some confidence, we claim we can catch a walleye dinner whenever we want one. It is called “fishing” and not “catching,” however, for a reason. Sometimes the walleye just do not cooperate and we have to settle for grilled hamburgers. Fortunately, even hamburgers taste better in the North Woods.

In 1973, Priscilla’s widowed mother, Helen Lohr, married Dr. Rolland Morrison, a prominent doctor from Carroll, Iowa. Jim and I discovered a decade later that Priscilla’s new step father was an avid fisherman. His favorite fishing venue was Lake of the Woods, a huge body of water that straddles the Minnesota/Ontario border. One distinction of Lake of the Woods is that it is home to 1400 islands greater than an acre in size, giving it a shoreline larger than all of the five Great Lakes combined. In 1983, Dr. Morrison invited Jim and me to go with him on a fishing trip to Lake of the Woods to fish for walleyed pike and yellow perch. Dr. Morrison had already retained the services of a top local fishing guide who could safely navigate us through the maze of islands to prime fishing spots. We enjoyed fantastic walleye fishing. Jim’s 9-year old son Jeff joined us for this fishing excursion, and imitating his father, Jeff caught the largest walleye of the trip, bigger than any of us had ever caught. Jeff’s big fish won the resort’s prize for largest walleye for the month, and every year thereafter when Jeff joined us for the Lake of the Woods outing we had to check
at the resort’s display board to make sure it still featured Jeff’s “big fish” photo.

When Dr. Morrison dropped out of the Lake of the Woods trips for health reasons after a couple of years, we recruited some of our Ozark fishing buddies and Star Island regulars to join us in continuing this summer tradition. We continued to make at least one trip to Lake of the Woods every year for the next three decades, and always enjoyed spectacular walleye fishing. Jim last participated in our annual Lake of the Woods adventure in July, 2014. Thanks to the special attention paid him by Doug Freitag, our excellent guide, Jim had three memorable days of fishing, catching the biggest walleye and a good number of other “keeper” fish. The annual fishing trips to Table Rock and Lake of the Woods, and our summers on Star Island just have not been nearly as enjoyable since Jim became unable to participate in them.

VI. MISSING JIM

The reality that Jim was actually no longer alive hit me hard for the first time on a Saturday afternoon late in the fall of 2017. Amazingly, Iowa had just demolished Ohio State on the football field, and I picked up the phone to start to call Jim to gloat over Iowa’s stunning victory. Then I realized Jim would not be answering the phone, and I would never be able make such a call again. I had already lost Jim as a fishing buddy a couple of years earlier when his disability grounded him; now he was lost to me forever. The realization that Jim was no longer with us was very difficult for me to accept, and I am sure all of Jim’s family and most of Jim’s colleagues, friends and acquaintances reflect from time to time on how big a gap Jim’s passing left in their lives.

Jim was successful in almost everything he undertook in life, not only because he was smart, honest, creative, caring and incurably optimistic, but also because he was blessed with outstanding people skills. He was a very good listener and possessed an extraordinary degree of empathy that enabled him to understand and relate to the problems a wide range of people brought to him. Jim was the ultimate “team player,” who could work comfortably with anyone from anywhere on almost any type of venture, all the time making others around him feel like their contributions were the key to the success of the joint project.

Jim was definitely one of the “good guys”—the type of person when you were young your mother encouraged you to hang out with for your own self-improvement. I know this is true because my mother was one of Jim’s biggest admirers, often encouraging me to bring him along to family events during the five years he was single on first arriving in Iowa City. Later, in summers after Jim and Priscilla married, summers when my parents were in residence at their cabin on Star Island, they always looked forward to Jim and members of the Meeks family dropping by to visit with my mom and my disabled dad. Jim and Priscilla’s mother Helen were among my parents’ favorite summer Star Island bridge opponents, and Jeff and Kathy became good friends with several of my nephews and nieces, who were their ages.
VII. CONCLUSION

In conclusion, it dawned on me in the course of writing this tribute to Jim that it is more than a little autobiographical—in telling Jim’s story I was also telling much of the story of my own life. The parallels are hard to miss. I am only two years older than Jim, and we were both greatly blessed to live during the past eight decades, largely a time of unprecedented peace, prosperity and technological advancement in America. We both grew up in the Midwest, were nurtured by loving parents and relatives, were supported by a family culture that encouraged our highest ambitions, were afforded the chance to profit from a first-rate education, were fortunate in not having been called to military service, were surrounded as adults by devoted family and friends, worked for a lifetime at jobs we genuinely loved, and we both enjoyed an active retirement, until accelerating health problems intervened to cut short Jim’s life.

Jim with a Large Lake of the Woods Walleye

Jim truly was one of the most decent, honorable and caring people I’ve ever met. He richly deserved a much longer retired life than he was afforded, and a much less miserable ending than he had to endure. Jean and I join Jim’s family and his legion of friends in grieving his loss. I count it as one of the greatest privileges of my life to have known Jim so well for so long, and to have spent so much enjoyable time with him and his wonderful family. Knowing and interacting with Jim enriched my life in more ways than I can count, and I will forever be grateful for the opportunity to have enjoyed his delightful friendship on so many occasions for over fifty years.
Toying with Privacy:
Regulating the Internet of Toys

ELDAR HABER*

Recently, toys have become more interactive than ever before. The emergence of the Internet of Things (IoT) makes toys smarter and more communicative: they can now interact with children by “listening” to them and responding accordingly. While there is little doubt that these toys can be highly entertaining for children and even possess social and educational benefits, the Internet of Toys (IoToys) raises many concerns. Beyond the fact that IoToys devices might be hacked or simply misused by unauthorized parties, datafication of children by toy conglomerates, various interested parties, and perhaps even their parents could be highly troubling. It could profoundly threaten children’s right to privacy by subjecting and normalizing them to ubiquitous surveillance and datafication of their personal information, requests, and any other information they divulge. While American policymakers acknowledged the importance of protecting children’s privacy online back in 1998 when crafting Children’s Online Privacy Protection Act (COPPA), this regulatory framework might become obsolete in the face of the new privacy risks that arise from IoToys. Do fundamental differences between websites and IoToys necessitate a different legal framework to protect children’s privacy? Should policymakers recalibrate the current legal framework to adequately protect the privacy of children who have IoToys devices? Finally, what are the consequences for children’s privacy of ubiquitous parental surveillance through IoToys—allegedly granted to safeguard children from online risks? And how might children’s privacy be better framed and protected in this context?

* Senior Lecturer, Faculty of Law, University of Haifa; Faculty Member, Haifa Center for Law & Technology (HCLT) and the Center for Cyber Law & Policy (CCLP), University of Haifa; Faculty Associate, Berkman-Klein Center for Internet & Society, Harvard University (2016–2018). I am much grateful to Meryl Alper, Michael Birnhack, Niva Elkin-Koren, Esther Tabitha Earbin, Michal Gal, Natali Helberger, Sunny Kalev, Omri Rachum-Twaig, Arianne Renan Barzilay, Galia Schneebaum, Yoram Shachar, Adam Shinar, Lev Streltsov and Tal Zarsky for their extremely helpful suggestions and comments. I also wish to thank Chen Arobas and Ori Gorali for their excellent assistance in research, and participants of the Haifa law school research seminar (Feb. 2018); GYSM “Legal Rules for the Digital Economy” workshop, Potsdam, Germany (Feb. 2018); Law & Emerging Technology Event at the Max Planck Institute for Foreign and International Criminal Law, Freiburg, Germany (Apr. 2018); Faculty seminar at Radzyner Law School at IDC Herzliya (May 2018). This work was supported by the Center for Cyber Law & Policy at the University of Haifa in conjunction with the Israel National Cyber Directorate in the Prime Minister’s Office.
This Article focuses on the privacy concerns that IoToys raises. Part II briefly outlines the evolution of IoToys while examining its devices’ capacity to collect and retain data. Then, in reference to the legal framework chosen to protect children from online datafication twenty years ago, Part III discusses the American perception of children’s privacy, focusing on COPPA. Through this analysis, this Part will show how key market players currently comply with COPPA regulation, and it will evaluate whether such compliance is relevant to IoToys’s dangers and challenges. Part IV revisits COPPA, challenges it, and in calling for its recalibration, offers some practical solutions to IoToys’s privacy threats. Thereafter, Part V normatively evaluates children’s conception of privacy, argues that IoToys’s monitoring practices could jeopardize the parent–child relationship, and calls for recalibrating children’s privacy in the digital era. The final part summarizes the discussion and concludes that children’s privacy matters today perhaps more than ever before and that the potential movement toward a ubiquitous surveillance era should not lead to its demise.

TABLE OF CONTENTS

I. INTRODUCTION ..................................................................................401
II. THE INTERNET OF TOYS....................................................................403
   A. The Evolution of Connected Smart Toys.........................................403
   B. Surveillance and Datafication of Children in IoToys ....................409
III. REGULATING PRIVACY WITHIN THE INTERNET OF TOYS.................411
   A. Children’s Right to Privacy ...................................................412
   B. Applicability of the Legal Framework .......................................416
IV. REEVALUATING AND RECALIBRATING CHILDREN’S PRIVACY ........424
   A. Revisiting Children’s Privacy in IoToys ........................................425
   B. Recalibrating the Legal Framework ..........................................428
      1. Raising Awareness ............................................................431
      2. Redefining Choice ...............................................................435
      3. Data Minimization and Transparency ....................................436
      4. Toy and Information Security ..............................................438
      5. Effective Enforcement .......................................................441
V. TAKING CHILDREN’S PRIVACY SERIOUSLY ..................................443
   A. Parenting in the IoToys Era .....................................................444
   B. Child Development and Privacy ..............................................446
   C. Children’s Choice? .................................................................451
VI. CONCLUSION...................................................................................453
I. INTRODUCTION

Children’s toys are more communicative now than ever before. Implementing the advantages of what is commonly termed the Internet of Things (IoT),1 many toy conglomerates have begun to produce and sell connected so-called smart toys, namely toys that can listen and actively respond to their users in real time. Being triggered, usually via a voice command, these toys will then send the message to a remote server, analyze it, and issue a timely response through the toy, as if it were talking to the child.2

Developments in this relatively new Internet of Toys (IoToys) market are advancing apace. At first, communicative toys were fairly limited in their communication abilities,3 but now this expanding market offers various types of child-targeted toys and other devices that are both smart and connected to the internet.4 Many are now equipped with microphones, speakers, cameras, and GPS trackers, along with other sensors designed to improve the toy’s abilities, and ultimately the child’s experience.5

IoToys devices sound almost like every child’s dream. But while many benefits might accrue from their use, they may also quickly turn into nightmares.6 Generally these toys, along with the cloud in which the gathered data is stored, could be hacked or accessed by third parties, thus exposing children to harmful content, and worse—endangering their personal safety and mental health.7 More closely—and within the scope of this Article—children are also subjected to ubiquitous surveillance and datafication by toy conglomerates and their trusted partners, unauthorized third parties like hackers, and even their parents.8 In other words, these seemingly harmless toys could

---


2 See discussion infra Part II.A.


5 See infra Part II.

6 See infra note 48.

7 See infra Part IV.B.4.

8 This Article will use the term “parents” in reference to legal guardianship for minors in general. Subsequently, the use of the term “surveillance” will refer to various facets of monitoring and datafication of children’s data within the Internet of Toys (IoToys). This type
potentially generate substantial harm, and perhaps worst of all, endanger children’s right to privacy.

Potential datafication and misuse of children’s data troubled policymakers long before the emergence of IoToys. Recognizing the potential dangers of the internet to children’s privacy, American policymakers designed a framework known as the Children’s Online Privacy Protection Act (COPPA) regulation, which applies to websites that target or knowingly collect personal information from children under age thirteen.\(^9\) COPPA regulation was devised long before the invention of IoT,\(^10\) but it remains the current regulatory framework governing IoToys. Do fundamental differences between websites and IoToys necessitate a different legal framework to protect children’s privacy? Should policymakers recalibrate the current legal framework to adequately protect the privacy of children who have IoToys devices? And if so, how should it be done? Finally, what are the consequences for children’s privacy of ubiquitous parental surveillance through IoToys—allegedly granted to safeguard children from online risks—and how might children’s privacy be better framed and protected in this context?

This Article approaches these and related questions by analyzing the current legal framework fashioned twenty years ago to protect young children’s privacy online and by examining—practically and normatively—how applicable it is to IoToys. Part II briefly introduces the evolution of IoToys and further examines the datafication of children within it. Part III scrutinizes children’s right to privacy at the federal level as to whether COPPA regulation is applicable to IoToys. Then Part IV reevaluates children’s privacy within the IoToys legal framework and proposes to recalibrate it in keeping with COPPA’s requirements. Part V zooms out to discuss how children’s privacy is affected by IoToys from the perspective of the parent–child relationship. It argues that children’s privacy should not be viewed as protection just from third parties but also from their parents. Part VI summarizes the discussion and concludes that children’s privacy is of profound importance, especially given a potential movement toward a ubiquitous surveillance era.

---

\(^9\) See infra Part III.A.

\(^10\) See infra Part III.A.
II. THE INTERNET OF TOYS

Toys have existed almost as long as humanity itself. According to archaeologists, they date back at least four millennia.\textsuperscript{11} While adults might occasionally play with them, traditional toys appeal mostly to children of various ages. But the meaning of \textit{traditional} in the toy realm can change swiftly, considering technological innovations. Through the application of advanced learning capabilities and connection to the internet, many toys have become more interactive than ever before in human history\textsuperscript{12} and most likely will continue to evolve for years to come.

Aside from their enjoyment and other potential educational and social benefits,\textsuperscript{13} IoToys might also have a dark side. Along with IoToys devices’ datamining capabilities, they could be exploited by various entities and eventually harm children and violate their legal rights.\textsuperscript{14} For a better understanding of these concerns, Part II.A briefly tells the story of how toys became interactive from the first talking doll in 1890 to the latest technological developments of IoToys. The second section exposes and evaluates the potential dangers that IoToys raises in general and reviews the datamining practices of key market players in the IoToys industry to prepare the way for evaluating IoToys’s implications for children’s privacy.

A. The Evolution of Connected Smart Toys

In 1890, Thomas Edison introduced the first-ever talking doll to the world.\textsuperscript{15} Edison inserted a miniature model of his phonograph into a doll’s chest, which enabled it to recite a twenty-second rendition of a well-known rhyme.\textsuperscript{16} Humanity, though, did not care for Edison’s invention at that time, as the toy proved a commercial failure.\textsuperscript{17} However, the importance of Edison’s first-ever communicative toy lay mainly in its innovative thinking: it marked the potential birth of a new market, namely toys that could interact with children.

\textsuperscript{13} See infra Part II.A.
\textsuperscript{14} See infra Part II.A.
\textsuperscript{15} Dawson, supra note 3. Edison’s idea for commercializing his phonograph through dolls could be traced to a notebook entry in 1877. \textit{See} James Vlahos, \textit{Barbie Wants to Get to Know Your Child}, \textsc{N.Y. Times} (Sept. 16, 2015), https://www.nytimes.com/2015/09/20/magazine/barbie-wants-to-get-to-know-your-child.html [on file with \textit{Ohio State Law Journal}].
\textsuperscript{16} See Dawson, supra note 3.
\textsuperscript{17} Id.
A market demand for interactive toys can be traced back to the early 1960s. One of the key examples of this then-new market is pull-string dolls like Mattel’s Chatty Cathy. Only then did the market begin to thrive. Not long after Chatty Cathy’s commercial success, Mattel introduced other communicative toys like See ‘n Say. Years later, other toy manufacturers followed suit by introducing communicative toys like Teddy Ruxpin and Furby. Technology inspired life in toys, as they could now talk to children. At this stage, toys’ abilities were still quite limited. Prior to the development of IoT, when ordinary objects became connected to the internet, toys’ communication was still almost entirely one-sided. Even the most communicative toys had tightly limited storage capacity and learning capabilities, and they could not transfer data beyond their physical space, let alone analyze it and respond to their users.

With the development of IoT, and along with various devices targeted at children, toys became more sophisticated or—stated differently—smarter. They began not only to repeat predefined phrases or well-known rhymes, but also to listen and respond. These smart toys interact with their users through an array of electronic features such as microphones, speakers, sensors, cameras, gyroscopes, and radio transmitters. Besides smart toys, another form of new toys emerged, capable of connecting to an external network, mostly the internet, via a Wireless Fidelity (Wi-Fi) connection, cellular data networks, or Bluetooth. These connected toys are designed to connect to the internet or

---

23 See Kids & The Connected Home, supra note 4. It is notable that the use of the word “smart” to describe various types of devices and toys might be perceived as somewhat inaccurate to describe their true functions. Nevertheless, I generally use this term in this Article as it is often used by many to describe these devices and toys.
24 Id. at 3–4.
other devices in order to receive and transmit data.\textsuperscript{25} The combination of these two innovations led to the formation of \textit{connected smart toys}, or more simply stated, IoToys. These toys could interact meaningfully with their users, hence they could be attractive to anyone, not just children. IoToys marked the birth of two-way communication toys.

Realizing a potential demand for IoToys devices, before long the market reacted. In 2015, Mattel collaborated with ToyTalk (later rebranded as PullString, Inc.) to introduce a Barbie doll that “actually listen[s] and talk[s] back.”\textsuperscript{26} Using speech recognition, Hello Barbie connects to the internet via Wi-Fi, and by the press of a buckle button on its belt, Hello Barbie turns its microphone on and begins recording.\textsuperscript{27} The data is then sent from the doll to a cloud-based service of ToyTalk, and following analysis, a response is streamed back to the user through the doll’s speaker.\textsuperscript{28}

Hello Barbie clearly marked the beginning of a thriving new market.\textsuperscript{29} To name a few examples, following Hello Barbie, Mattel introduced the Hello Barbie Dreamhouse (hereinafter The Dreamhouse), a smart connected home for Barbie dolls;\textsuperscript{30} Fisher-Price, a subsidiary of Mattel, introduced a Wi-Fi-connected smart toy bear that “talks, listens, and ‘remembers’ what your child says and even responds when spoken to”;\textsuperscript{31} CogniToys introduced various

\begin{itemize}
\item Smart toys and connected toys are not necessarily synonymous. The fact that a toy is smart does not mean it is connected, nor the other way around. Smart toys could be offline and connected toys might not be equipped with technological capabilities to elevate them to the level of being categorized as “smart.” For more on smart and connected toys, see \textit{id.} at 2.
\item Lobosco, \textit{supra} note 12.
\item See Iain Thomson, \textit{Hello Barbie: Hang on, This Wi-Fi Doll Records Your Child’s Voice?}, \textit{The Register} (Feb. 19, 2015), http://www.theregister.co.uk/2015/02/19/hello_barbie [https://perma.cc/4HS4-WX4D].
\item It seems that it will not take long before market players expand their variety of IoToys devices and new companies will join this growing market. Google, for instance, has filed a patent request back in 2015 for a teddy bear outfitted with sensors and cameras. See Hope King, \textit{Google Files Patent for Creepy Teddy Bear}, CNN (May 22, 2015), http://money.cnn.com/2015/05/22/technology/google-doll-toy-connected-device-patent [https://perma.cc/PG24-ZGGL]; Press Release, Juniper Res., Smart Toy Revenues to Hit $2.8BN This Year, Driven by Black Friday & Christmas Holiday Sales (Nov. 9, 2015), https://www.juniperresearch.com/press/press-releases/smart-toy-revenues-to-hit-$2-8bn-this-year [https://perma.cc/8CK5-LJUT].
cloud-connected toy dinosaurs that listen to children’s questions and answer according to their age; and Genesis, a company incorporated under the laws of Hong Kong, introduced My Friend Cayla (hereinafter Cayla), a doll that could talk and interact with users, play games, share photos, and read stories. This market appears to be growing continuously.

The children’s IoT market has recently expanded beyond toys. This expansion was first proclaimed early in 2017, when Mattel, under its “Nabi” brand, announced its plan to manufacture a smart Wi-Fi-connected speaker for children. This device, named Aristotle, was supposed to be equipped with a microphone, LEDs, and a camera, and it was designed to act like a computerized personal assistant akin to Amazon Echo or Google Home.

4CVZ-3QGJ (describing the current range of toys).


36 See id.

37 Computerized personal assistants (also known as intelligent personal assistants) are software agents that can perform tasks or services for an individual, usually based on user input, location awareness, and the ability to access information from a variety of online sources. There are various types of computerized personal assistants, e.g., Apple’s Siri and Microsoft’s Cortana. Google had even embedded such technology in 2014, under a pre-installed ability in Google’s Chrome browser that passively listened for the words “OK, Google” to launch a voice-activated search function. See Tony Bradley, ‘OK Google’ Feature Removed from Chrome Browser, FORBES (Oct. 17, 2015), http://www.forbes.com/sites/tonybradley/2015/10/17/ok-google-feature-removed-from-chrome-browser/#16d299a44e27 [https://perma.cc/Y9TZ-9JU3]; Top 22 Intelligent Personal Assistants or Automated Personal Assistants, PAT Res., http://www.predictiveanalyticstoday.com/top-intelligent-personal-assistants-automated-personal-assistants/#content-anchor [https://perma.cc/DQ9Z-FW3M]. More specifically, Amazon Echo is “a hands-free speaker you control with your voice.” Amazon Echo, AMAZON, https://www.amazon.com/Amazon-Echo-Bluetooth-Speaker-wiFi-Alexa/dp/B00X4WHP5E [https://perma.cc/C6XL-KZZQ]. It “connects to the Alexa Voice Service to play music, ... provide information, news, sports scores, weather, and more—instantly.” Id. Google Home is a voice-activated speaker powered by the Google Assistant. “Ask [it] questions. Tell it to do things. It’s your own Google, always ready to help.” Google Home Devices, GOOGLE HOME HELP,
programmed for children’s purposes. As for now, Mattel decided that Aristotle is not fit for release, and its future is still uncertain. Mattel, however, currently still plans to release the Hello Barbie Hologram (hereinafter The Hologram): a small box with an animated projection of Barbie that responds to voice commands. Closely akin to computerized personal assistants like Amazon Echo or Google Home, the Hologram uses a wake phrase (“Hello Barbie”), so unlike Hello Barbie, this device operates in an “always on” mode: for the device to begin functioning, it must constantly listen for the wake phrase. Respectively, Amazon had already entered this market recently, introducing the Echo Dot “Kids Edition”—a standard Echo Dot with “parental controls, kid-friendly content, and an optimized experience for kids.” All in all, as could be drawn from these innovative projections of new devices, IoT will most likely play a substantive role in child-targeted devices in the foreseeable future.

IoToys presents children with interactive playing. Beyond the toys’ fun, they could carry educational and social benefits for children: opportunities to learn, pick up, and improve communication skills; retain interest in playing despite children’s short attention spans; encourage active play and toy interaction, which might be preferable to passive screen time; foster collaborative play with other children; identify learning difficulties or medical problems; and be economically efficient for parents because their software could be updated. On the other hand, IoToys devices have been criticized for


An “always on” mode refers to devices where there is no need to physically push a button to turn them on, but rather they are activated by a voice command or through the device app. Using speech recognition, users simply need to say a trigger phrase to activate them. Examples include Amazon Echo and Google Home, both activated by a trigger phrase such as “Alexa” or “OK Google” respectively, and once activated record the voice command of their user. See sources cited supra note 37.


their potential educational, social, and psychological drawbacks. To name a few: providing poor quality of play; potentially harming children’s development, impeding child–parent interaction; obstructing children’s well-being and healthy development, which require real relationships and conversations; and posing a risk to health from electromagnetic radiation (EMR).

IoToys devices’ potential drawbacks do not stop there. They might subject children to various risks, for example, exposure to harmful content. There is even the danger of mental and bodily harm by predators, some of whom could have access toys and use them to listen to, watch, track, and even directly contact children. Along with these important challenges, these IoToys devices further raise human rights concerns. Potentially, they can subject children to ubiquitous surveillance and datafication, which could profoundly impact their right to privacy.

---


45 Digital caretaking could negatively affect children’s development as it lacks necessary physical bonding. See id.

46 See, e.g., Richard Chirgwin, Mattel’s Parenting Takeover Continues with Alexa-Like Dystopia, THE REGISTER (Jan. 4, 2017), https://www.theregister.co.uk/2017/01/04/mattels_parenting_takeover_continues_with_alexalike_dystopia [https://perma.cc/NXP5-7GW3].


48 As these toys rely on remotely stored data, they could be subjected to harmful content as information might become vulnerable and could be changed by a malicious entity which gained access to the toy or simply due to bad or error in programing. See, for instance, how a misunderstanding led Amazon Echo to spout porn search terms to a toddler. Amazon Alexa Gone Wild, YOUTUBE (Dec. 29, 2016), https://www.youtube.com/watch?v=r5p0gqCIEa8 [https://perma.cc/SE3G-M5ZU]. See also how a specialist team hacked Cayla to quote Hannibal Lecter and lines from 50 Shades of Grey. See David Moye, Talking Doll Cayla Hacked to Spew Filthy Things, HUFFPOST (Feb. 9, 2015), http://www.huffingtonpost.com/2015/02/09/my-friend-cayla-hacked_n_6647046.html [https://perma.cc/78HN-89F6].

49 When children assume that it is the toy that is “talking” to them, predators might be able to persuade them to convey sensitive information. These predators could obtain information from children like where they live and, perhaps even worse, convince them to act on their behalf. See Abby Haglage, Hackable ‘Hello Barbie’ the Worst Toy of the Year (and Maybe Ever), DAILY BEAST (Dec. 10, 2015), http://wwwthedailybeast.com/hackable-hello-barbie-the-worst-toy-of-the-year-and-maybe-ever [https://perma.cc/85E4-AGQW]. For a typology of risks to children online, see ORG. FOR ECON. CO-OPERATION & DEV. (OECD), THE PROTECTION OF CHILDREN ONLINE - RECOMMENDATION OF THE OECD COUNCIL REPORT ON RISKS FACED BY CHILDREN ONLINE AND POLICIES TO PROTECT THEM 24–39 (2012), https://www.oecd.org/sti/ieconomy/childrenonline_with_cover.pdf [https://perma.cc/33T7-R645].

50 For more on children’s right to privacy, see infra Part III.A.
purpose of this Article—the next section briefly surveys the proclaimed datamining practices of key market players in the IoToys realm.

B. Surveillance and Datafication of Children in IoToys

While toys have evolved to become smarter and connected, the various IoToys devices may evince wide differences. Some are smarter than others. Some are equipped with more technological tools that enhance their capabilities; others are simply more sophisticated, for example, by being equipped with a microphone, while others have cameras and other sensors. Some, like Hello Barbie, require their users to turn them on manually, while others, like the Dreamhouse and the Hologram, operate in an “always on” mode, namely by constantly operating as they await their wake phrase. Yet their different characteristics notwithstanding, the core functions of IoToys devices are fairly similar: upon activation, each toy acquires data from its user, sends it to a remote server where it is analyzed, and transmits a response through the toy’s speaker. Datamining is essentially at the core of their functioning.

Take, for example, Mattel, which manufactures several types of IoToys and connected smart devices such as Hello Barbie (doll and hologram) and the Dreamhouse. The speech processing services for Hello Barbie and the Dreamhouse (hereinafter Barbie Products) are currently operated by ToyTalk. Barbie Products capture recordings upon users’ interaction with them, whether by pressing the “talk” button or saying the wake phrase. Other products, like Cayla, also capture their users’ recording, usually after a wake phrase. Fisher-Price’s Smart Toy bear collects a parent’s email address and login password; child’s first name, birthdate, and gender; toy name and identifier; Wi-Fi password; and mobile device information. Essentially, most of these IoToys devices capture audio recordings and collect some forms of data.

The information mined through these toys is then stored, usually in the cloud, for various purposes. Obviously, data can be highly valuable for various

52 Thomson, *supra* note 27.
53 See Moynihan, *supra* note 40.
55 See id. (“When children or other users talk with Hello Barbie by pressing and holding the ‘Talk’ button, interact with Barbie Hello Dreamhouse after saying the Gate Phrase, or record their voice to customize the sounds in a room, we may capture voice recordings.”).
56 *Privacy Policy*, *supra* note 33; This Is Cayla, *supra* note 33.
57 MINORITY STAFF OF S. COMM. ON COMMERCE, S. CI., & TRANSP., 114TH CONG., REP. ON CHILDREN’S CONNECTED TOYS: DATA SECURITY AND PRIVACY CONCERNS 12 (Comm. Print 2016) [hereinafter CHILDREN’S CONNECTED TOYS]. Images and audio, however, are currently only stored locally on the bear. *Id.*
58 ToyTalk and Genesis both mention that they store voice recordings in the cloud. ToyTalk announced that they may “use, store, process, convert, transcribe, analyze or review
interested parties for a variety of business purposes, much like any data gathered online.\textsuperscript{59} Data can potentially be commercialized and shared with other interested parties.\textsuperscript{60} From a functional aspect, data could be valuable for the toy’s improvement. As some toy manufacturers and online service providers (OSPs) posit, the entertainment experience from the toy is based to some extent on the audio recordings sent from it, which are then analyzed and stored.\textsuperscript{61} Improving the functioning of the speech-processing services is essential, as is the development, testing, and improvement of speech-recognition technology and artificial-intelligence algorithms;\textsuperscript{62} likewise the development of acoustic and language models.\textsuperscript{63} It might also be necessary for other research, development, and data analysis purposes.\textsuperscript{64} Finally, in the sense of innovation, companies might need the data to ameliorate services, functionality, and the development of other toys and devices in the IoT market.

To recap briefly, while it is difficult to assess how and to what extent the collected data is used, and by whom, these companies evidently are able to capture various types of data. Toys with microphones could allow listening to and recording any conversations taking place in relatively close proximity to the toys. Toys equipped with sensors could give third parties access to data in real-time from these sensors. Toys with GPS trackers let third parties know where the toys are currently located and where they have been since they were first voice recordings.” See, e.g., TOYTALK, Privacy, supra note 54. As for the Hologram, however, Mattel announced that it does not save the recordings in its servers. See Moynihan, supra note 40.

\textsuperscript{59} See, e.g., Grace Chung & Sara M. Grimes, Data Mining the Kids: Surveillance and Market Research Strategies in Children’s Online Games, 30 CAN. J. COMM. 527, 533 (2005).

\textsuperscript{60} Genesis, for instance, mentions that upon consent, they are entitled to collect, process, maintain, and transfer personal information in and to the United States and other applicable territories in which their privacy laws are not as comprehensive as or equivalent to those in the country where the data subject resides or is a national. They also share information with “trusted partners” and other entities in the “family of companies controlled by Genesis” for internal reasons, primarily for business and operational purposes. See Privacy Policy, supra note 33. ToyTalk shares captured data with third parties under exception listed in the privacy policy. Interestingly, however, ToyTalk claims that they will not share voice recordings with Mattel, rather only anonymized information that does not count as personal information. See TOYTALK, Privacy, supra note 54; Hello Barbie and Hello Dreamhouse Privacy FAQ, TOYTALK, https://toytalk.com/hellobarbie/privacyfaq [https://perma.cc/57MY-4ZAA] [hereinafter TOYTALK, FAQ].

\textsuperscript{61} ToyTalk claims that they use audio recordings to create the entertainment experience. According to Martin Reddy, a chief technical officer at ToyTalk, analyzing recordings enables ToyTalk to boost the accuracy of what Hello Barbie hears by about 15%. See Mark Harris, Virtual Assistants such as Amazon’s Echo Break US Child Privacy Law, Experts Say, THE GUARDIAN (May 26, 2016), https://www.theguardian.com/technology2016/may/26/amazon-echo-virtual-assistant-child-privacy-law [https://perma.cc/EKT5-DN93]. It should also be further noted that ToyTalk archives users’ play sessions. See TOYTALK, FAQ, supra note 60.

\textsuperscript{62} See TOYTALK, Privacy, supra note 54; Privacy Policy, supra note 33.

\textsuperscript{63} See TOYTALK, Privacy, supra note 54.

\textsuperscript{64} Id.
configured. And finally, toys equipped with cameras could enable third parties to see what the toys are currently seeing. These companies can then store the data for indefinite periods, use it for their own purposes, and share it with interested parties.

While children’s datafication in IoToys might be integral for the toys’ existence and development, it also raises substantial privacy concerns. How can we properly safeguard the data aggregated through IoToys from authorized and unauthorized entities that have gained access to the data? Does the current American legal framework—originally crafted to protect children online—apply to IoToys? And does it adequately protect their right to privacy? To answer these questions, the next Part revisits and evaluates children’s right to privacy in light of IoToys.

III. REGULATING PRIVACY WITHIN THE INTERNET OF TOYS

It is generally uncontested that children require special care and assistance. As a cohort, they are less equipped with the skills and cognitive ability to comprehend some risks and concerns as adults do, let alone the depth and complexity of human rights and liberties. They might lack the requisite “maturity, [ability,] knowledge, or experience to protect themselves,” and they could be more trusting than adults. They might value their immediate needs more than their long-term interests, not understand the true nature or appropriate use of the collected information, and value privacy differently from their parents. In other words, while accounting for potential age

65 This Article focuses on the federal level, but it is also important to note that state legislators also enact privacy laws which could be applicable on IoToys as well. For more on states’ privacy legislation, see, for example, DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS 145–56 (Int’l Ass’n of Privacy Professionals ed., 2015).


71 See Jerry S. Birenz, Caching World Wide Web Sites, 16 COMM. L AW. 13, 13 (1998); Hertzel, supra note 69, at 434.

differences, children often need guidance on various aspects of their lives, including how to properly protect their privacy.

A. Children’s Right to Privacy

There are many different views on what privacy means and how best to protect it. The modern concept of privacy is generally attributed to the famous law review article by attorneys Samuel Warren and future Supreme Court Justice Louis Brandeis, published in the same year that Edison introduced the first-ever talking doll, which articulated the right to privacy as the “right to be let alone.” Since then, privacy scholars have articulated the right to privacy diversely. Key examples include the classic “control theory,” which conceptualizes privacy as the right to control information about oneself; “limited access theory,” which posits that privacy is related to our concern about our accessibility to others; and a conceptual framework of privacy as “contextual integrity,” which links the protection of personal information to the norms of specific contexts. Without belittling the importance of this scholarly debate, privacy in the context of this Article is scrutinized from the viewpoint of children, who require special protection from the harm that the internet entails, under the American approach known as “sectoral privacy.”

American policymakers chose this sectoral approach to privacy, seeking to provide legal safeguards that would presumably improve children’s safety.

---

75 ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (1968) (“[T]he claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.”).
online and reasonably secure their privacy. In 1998, under this perceived need to protect children’s privacy online, Congress enacted the Children’s Online Privacy Protection Act (COPPA). To supplement COPPA, the Federal Trade Commission (FTC) issued a rule, last updated in 2013, which is commonly referred to as the “COPPA Rule.” Both forms of regulation (hereinafter COPPA regulation) were crafted to prohibit unfair or deceptive acts or practices in connection with personal information from and about children on the internet; it is enforced by the FTC.

79 See The Child Online Protection Act, Pub. L. No. 105–277, 112 Stat. 2681–736 (1998). Information privacy was defined by the Clinton Administration’s Information Infrastructure Task Force as “an individual’s claim to control the terms under which personal information—information identifiable to the individual—is acquired, disclosed, and used.” INFO. INFRASTRUCTURE TASK FORCE, PRIVACY AND THE NATIONAL INFORMATION INFRASTRUCTURE: PRINCIPLES FOR PROVIDING AND USING PERSONAL INFORMATION 1 (1995). The conventional concept of information privacy refers to protecting a right to control one’s personal data. For further reading on information privacy, see generally Joel R. Reidenberg, Resolving Conflicting International Data Privacy Rules in Cyberspace, 52 STAN. L. REV. 1315 (2000) (exploring the divergence in internet privacy approach and substance between Europe and the United States).

80 It is worth mentioning that Congress also sought to regulate the exposure of children to inappropriate materials online by enacting the Child Online Protection Act (COPA), but it eventually failed to pass constitutional muster as it placed an “impermissible burden” on speech. See The Child Online Protection Act, Pub. L. No. 105–277, 112 Stat. 2681–736 (1998); ACLU v. Reno, 217 F.3d 162, 166–69 (3d Cir. 2000).


An ‘unfair or deceptive’ act or practice is a material ‘representation, omission or practice that is likely to mislead the consumer acting reasonably in the circumstances, to the consumer’s detriment’ or a practice that ‘causes or is 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.’

COPPA regulation applies to OSPs that target children under the age of thirteen or knowingly collect personal information from them. An OSP is any person operating an online service, including websites, “who collects or maintains personal information from or about the users of, or visitors to,” such online services. It also includes any person “on whose behalf such information is collected or maintained, where such a website or online service is operated for commercial purposes, including any person offering products or services for sale through that website or online service, involving commerce.”

As a form of market self-regulation—commonly termed privacy self-management, COPPA incorporates five essential Fair Information Practice Principles (FIPPs): (1) Notice, (2) Choice, (3) Access, (4) Security, and (5) Enforcement. Websites that fall under COPPA regulation must include a

---

Personal information means individually identifiable information about an individual collected online, including: (1) A first and last name; (2) A home or other physical address including street name and name of a city or town; (3) Online contact information as defined in this section; (4) A screen or user name where it functions in the same manner as online contact information, as defined in this section; (5) A telephone number; (6) A Social Security number; (7) A persistent identifier that can be used to recognize a user over time and across different Web sites or online services. . . . ; (8) A photograph, video, or audio file where such file contains a child’s image or voice; (9) Geolocation information sufficient to identify street name and name of a city or town; or (10) Information concerning the child or [parent] that the operator collects online from the child and combines with an identifier described in this definition.


85 Id.

88 Privacy self-management is an approach to privacy regulation whereas the law provides people with a set of rights, e.g., primarily rights to notice, access, and consent regarding the collection, use, and disclosure of personal data, to enable them to make decisions about how to manage their data. See Daniel J. Solove, Introduction: Privacy Self-Management and the Consent Dilemma, 126 HARV. L. REV. 1880, 1880 (2013).

89 More generally, Fair Information Practice Principles (FIPPs) includes notice, access, choice, accuracy, data minimization, security, and accountability. See Shackelford et al., supra note 1, at 441.

90 FED. TRADE COMM’N, PRIVACY ONLINE: FAIR INFORMATION PRACTICES IN THE ELECTRONIC MARKETPLACE: A REPORT TO CONGRESS i, 4 (May 2000), available at https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-fair-information-
notice containing what information is collected, how it is used, and its information disclosure practices.\textsuperscript{91} OSPs must “obtain verifiable parental consent for the collection, use, or disclosure of such personal information from children.”\textsuperscript{92} The parent of a child who supplies personal information must have the right to obtain “a description of the specific types of personal information collected from the child by that operator” and have “the opportunity at any time to refuse to permit the operator’s further use or maintenance . . . or future online collection, of personal information from that child.”\textsuperscript{93} The operator must also provide reasonable means, in the given circumstances, for “the parent to obtain any personal information collected from that child.”\textsuperscript{94} COPPA further prohibits “conditioning a child’s participation in a game, the offering of a prize, or another activity on the child disclosing more personal information than is reasonably necessary to participate in such activity.”\textsuperscript{95} In terms of security, COPPA regulation requires OSPs to “establish and maintain reasonable procedures to protect the confidentiality, security, and integrity of personal information collected from children.”\textsuperscript{96}

To enforce COPPA regulation, the FTC has the authority to create rules and police unfair and deceptive trade practices, which include private companies’ privacy policies.\textsuperscript{97} Consequently, it can issue fines and seek preliminary or permanent injunctive remedies for those who do not comply with COPPA regulation.\textsuperscript{98} While to date most cases have resulted in settlement agreements,\textsuperscript{99}
the FTC reported that from 2000 to 2016 it “brought over 20 COPPA cases and collected millions of dollars in civil penalties.”

COPPA has received much scholarly attention since its inception, but it now extends far beyond regulation for the internet. Being online in 2019 means something different than what it meant back in the late 1990s when COPPA was enacted. Naturally, Congress could not have foreseen the technological developments that might pose new threats to children like that of IoT. Despite these developments, COPPA regulation still governs the datafication of children online. Does COPPA apply to IoToys and other devices within the IoToys market? Are the legal safeguards to protect children’s privacy under COPPA—initially set twenty years ago—still relevant to regulate IoToys? How should policymakers balance the potential benefits of this innovative technology with the dangers they entail for children?

B. Applicability of the Legal Framework

Although crafted long before the emergence of IoToys, COPPA regulation undoubtedly applies on them. These toys generally target children, and most—if not all—should be labeled as targeting children aged under thirteen. Even if the prime audience for some of these toys is arguably older than thirteen, COPPA will still apply when those OSPs knowingly collect personal information from younger children. This second category encompasses gathering any personal information from a child, including the following: (1) “Requesting, prompting, or encouraging a child to submit personal information online; (2) Enabling a child to make personal information publicly available in identifiable form. . . . or (3) Passive tracking of a child online.”


101 While many articles that relate to COPPA are further cited within this Article, here are few examples of such scholarly work: Garber, supra note 69 (discussing the need for privacy with respect to the increase in technology use by children); Solove & Hartzog, supra note 83 (examining the FTC’s privacy law jurisprudence); Joseph A. Zavaletta, COPPA, Kids, Cookies & Chat Rooms: We’re from the Government and We’re Here to Protect Your Children, 17 SANTA CLARA COMPUTER & HIGH TECH. L.J. 249 (2000–2001) (examining the evolution of the need for privacy online); Joshua Warmund, Note, Can COPPA Work? An Analysis of the Parental Consent Measures in the Children’s Online Privacy Protection Act, 11 FORDHAM INTELL. PROP., MEDIA & ENT. L.J. 189 (2000) (analyzing the parental consent measures in COPPA).

102 See 16 C.F.R. § 312.2(1)–(2) (2012).

103 Id. § 312.2(1)–(3). Note, however, that an OSP will not be considered to have collected personal information under the COPPA rule “if it takes reasonable measures to delete all or virtually all personal information from a child’s postings before they are made public and also delete such information from its records.” Id. § 312.2(2).
Children’s data in IoToys easily fall within these definitions. The mere use of IoToys devices that children can talk to should be deemed a way of encouraging the child to submit personal information. To clarify the applicability of COPPA to IoToys, the FTC recently stated clearly that “connected toys or other Internet of Things devices” will be deemed a website or online service for COPPA regulation.

While the IoToys market is rapidly expanding, not all toys raise similar concerns. Smart toys that are not connected to the internet naturally do not raise COPPA-related concerns. Connected toys, while potentially able to trigger COPPA regulation, pose no risks to children’s privacy as long as their ability to collect, retain, and transmit data is relatively low to non-existent, and as long as connecting to them, lawfully or not, cannot generate sensitive information. It might be presumptuous to assume that all IoToys devices trigger COPPA by default, but at least the majority of this market will easily fall under one of COPPA’s categories. For example, audio recordings containing a child’s voice or imagery, if collected by an OSP, would suffice to be deemed personal information under COPPA. In addition, when a device enables recording and transmitting data, it could potentially capture personal data such as the name, home address, online contact information, and even social security numbers of children, and thus might also trigger COPPA.

Having established that COPPA generally applies to IoToys, the next question is whether OSPs comply with their legal obligations. As noted, COPPA regulation necessitates OSPs to meet the following five requirements: “(1) notice; (2) [verifiable] parental consent prior to the collection, use, and/or disclosure of personal information from a child; (3) a right of parental review of such information; (4) proportionality; and (5) reasonable security policies.” To enjoy safe haven from enforcement action under COPPA regulation, companies could also follow self-regulatory guidelines pre-approved by the FTC. As for

104 See id. § 6502(b)(1)(C)–(D).
105 See Children’s Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business, FED. TRADE COMM’N (June 2017), https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance [https://perma.cc/FUG2-FURG]; see also Letter to Senator Warner, supra note 99 (“The COPPA Rule applies not only to websites, but also to other online services, including connected toys and associated mobile apps.”).
106 See 15 U.S.C. § 6502 (regulating collection of only information on the Internet). It should be further clarified that if a toy could connect to another device via Bluetooth, then some privacy risks might also rise, as hackers could potentially gain access to these toys.
107 Id.
110 Ira S. Rubinstein, Privacy and Regulatory Innovation: Moving Beyond Voluntary Codes, 6 I/S: J.L. & POL’y FOR INFO. SOCI’Y 355, 394 (2011) (internal citation omitted).
the latter, without transparency of FTC-approved practices,\footnote{While the FTC announced that it approved applications like the iKeepSafe Safe Harbor Program, it is difficult to assess their practices without transparency. See Letter from Donald S. Clark, Sec’y, Fed. Trade Comm’n, to Marsali S. Hancock, President & CEO, Internet Keep Safe Coal., Application of iKeepSafe Safe Harbor Program for Approval of Its Children’s Online Privacy Protection Rule Safe Harbor Program (Aug. 1, 2014), https://www.ftc.gov/system/files/documents/public_statements/573811/140806ikeepsafeap.pdf [https://perma.cc/4W43-5PU5].} this Article focuses on COPPA’s five general requirements. Each of these is followed by examples of its being satisfied by key market players in the IoTtoys market.\footnote{It should be noted that Hello Barbie is currently certified by the FTC as COPPA compliant under the kidSAFE Seal Program. See infra note 216. Hence, the use of Hello Barbie is not to imply that it does not comply with COPPA regulation, but rather to exemplify the practices of key-market players within each of the five FIPPs within the regulatory framework.}

The first component is notice.\footnote{16 C.F.R. § 312.3(a) (2012).} This form of regulation-by-information is a well-known practice in many markets.\footnote{Omri Ben-Shahar & Carl E. Schneider, The Failure of Mandated Disclosure, 159 U. PA. L. REV. 647, 650 (2011) [hereinafter Ben-Shahar & Schneider, Failure]. Regulation by information refers to a broad type of regulatory mechanisms that rely mostly on the notion that individuals can make more-educated choices when they obtain more information. Id. at 649. Under such regulatory mechanism, the “discloser” gives the “disclosee” information, and thus the latter can make better decisions for him, and likewise reduce the “power” of the former to control the latter. Id. For examples of disclosure requirements set by legislation, see id. at 649–50. For more on regulation through information, see generally OMRI BEN-SHAHAR & CARL E. SCHNEIDER, MORE THAN YOU WANTED TO KNOW: THE FAILURE OF MANDATED DISCLOSURE (2013) [hereinafter BEN-SHAHAR & SCHNEIDER, MORE] (exploring “Digital Natives” in regards to privacy, creativity, cyber-bullying, and online political activism).} Under it, consumers must be apprised of the various implications of using a product they have purchased or a service they registered to.\footnote{See Ben-Shahar & Schneider, Failure, supra note 115, at 649.} As COPPA applies to the internet, regulators require that a notice must be posted on the website.\footnote{15 U.S.C. § 6502(b)(1)(A)(i) (2012).} A link to the notice must be prominent and clearly labeled, and appear on the home or landing page or screen offering services where personal information is collected from

---

There are three key criteria for safe harbor approval. Self-regulatory guidelines must (1) meet or exceed the five statutory requirements identified above; (2) include an ‘effective, mandatory mechanism for the independent assessment of . . . compliance with the guidelines,’ such as random or periodic review of privacy practices conducted by a seal program or third-party; and (3) contain ‘effective incentives’ to ensure compliance with the guidelines such as mandatory public reporting of disciplinary actions, consumer redress, voluntary payments to the government, or referral of violators to the FTC.

children. The notice must include “what information is collected from children by the operator, how the operator uses such information, and the operator’s disclosure practices for such information.” It must also be clear and understandable and in writing, and the OSP must make reasonable efforts to notify parents directly regarding its practices.

Many of the key market players, like ToyTalk, for instance, are found largely to comply with the notice component. ToyTalk posts clear links to its privacy policy and statements on what information is collected, how it is used, and its disclosure practices on both its homepage and the designated webpage for downloading the companion app for both Barbie products. While its evaluation is subjective, it also uses clear and understandable language. Genesis, however, might fulfill this requirement less. Cayla’s homepage currently does not contain such a link. Nor does the App Store, when the designated app is downloaded. Cayla’s privacy policy is only visible after a user goes to the “More” section on the top menu.

---

118 16 C.F.R. § 312.4(d) (“The link must be in close proximity to the requests for information in each such area.”).


120 16 C.F.R. § 312.4(a) (2012) (“Such notice must be clearly and understandably written, complete, and must contain no unrelated, confusing, or contradictory materials.”).

121 See supra notes 122–23.


124 See supra notes 122–23.


127 See Original Cayla, supra note 125.
The second component of COPPA requires verifiable parental consent, namely more than parents’ implied consent, for the collection, use, or disclosure of personal information obtained from children. The parent must receive notice of such use and authorize the “collection, use, or disclosure of the personal information” and must have the option not to consent to disclosure of information to third parties. The steps for verifiable parental consent are vaguely articulated as “any reasonable effort (taking into consideration available technology), including a request for authorization.” There are some exceptions to the consent requirement. For example, if an OSP uses a child’s personal information for internal purposes alone and does not disclose this information, it could obtain consent through the method known as “email plus.” In addition, the FTC could approve other methods that satisfy the parental consent requirement.

What should be deemed a reasonable effort in the IoT realm? Connecting the device, including configuration with the home Wi-Fi, strikes one as insufficient to fulfill this requirement, as COPPA insists on parents’ explicit verifiable consent and lists methods such as a signed letter/form, video chat, or phone call with trained personnel. Currently, parental consent for Barbie

---

130 16 C.F.R. § 312.2 (2012).
131 Id. § 312.5(a)(2).
133 See FED. TRADE COMM’N, supra note 105. Under this method, the OSP sends an email to the parent and has them respond with their consent. Id. The OSP then sends a confirmation to the parent (via email, letter, or phone call). Id. OSPs must also notify the parents how to revoke their consent at any given time. Id.
134 16 C.F.R. § 312.5(b)(3) (2012). Under this safe harbor program, the FTC could determine that the method of the OSP meets the requirements set for verifiable parental consent. See id.
135 See id. § 312.5(b)(2). These methods include:

Requiring a parent, in connection with a monetary transaction, to use a credit card, debit card, or other online payment system that provides notification of each discrete transaction to the primary account holder and verifying a parent’s identity by checking a form of government-issued identification against databases of such information, where the parent’s identification is deleted by the operator from its records promptly after such verification is complete.

Id. § 312.5(b)(2)(ii), (v). If the OSP “does not disclose (as defined by § 312.2) children’s personal information,” it “may use an email coupled with additional steps to provide assurances that the person providing the consent is the parent.” Id. § 312.5(b)(2)(vi) (“Such additional steps include: Sending a confirmatory email to the parent following receipt of consent, or obtaining a postal address or telephone number from the parent and confirming the parent’s consent by letter or telephone call.”). Id.
products is obtained by creating an account and accessing ToyTalk services.\textsuperscript{136} Genesis merely states that using its website or providing it with any information constitutes consent to the “collection, processing, maintenance and transfer of personal information.”\textsuperscript{137} It further states: “If you do not agree to this, please do not use our website or provide us with any information.”\textsuperscript{138} Genesis, however, notes that it “will not knowingly accept any information by any children under the age of [thirteen] without the express permission of their parent and/or guardian.”\textsuperscript{139}

The third step is right of parental review.\textsuperscript{140} At a parent’s request, OSPs are required to provide the following three things: “(1) A description of the specific types or categories of personal information collected from children by the operator;\textsuperscript{141} “(2) The opportunity . . . to refuse . . . further use or future online collection of personal information from that child, and to direct the operator to delete the child’s personal information;\textsuperscript{142} and (3) Grant parents the right to review the collected information.\textsuperscript{143}

For Barbie products, ToyTalk specifies that parents have the right to review or delete any personal information collected from their child that it retains.\textsuperscript{144} Parents also have the “right to review and delete” any audio files in their account and “may also permanently delete their accounts via ToyTalk’s website.”\textsuperscript{145} Even lacking a request, ToyTalk claims that it will delete personal information that children provide when it “becomes aware of it, and [it] will contractually require [its service] providers” to act similarly.\textsuperscript{146} For Cayla, Genesis claims that parents have the right to ask not to process their personal information for marketing purposes, the right to ask to update their records or delete any personal information the company holds about them (but mentions that it “may need to keep that information for legitimate business or legal purposes”), and

\textsuperscript{136} See TOYTALK, Privacy, supra note 54 (“Unless Barbie Products are used only in offline mode, we obtain parental consent for the use of the Service using an approved method under the Children’s Online Privacy Protection Act (‘COPPA’). By creating an account and accessing the Services, you are certifying that you are authorized to provide such consent and responsible for all activities under the account.”).


\textsuperscript{138} Id.

\textsuperscript{139} Id.

\textsuperscript{140} 16 C.F.R. § 312.3(c) (2012).

\textsuperscript{141} Id. § 312.6(a)(1). Examples are “name, address, telephone number, email address, hobbies, and extracurricular activities.” Id.

\textsuperscript{142} Id. § 312.6(a)(2).

\textsuperscript{143} To comply, considering available technology, OSPs must “[e]nsure that the requestor is a parent of that child” and that the means “not be unduly burdensome to the parent.” Id. § 312.6(a)(3)(i)–(ii).

\textsuperscript{144} TOYTALK, FAQ, supra note 60.

\textsuperscript{145} Id.

\textsuperscript{146} Id.
the right to access information it holds about them. Essentially, these
practices comply with the third step of COPPA regulation.

The fourth step requires scrutiny of whether OSPs “condition a child’s
participation in a game, the offering of a prize, or another activity on
the child’s disclosing more personal information than is reasonably necessary to
participate in such activity.” This step might be trickier with respect to IoToys
than to websites. Arguably, regarding toys, almost every activity could be
viewed as imposing conditions and disclosure of data on the child’s
participation. Also, while not all data will be deemed personal information,
many data might. The difficulty in IoToys, however, would be assessing
whether such disclosure is “necessary to participate in such activity,” and more
closely, whether it is reasonable. Practically, without disclosure of the
data mining practices of OSPs and scrutiny of how personal information is
linked to the child’s participation, it is difficult to examine how companies comply
with this requirement.

The final evaluation step is whether OSPs maintain reasonable security
policies. OSPs are obliged to “[e]stablish and maintain reasonable procedures
to protect the confidentiality, security, and integrity of personal information
collected from children.” Releasing the information to a third party requires
ensuring that the third party takes similar steps to protect the data and can vouch
for these measures. To reduce the risk of privacy violations in a cybersecurity
breach, the FTC also imposes on OSPs “[d]ata retention and deletion
requirements.”

Surveys have shown that many IoToys OSPs implement data security
measures in their toys. Barbie products use secure, encrypted
communications when transferring all personal information over the web. Wi-Fi
credentials are stored in an encrypted section so that the products can
connect to the internet. The Hello Barbie Hologram uses 256-bit encryption

\[\text{supra note 33.}^{147}\]
\[16 \text{ C.F.R. } \S 312.3(d) (2012).\]
\[\text{Id. } \S 312.2.\]
\[\text{Id. } \S 312.3(d).\]
\[\text{Id. } \S 312.3(e).\]
\[\text{Id. } \S 312.8; \text{ see also CHILDREN’S CONNECTED TOYS, supra note 57, at 6 (“If the}\]
\[\text{operator transfers children’s personal information to a third party, the operator must also}\]
\[\text{ensure that the third party has taken similar steps to protect the data.”}).\]
\[154 \text{ 16 C.F.R. } \S 312.10 (2012).\]
\[\text{CHILDREN’S CONNECTED TOYS, supra note 57, at 9. These measures include but are}\]
\[\text{not limited to “firewalls; user restrictions, access controls, and authentication procedures;}\]
\[\text{remote access through an encrypted VPN tunnel; monitoring networks for unauthorized}\]
\[\text{activity; regular updates and patches to software; vulnerability testing; and engaging}\]
\[\text{independent security services to test systems for vulnerabilities.” Id.}\]
\[156 \text{ TOYTALK, Privacy, supra note 54.}\]
\[157 \text{ See id.}\]
when it sends queries to the cloud.\(^{158}\) For Cayla, Genesis claims that it undertakes internal reviews of its data management, including “appropriate encryption and physical security measures to guard against unauthorised access to systems where we store personal information.”\(^{159}\)

Are these security policies reasonable? Difficult to say, as it depends on the toy in question.\(^{160}\) But in practice they are found not secure enough: IoToys has often been breached since its inception,\(^{161}\) including Hello Barbie.\(^{162}\) Another problem is that under the current regulatory framework, the reasonableness of the security measures will usually be evaluated ex post, mostly after a data breach.\(^{163}\)

\(^{158}\) See Moynihan, supra note 40. It should be noted that Aristotle was supposed to use encryption to keep at least some form of information private. Aristotle, QUALCOMM (Jan. 3, 2017), https://www.qualcomm.com/media/documents/files/mattel-s-nabi-brand-introduces-first-ever-connected-kids-room-platform-in-tandem-with-microsoft-and-qualcomm.pdf [https://perma.cc/K5Z4-ZZCT]. Mattel claimed that they encrypt every piece of data using AES 256-bit end-to-end symmetric key encryption and create a unique device-to-device key to ensure safety of data streams. \(\text{Id.}\)

\(^{159}\) Privacy Policy, supra note 33.

\(^{160}\) For an analysis of security flaws in IoToys, see Valente & Cardenas, supra note 51, at 19.


breach. A recent example concerns VTech Electronics Limited, an electronic toy manufacturer, which experienced a major cybersecurity breach. Only then did consumers learn that their children’s data was not encrypted even though the firm’s privacy policy stated that it was.

Whether OSPs generally comply with COPPA is disputable. With some exceptions for actions subject to legal interpretation, most of the key market players probably comply with most of COPPA requirements, at least in their narrowest sense. Bearing in mind the FTC’s enforcement prerogative, one would presume that at least the key players will comply with the default requirements of COPPA in the absence of any substantial market failures. Nevertheless, compliance with COPPA does not mean that COPPA in its current form properly safeguards children’s privacy within the realm of IoToys. As the next Part shows, the transition from the internet to IoToys necessitates a reevaluation of COPPA as to whether it is the optimal mechanism to protect children’s privacy online; a recalibration of COPPA in light of IoToys’s challenges is suggested.

IV. REEVALUATING AND RECALIBRATING CHILDREN’S PRIVACY

While it may be disputable whether IoToys OSPs currently comply with COPPA regulation, the broader normative question is whether COPPA regulation adequately meets the challenge of IoToys. This is not to argue that COPPA must be directed towards a specific technology or a sector (unlike a cohort, as currently crafted), but rather that the implications of COPPA—through the examination of new technologies—might suggest broad implications on the perception of American privacy regulation. Accordingly, this Part assesses how to protect children’s privacy in IoToys under the current American framework. The argument proceeds in two stages: the first differentiates regular online activities from activities within the IoToys realm as regards regulating children’s privacy. It maintains that fundamental differences between the two require policymakers to recalibrate the regulatory framework that governs children’s privacy. The second stage offers insights into such recalibration, while revisiting COPPA’s five essential incorporated FIPPs by suggesting practical adjustments to COPPA regulation in the IoToys realm.

164 See id.
165 See id. VTech eventually settled with the FTC and was obliged to pay $650,000 for a COPPA violation. Id.
A. Revisiting Children’s Privacy in IoToys

The common purpose of regulating conduct that relates to both the internet and IoToys is obviously to provide safeguards for children against potential harms, mainly risks to their informational privacy. On the other hand, a one-size-fits-all approach may be inappropriate, as key differences may exist between the internet and IoToys regarding children’s privacy interests. While IoToys depends on the internet, its implications for children’s privacy are not necessarily synonymous with visiting websites.

COPPA was crafted in an era when policymakers sought to protect the privacy of personal information collected from and about children on the World Wide Web.\textsuperscript{166} The need to protect children’s privacy in IoToys not only exists but is actually greater.\textsuperscript{167} It is based on the core differences between the internet and IoT in general, where IoT “increase[s] the number of vulnerabilities that could potentially be exploited to conduct” unlawful activities; it increases the amount of data collected on individuals and thereby increases the chances of privacy violations; and it reduces the capacity to control the vast amount of information.\textsuperscript{168} More closely, IoToys’s design, or stated differently, architecture, affects the volume of data gathered, its potential variety, and access to it.

IoToys broadens the volume of children’s data due to various factors. As a rather intuitive argument, it does so simply by adding another form of connection to the internet. Arguably, however, children might view IoToys devices as substitute goods for websites, that is, essentially they will merely replace data that might have been shared online with data that is shared with the toy. But it is hard to see these two different forms of children’s play as basically the same, as they sometimes perform different functions and might appeal differently at least to some children. The two might offer different types of interaction or play, hence they are unlikely to be considered interchangeable (substitute) goods for all children.

More closely, IoToys expands the volume of data as it widens the target audience by increasing accessibility to it. IoToys shifts the form of communication from writing (typing) to talking, thereby making the toys accessible to a wider cohort of children who are otherwise unable to use a computer or browser, or simply cannot yet read or write.\textsuperscript{169} This relates not only to younger children, but also to other children who experience difficulty writing or reading. These toys offer them increased access to the internet.

\textsuperscript{166} See 16 C.F.R. § 312.1 (2012).
\textsuperscript{167} See Shackelford et al., supra note 1, at 427.
\textsuperscript{168} Id.
\textsuperscript{169} Notably, however, IoToys might be more challenging than the internet for children that experience hearing impairment or speech impediments.
Another factor that increases volume is computer or technological illiteracy. As a core argument, children, at least young ones, might be more accustomed to playing with toys than using a computer; hence, IoToys devices will appeal to them more and be generally easier to use. Notably, however, this argument might become less relevant for digital natives, as the use of computers like smartphones or tablets might begin at relatively early stages of their lives. Still, after the setup step, usually undertaken by the child’s parent, operating IoToys devices like Hello Barbie or Cayla is generally easier and quicker than using the internet via computers. Perhaps IoToys devices might also be more enjoyable, hence, the gamification by itself increases the volume of data.

Volume could also be linked with mobility. Computers are not naturally limited physically to remote rooms of a house, and laptops, mobile phones, tablets, and other potential connected devices can also connect to the internet. Nevertheless, parents might decide to limit their children’s accessing the internet, especially young ones, to a computer that is fairly visible to the parents. IoToys devices’ mobility, however, is different due to the toys’ architecture. They can be used wherever the children want, as long as an internet connection is available. Thus, the mere fact that these devices are generally more mobile than traditional computers can increase children’s access to the internet and increase the volume of gathered data.

Finally, volume of data could also be under parental control—less as regards the physical space than the gathered information. On the internet, parents can sometimes use self-management tools—also known as Privacy-Enhancing

170 Computer illiteracy usually refers to the lack of knowledge and ability a person has to use computers, while technological illiteracy refers to reduced knowledge on the handling and use of technological tools, including computers but also internet use. For further reading on these definitions, see Randall S. Davies, *Understanding Technology Literacy: A Framework for Evaluating Educational Technology Integration*, 55 TECHTRENDS 45, 46–47 (2011).

171 While these definitions evolve over time, “digital natives” generally refers to those who grew-up in the digital age, as opposed to “digital immigrants.” For more on these terms, see Marc Prensky, *Digital Natives, Digital Immigrants Part 1*, 9 ON HORIZON 1, 1 (2001).


173 *See supra* note 27 and accompanying text.
Technologies (PET)—designed to enhance users’ privacy. We also encounter other filtering software as a partial solution to online dangers, indeed, perhaps above all, to limit children’s ability to access websites or provide personal information. While these are far from a perfect solution to regulate children’s online behavior, the IoToys market is more complex. Once a toy is in use, it is difficult for parents to control what their children are doing at any given time if the OSP does not provide them with privacy setting tools. Thus, the ability to control or block access might be more limited without such self-management tools, consequently the volume of the shared data might rise.

Regarding the data’s variety, if the toy seems trustworthy from a child’s perspective, he or she might also share diverse information with it, which might also be more sensitive. Toys in general might seem harmless from a child’s perspective. Children might, for instance, conceive their toy to be their new best friend and form an attachment. Children might even anthropomorphize these toys, that is, become convinced that they are human, which might lure them to disclose data that is sensitive, at least from their own perspective (like secrets). Naturally, however, this aspect could be challenged to the extent that IoToys might also be more limited in the types of gathered data. By this argument, websites could be more diverse in the types of interactions offered, thus could consequently extract a wider variety of data from their users. It could also be further challenged that anthropomorphizing these toys might actually lead to children not trusting them, or rather, telling them lies. Still, along with developments in IoToys devices, their ability to offer more types of interactive

174 See generally Ian Goldberg et al., Privacy-Enhancing Technologies for the Internet, PROCEEDINGS OF IEEE COMPCON ’97 103 (1997) (overviewing PETs). Good examples of PETs are communication anonymizers and Enhanced Privacy ID (EPID), digital signature algorithms supporting anonymity. Other examples include the Platform for Privacy Preferences (P3P) designed to provide “smarter Privacy Tools for the Web.” Platform for Privacy Preferences (P3P) Project, W3C (Oct. 3. 2007), https://www.w3.org/P3P [https://perma.cc/WWF9-BB4X]. Essentially, P3P is a protocol that allows websites to declare their intended use of information they collect. See id. A final example is the TrackMeNot browser plug-in, which “send[s] ‘decoy’ queries to popular search engines . . . whenever a user searches” them while generating “algorithmically generated ‘noise.’” Daniel C. Howe, Surveillance Countermeasures: Expressive Privacy via Obfuscation, INTERARTIVE (June 2016), https://interartive.org/2016/06/surveillance-countermeasures-expressive-privacy-via-obfuscation-daniel-c-howe [https://perma.cc/J29E-Z3JL].


176 See Vlahos, supra note 15. Upon initiation, Hello Barbie explicitly communicates that to the user. Id. Upon asking the child’s name, Hello Barbie replies, “I just know we’re going to be great friends.” Id.

177 See id. Professor Doris Bergen argued that it is very difficult for children, especially young ones, “to distinguish what is real from what is not real.” Id.; see also Woodrow Hartzog, Unfair and Deceptive Robots, 74 MD. L. REV. 785, 787 (2015) (arguing that young children might become attached to robots “acting autonomously” and “disclose secrets that they would not tell their parents or teachers”).
games will not be more limited than websites and will most likely continue to expand.

The final aspect is access to the toy and the stored data. For its evaluation, access should be divided between authorized and unauthorized. In terms of authorized access, the data gathered through websites and IoToys devices should not differ greatly, depending on their marketing purposes. Unauthorized access, however, is generally facilitated in IoToys due to potential security flaws.\(^ {178} \) Indeed, it is difficult to assess the differences between the security of websites and of IoToys in general. On the whole, IoToys and websites could greatly differ in their cybersecurity measures. The difference would mainly be that IoToys’s data storage is divided into three hackable methods to obtain data (through the toy, the app, or the cloud), while websites can rely on a single database.\(^ {179} \) Thus, the insecurity of children’s data in IoToys may be greater simply because there are more ways of obtaining it.

The differences between the volume of data gathered, its potential variety, and access to it imply that IoToys can gather more information than the internet can and that this information might be more sensitive and less secure. These differences could essentially lead to higher risks to children’s privacy. To mitigate these risks within the COPPA framework, policymakers must revisit and recalibrate parents’ self-management of their children’s privacy, the OSP’s requirements, and public enforcement of IoToys.

### B. Recalibrating the Legal Framework

COPPA fails to regulate IoToys properly. While the FTC has amended the COPPA rule and has issued further guidelines for parents as well as OSPs in the IoToys market, regulating IoToys requires acknowledging the differences between it and the internet.\(^ {180} \) Examining the current COPPA requirements in light of these differences clearly shows how inadequate COPPA is to properly safeguard children from privacy risks. This inadequacy must be further addressed by recalibration.

As a general matter, one might argue that the legal framework of sectoral privacy in general is no longer applicable in this age and that the United States should take the path chosen by the European Union and embrace an omnibus privacy regime.\(^ {181} \) One might argue that it is not wise to keep updating laws such as COPPA due to the rise of new technologies, but rather craft technology-

\(^ {178} \) See generally Valente & Cardenas, *supra* note 51 (analyzing IoToys’s security systems).

\(^ {179} \) See id. at 19–21 (mentioning three data entry points).

\(^ {180} \) See *supra* notes 82, 105, and accompanying text.

neutral laws. While such moves could very well be advisable, this Article will not undertake this important theoretical debate but will rather pragmatically focus on the current approach to American privacy and examine its current applicability.

But before suggesting how COPPA should be recalibrated, it is crucial to rule out other potential legal measures currently set in the United States to allay these risks. For instance, the potential constitutional protection of children’s privacy will not advance the discussion on IoToys much. Privacy is often interpreted as a right that could be located within various constitutional amendments such as the Fourth Amendment, but by its present interpretation of the Supreme Court, it will not extend to non-state actors, which include IoToys manufacturers and OSPs, so information privacy will generally not be protected by it. Accordingly, tort law will be fairly limited in dealing with the risks of IoToys as it mainly concerns disclosure of embarrassing personal information and not simply the collection and use of personally identifiable information. Consumer protection law could be invoked to some extent, but it will mainly deal with the IoToys device itself, and less with the practices of safeguarding the stored data, at least on the federal level.

182 For more on technology-neutral legislation, see generally Michael Birnhack, Reverse Engineering Informational Privacy Law, 15 YALE J.L. & TECH. 24 (2012).

183 See U.S. CONST. amend. IV.

184 Joel R. Reidenberg, Setting Standards for Fair Information Practice in the U.S. Private Sector, 80 IOWA L. REV. 497, 502 (1995). As interpreted by the Supreme Court, the Bill of Rights grants implicit constitutional protection for privacy. See, e.g., Roe v. Wade, 410 U.S. 113, 152 (1973); Griswold v. Connecticut, 381 U.S. 479, 484–85 (1964). Examples of this protection include prohibiting unreasonable searches and seizures and protecting freedom of assembly. U.S. CONST. amends. I, IV. Invoking constitutional rights, however, requires that a state action be present. Reidenberg, supra, at 502. Thus, these rights protect citizens against the government, while they fail to grant protection for citizens against each other (including against private companies); see id. at 501–03.

185 See RESTATEMENT (SECOND) OF TORTS § 652 (AM. LAW INST. 1977). As described by Professor William L. Prosser, the right to privacy could be protected to some extent by tort law under four branches: “(1) Intrusion upon the plaintiff’s seclusion or solitude, or into his private affairs; (2) Public disclosure of embarrassing private facts about the plaintiff; (3) Publicity which places the plaintiff in a false light in the public eye; [and] (4) Appropriation, for the defendant’s advantage, of the plaintiff’s name or likeness.” William L. Prosser, Privacy, 48 CALIF. L. REV. 383, 389 (1960). Establishing a tort claim under these branches in IoToys will be difficult in most instances as misappropriation protects only against the unauthorized use of a person’s name or likeness for commercial purposes, Prosser, supra, at 401–07, public disclosure of private facts protects against the circulation to the general public of offensive information (that is not otherwise publicly available), Id. at 392–98, and false light protects against wide dissemination of information that is misleading or erroneous, Id. at 398–401. What might be relevant is intrusion upon seclusion, which protects against highly offensive methods of gathering information in private areas. Id. at 389–92. For more on torts and privacy, see Reidenberg, supra note 184, at 504–06, and Jessica Litman, Information Privacy/Information Property, 52 STAN. L. REV. 1283, 1291 (2000).

186 For more on consumer protection law in the United States, see generally Spencer Weber Waller et al., Consumer Protection in the United States: An Overview, EUR. J.
COPPA regulation is not the sole component of the current regulatory framework that potentially protects children’s privacy from the risks of IoToys. Still, it is highly improbable that other legal measures could be invoked in the IoToys context or be sufficient to protect children’s privacy. An obvious ex ante solution for not only reducing the potential risks of IoToys devices but also removing them altogether would be for policymakers to simply ban their manufacture, import, and even use. This solution might not be as farfetched as it might sound. When Furby was first introduced in 1998, the National Security Agency banned it out of fear that it might record classified conversations.187 In the IoToys market, German authorities embraced this approach recently when they decided to ban the IoToys device Cayla due to its (proclaimed) inherent security flaws.188 Germany’s Federal Network Agency even took this approach a step further and classified Cayla as an “illegal unlicensed radio device,” meaning that parents who possessed this doll might be prosecuted and face up to two-years imprisonment for possessing a banned surveillance device.189

This Article does not support such solutions as an agenda, and they are also highly unlikely in the United States. Beyond the potential benefits to children, IoToys could be valuable for technological developments and innovation.190 This solution might negatively affect the progress of knowledge as flow of information could enhance innovation. Datafication could develop technology for analysis and “business models to utilize the derived information,”191 and it could further “lead to social benefits and the enhancement of social welfare.”192 Thus, heavily regulating the flow of information, let alone banning IoToys devices altogether, could stifle innovation and should be carefully examined.193

Instead of banning IoToys, policymakers should consider other less-restrictive legal measures, which could lessen the risks that IoToys entails while preserving its benefits. To achieve such a balance, policymakers must combine

---


191 Zarsky, supra note 190, at 118.


193 See Zarsky, supra note 190, at 118 n.5, 119.
ex ante and ex post measures, by allowing developments in IoToys, while setting a framework in which these toys operate, are manufactured, and are sold, and especially how, by whom, and for which purposes data are used. Essentially, COPPA regulation attempts to do precisely this, but as previously mentioned, it requires far-reaching modifications to its requirements.

1. Raising Awareness

Any legal guardian, even without purchasing IoToys devices, must be aware of their potential implications. They must certainly understand the risks of IoToys to information privacy and security by understanding the information the OSP collects, “how that information will be used,” “whether it will be shared,” and if so with whom, and “how long the information will be retained.”194 Parents and guardians must assume a position enabling them to make educated decisions regarding their children’s privacy. They have to be aware of these toys’ implications, as their children might also become secondary users, namely by playing with an IoToys device without their parents’ knowledge or consent.195

Awareness can be promoted in various ways. One way is to reduce information gaps through regulation-by-information. Under this regulatory approach, toy manufacturers and OSPs will be obliged to apprise consumers of IoToys’s privacy risks, thereby reducing the disclosers’ power to control the disclosees by granting them informed choice on whether to use these

---

194 See CHILDREN’S CONNECTED TOYS, supra note 57, at 2.
195 The notions of awareness and consent in IoToys might be also perceived as tricky due to secondary users. What happens, for instance, when a child uses his friend’s IoToys device, consented for use only by the parent of the friend? Indeed, a class action revolving secondary users in Hello Barbie was filed against ToyTalk, Inc. and Mattel in the California Superior Court. The class action alleged, inter alia, that OSPs violated COPPA as the IoToys device captured the voices of other children whose parents had not consented (Hello Barbie recorded conversations of the plaintiff while attending a friend’s birthday party). Notice of Removal at 1, 2, Archer-Hayes v. Toytalk, Inc., No. 2:16-cv-02111-JAK-PLA (C.D. Cal. Mar. 29, 2016). From a legal certainty perspective, this case was unfortunately voluntarily dismissed, leaving void the applicability to secondary use within IoToys. See Stipulation of Voluntary Dismissal with Prejudice at 1, Archer-Hayes v. Toytalk, Inc., No. 2:16-cv-2111-JAK-PLA (C.D. Cal. July 22, 2016). It is generally still unclear whether a secondary use of an IoToys device will be deemed as personal identifiable information under COPPA, as an unnamed and unidentified voice is not necessarily “personal information” (unlike the child who owns the toy). Practically, if we take ToyTalk’s privacy policy as an example, allowing other people to use the service via their account is considered a confirmation of the right to consent on their behalf to ToyTalk’s collection, use, and disclosure of their personal information. Alex B. Lipton, Note, Privacy Protections for Secondary Users of Communications-Capturing Technologies, 91 N.Y.U. L. REV. 396, 406 (2016) (“By allowing other people to use the Service via your account, you are confirming that you have the right to consent on their behalf to ToyTalk’s collection, use, and disclosure of their personal information as described below.” (quoting Privacy Policy Terms of Use FAQ, TOYTALK, https://toytalk.com/hellobarbie/privacy/ [https://perma.cc/A6XC-59SM]).
products. While COPPA promotes this type of regulation by its notice requirement, it generates insufficient awareness regarding IoToys, as it fails to acknowledge the difference between using a website and playing with a toy. Merely placing a notice on a website will hardly raise awareness. When the internet is embedded in the operation of devices, direct exposure to a website does not exist, even if OSPs maintain one. Thus, the existence of a notice in a website regarding the collection, retention and use of information does little in itself to detail the rationale behind the notice requirement. The notice must appear on the toy’s packaging and on online platforms like the app that is used to set up the toy. But on its own, this requirement is still insufficient to properly raise awareness.

One of the main problems of the notice requirement in terms of awareness concerns the known practice of confusing users with long and incomprehensible policies. Regarding IoToys, the FBI advises parents to carefully read disclosures and privacy policies. But practice shows that this is unlikely to occur. As may be drawn from terms of service (ToS) agreements and end-user license agreements (EULAs), most consumers do not bother to read them and they are usually long, broad and written in a legal language almost incomprehensible to most people, as are privacy policies or notices. Most

196 See generally Ben-Shahar & Schneider, supra note 115 (arguing that mandated disclosures are ineffective); Ben-Shahar & Schneider, Failure, supra note 115 (discussing the historical use of mandated disclosures).

197 16 C.F.R. § 312.3(a) (2012).


200 The use of ToS and EULAs are merely to exemplify how individuals treat vast amounts of information online. It should be stressed that this Article does not argue that these agreements are similar to privacy policies. While terms of use are the province of contract law, privacy policies seem currently to be mainly the province of the FTC. See Solove & Hartzog, supra note 83, at 589. For attempts to enforce privacy policies as contracts, see, for example, In re JetBlue Airways Corp. Privacy Litig., 379 F. Supp. 2d 299, 316–18 (E.D.N.Y. 2005); Dyer v. Nw. Airlines Corps., 334 F. Supp. 2d 1196, 1199–1200 (D.N.D. 2004).

201 See Paul Ohm, Branding Privacy, 97 MINN. L. REV. 907, 930 (2013); Ben-Shahar & Schneider, Failure, supra note 115, at 665–78; Solove, supra note 88, at 1885.


203 For studies on privacy notices, see, for example, NISSENBAUM, supra note 77, at 105; Annie I. Anton et al., Financial Privacy Policies and the Need for Standardization, 2 IEEE SECURITY & PRIVACY 36, 42–44 (2004); Aleecia McDonald & Lorrie Faith Cranor, The Cost of Reading Privacy Policies, 4 I/S: J. L. & POL’Y FOR INFO. SOC’Y 543 (2008); George R. Milne & Mary J. Culnan, Strategies for Reducing Online Privacy Risks: Why Consumers Read (or Don’t Read) Online Privacy Notices, 18 J. INTERACTIVE MARKETING 15, 20–21 (2004); Aaron Smith, Half of Online Americans Don’t Know What a Privacy Policy Is, PEW
people do not see, read or understand them, and they might also be changed frequently.\textsuperscript{204} Even shortening these policies might only insert marginal improvements to make them more comprehensible,\textsuperscript{205} and they might also leave out important information to make any consent truly informed.\textsuperscript{206} Essentially, individuals already experience information flooding and are unlikely to spend time or effort on reading these policies.\textsuperscript{207}

Even if parents do receive full information on IoToys practices, privacy self-management—at least in its current form—is insufficient to raise awareness efficiently.\textsuperscript{208} It is beset with cognitive failures and structural problems such as impediments to the parents’ ability to adequately assess the costs and benefits of the information they receive.\textsuperscript{209} Thus, information is generally substantially insufficient to reduce these risks. Cognitive abilities are required to understand something that may be highly complex in terms of informational privacy.

Within this regulatory framework, at the very least COPPA must be more precise. Assuming that the policy of these OSPs permits collection and sharing of information, they must be obliged to be concise and clear on how information is used and by whom.\textsuperscript{210} A clear and understandable notice on how OSPs use


\textsuperscript{204} Joel R. Reidenberg et al., \textit{Privacy Harms and the Effectiveness of the Notice and Choice Framework}, 11 I/S: J.L. & POL’Y FOR INFO. SOC’Y 485, 491 (2015); accord LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE 160 (1999) (“No one has the time or patience to read through cumbersome documents describing obscure rules for controlling data.”); Ohm, \textit{supra} note 201, at 930; Solove, \textit{supra} note 88, at 1885.

\textsuperscript{205} See, e.g., M. Ryan Calo, \textit{Against Notice Skepticism in Privacy (and Elsewhere)}, 87 NOTRE DAME L. REV. 1027, 1032–33 (2012).

\textsuperscript{206} See Solove, \textit{supra} note 88, at 1885.


\textsuperscript{208} See Solove, \textit{supra} note 88, at 1883–93.

\textsuperscript{209} As suggested by Professor Daniel Solove, cognitive problems arise from four aspects:

(1) [P]eople do not read privacy policies; (2) if people read them, they do not understand them, (3) if people read them, they often lack enough background knowledge to make an informed choice; and (4) if people read them, understand them, and can make an informed choice, their choice might be skewed by various decisionmaking difficulties.

\textit{Id}. at 1888.

\textsuperscript{210} It should be insufficient to declare that information might be shared “with third-parties” without listing who these third-parties are and what the purpose of this information sharing is. For more on the problem of vagueness, see Reidenberg et al., \textit{supra} note 204, at 518–19. Relating to their smart bear toy, Fisher-Price mentions on their website that “NO PERSONALLY IDENTIFIABLE DATA is transmitted by Smart Toy.” Yadron, \textit{supra} note 161 (describing how the toy was able to be hacked, revealing personal information about users).
such information,\textsuperscript{211} and their disclosure practices, must be prominently visible to anyone purchasing the toy; also, parents should be reminded of these matters periodically by accessible communication means such as email. The notice must explicitly spell out the potential risks to users when agreeing to the policy.\textsuperscript{212} Any vendor of these toys must first make sure that parents understand the risks, and what they are consenting to, at the point of sale.\textsuperscript{213}

Furthermore, sellers should be obliged to place simplified and clear privacy labels on the package.\textsuperscript{214} Beyond lucid warnings on IoToys devices’ packaging, it would be efficient to clearly signal how the toys protect privacy and comply with COPPA. Under this program, OSPs that implement sufficient measures to protect children’s privacy should be encouraged to display a privacy seal on the toy. This solution exists in the market, as toys can be certified “COPPA compliant” by the FTC or other organizations, for example, by the kidSAFE Seal Program—a children’s privacy certification program approved by the FTC.\textsuperscript{215} Hello Barbie is currently a member of such a program.\textsuperscript{216} While not perfect, seal programs are generally an efficient method to alert consumers to the potential risks of IoToys devices that do not have such a seal.\textsuperscript{217}

\begin{itemize}
\item \textsuperscript{211} The United States Senate Committee on Commerce, Science, and Transportation advised the FTC to suggest that toymakers will be required to “use clear, plain language to inform parents about the information the toys collect and how that information is used.” \textsc{Children’s Connected Toys, supra} note 57, at 2.
\item \textsuperscript{212} See Steinberg, \textit{supra} note 28; see also \textsc{Children’s Connected Toys, supra} note 57, at 15 (“Toymakers should also disclose in plain language the information that is collected from or about a child instead of burying it in their privacy policies.”); cf. Lobosco, \textit{supra} note 12 (quoting a Mattel spokeswoman that Hello Barbie conforms to COPPA).
\item \textsuperscript{213} See \textsc{Kids & The Connected Home, supra} note 4, at 13.
\item \textsuperscript{214} See Steinberg, \textit{supra} note 28; see also \textsc{Children’s Connected Toys, supra} note 57, at 15 (suggesting that providing the basics of what information is collected and how it is used conspicuously and in clear terms on a toy’s packaging would allow parents to be more informed about their children’s privacy and security).
\item \textsuperscript{215} The kidSAFE Seal Program is designed for children-friendly websites and technologies, including “online game sites, educational services, virtual worlds, social networks, mobile apps, tablet devices, connected toys, and other similar online and interactive services.” The service includes a list of products that meet their online safety and/or privacy standards. \textsc{About Our Program, Samet Privacy, LLC, kidSAFE\textsuperscript{®} Seal Program, \url{https://www.kidsafeseal.com/aboutourprogram.html}} [https://perma.cc/H3LX-RRLR]. One of the seals is an FTC-approved COPPA certification program called the “kidSAFE+ COPPA” seal. Beyond basic safety rules, this seal has six additional requirements: “Neutral age questions, Parental notice and consent procedures, Parental access to child’s personal information, Data integrity and security procedures, COPPA-compliant privacy policy, [and] COPPA oversight and enforcement by the kidSAFE\textsuperscript{®} Seal Program.” \textsc{About Our Seals, Samet Privacy, LLC, kidSAFE\textsuperscript{®} Seal Program, \url{https://www.kidsafeseal.com/aboutourseals.html}} [https://perma.cc/82HW-4VBR].
\item \textsuperscript{216} \textsc{Official Membership Page, Samet Privacy, LLC, kidSAFE\textsuperscript{®} Seal Program, \url{http://www.kidsafeseal.com/certifiedproducts/toytalk_hellobarbie_device.html}} [https://perma.cc/4LF8-4W7D] (noting that Hello Barbie is kidSAFE+ COPPA certified).
\item \textsuperscript{217} Compare with TRUSTe, a nonprofit organization, “the first online privacy seal program” in the United States. \textsc{Fed. Trade Comm’n, supra} note 90, at 6; Hertzel, \textit{supra} note
promote consumer trust, thereby persuading consumers to purchase only IoToys devices that meet FTC standards.

The state, too, should promote awareness. Policymakers must invest in heightening awareness of the potential implications of IoToys. As previously noted, it is crucial for all legal guardians to understand the ramifications of playing with an IoToys device, as their children might become secondary users.\(^2\) The state should therefore invest in advertisements and other forms of education that clearly explain their potential risks.\(^2\) One such effort that could be improved is the FBI’s consumer notice for internet-connected toys, which warns of potential risks to children’s privacy.\(^2\) While important, the FBI’s suggested steps are unlikely be taken by average parents, even if they are exposed to the warnings.\(^2\) Thus, raising awareness must be more meaningful and use practical forms of communication to advise the general public on the privacy risks of IoToys. Still, even awareness will be fairly limited to properly regulate IoToys.

**2. Redefining Choice**

Being alerted to and comprehending the risks, parents should be able to decide whether to consent to the practices that IoToys entails. COPPA currently promotes exercising “verifiable parental consent.”\(^2\) Generally, this form of privacy self-management is insufficient for IoToys.\(^2\) The efficacy of a notice and choice mechanism has largely been contested because, inter alia, it can uninform or misinform consumers,\(^2\) it is “impractical” and ineffective,\(^2\) and

\(^2\) See supra note 195.
\(^2\) See *Public Service Announcement*, supra note 199 (advising parents to take steps to protect their children’s privacy).
\(^2\) See Solove, supra note 88, at 1884.
\(^2\) 16 C.F.R. §§ 312.3(b), 312.5 (2012).
\(^2\) For a comprehensive review of the efficacy of notice and choice frameworks, see Reidenberg et al., supra note 204, at 489–97. For criticism on the efficacy of the notice and choice mechanism to regulate information privacy, see generally Fred H. Cate, *Protecting Privacy in Health Research: The Limits of Individual Choice*, 98 CALIF. L. REV. 1765 (2010).
\(^2\) Users are “uninformed—or misinformed, as people rarely see, read, or understand privacy policies.” Reidenberg et al., supra note 204, at 491.
\(^2\) The notice and choice mechanism is considered impractical due to the amount of privacy policies online (which might also change from time to time), users’ lack of knowledge of how third parties use data, users’ inability to understand the effects of future aggregation of their data, and how users suffer from “bounded rationality and cognitive biases.” Id. at 492–94 (quoting Ohm, supra note 201, at 931).
it creates undesirable externalities. Generally, individuals make incorrect assumptions on how their privacy is protected and misconceive of how the data are used; many lack expertise in assessing the consequences of consent.

If we accept consent as a proper form of regulation, policymakers must acknowledge that consent deals with IoT devices insufficiency in its current form. Due to the potential risks of IoT devices, regulators must require OSPs to do more than merely make “reasonable efforts” to obtain such consent. Verification of parental consent must cross a higher threshold than that which COPPA currently sets. Methods of obtaining verifiable parental consent should necessitate parents actively calling or video-conferencing trained personnel who could assess if they understand the policy to which they are consenting.

Policymakers could also oblige companies to delimit choice of privacy preferences. They can set various restrictions on consent to data collection and retention, such as an obligatory opt-in mechanism, where by default, companies do not collect data from toys and do so only upon enabling such an option. They could also reverse the choice and notice mechanism default so that consumers are obliged to signal their privacy preferences to the information collectors, not the reverse. They could also oblige companies to offer consumers a choice between more costly services that protect their privacy and cheaper services that protect it less.

3. Data Minimization and Transparency

COPPA currently requires data minimization through proportionality and necessity. It prohibits conditioning a child’s online activity on the child’s disclosure of more personal information than is reasonably necessary for participation in such activity. While this requirement requires OSPs to collect...
only data that are necessary for the purposes for which they are collected, without proper transparency, it is extremely difficult to assess their datamining practices, data retention, and data transfers to third parties.

COPPA must be much more precise on data minimization. The use of vague language for keeping recordings on the merits of “data analysis purposes” should not qualify as fulfilling this requirement. Policymakers must oblige companies to limit their data collection to what is required for the toy’s core functions. While defining core functions might not be easy, especially for IoToys devices that depend on advanced computational skills like machine learning, the default should still be set at no data collection unless these OSPs prove to the FTC that it is essential for the core functions of the toy.

Accordingly, policymakers should set limits on data retention and data sharing. Even if OSPs allow parents to change the privacy settings of IoToys devices, on its own this would be insufficient to mitigate IoToys’ risks. Currently, COPPA requires that an OSP retain personal information “only as long as is reasonably necessary to fulfill the purpose for which the information was collected.” Policymakers must clarify this vague current requirement. OSPs must be obliged to clarify to consumers how long data is stored and when it will be deleted. As for data sharing, OSPs should not be allowed to share data with any third party unless the OSP proves that it has full control of how that data is used and an ability to delete it when necessary.

Clearly, ensuring that OSPs comply with the data minimization requirements necessitates some form of oversight. Transparently explaining the need for data use might not be easy. OSPs might have to disclose trade secrets, and even if they do not, they might not know beforehand what data will be needed in the future. These difficulties, however, do not completely rule out oversight measures. The obvious candidate to perform such oversight is the FTC; it could examine OSPs’ practices, under secrecy if needed, and decide whether they comply with COPPA requirements. The Senate Committee on Commerce, Science, and Transportation actually suggested FTC monitoring of the connected toy space and exercising authority when appropriate. This

233 See, e.g., TOYTALK, Privacy, supra note 54.
235 CHILDREN’S CONNECTED TOYS, supra note 57, at 2; McReynolds et al., supra note 234.
236 Although a Senate committee report recommends for the FTC to advise parents to change the privacy settings of the toy to limit the amount of personal information that the toy collects and transmits and allow the toy to collect only information necessary for the toy to properly function, it might not be within the toy’s options. See CHILDREN’S CONNECTED TOYS, supra note 57, at 2.
238 CHILDREN’S CONNECTED TOYS, supra note 57, at 16.
oversight, however, must also be implemented carefully, as it grants a state agent surveillance powers over individuals; as history shows, these powers can be misused by the state.239 It would be wiser to invest a non-state data protection authority with such oversight powers.

4. Toy and Information Security

Properly securing the obtained data is naturally critical for safeguarding children’s privacy. COPPA currently requires OSPs to maintain reasonable security policies.240 The Senate Committee on Commerce, Science, and Transportation Office of Oversight and Investigations’s advice to parents to strengthen their passwords and frequently update the toy’s software,241 while important, is still insufficient for data security. This requirement must be clarified and recalibrated, as it does not greatly advance IoToys’s security levels.

Prior to such recommendations, one may at least presume that legal intervention might not be needed when market players possess high incentives to secure their products and services.242 Arguably, low security measures and data breaches could result in damage to toymakers’ reputations and monetary losses from fines, lawsuits, or simply losing customers. The state, in fact, encourages parents to respond actively to IoToys’s security measures. The Senate Committee on Commerce, Science, and Transportation Office of Oversight and Investigations advises parents to examine companies’ prior history of security breaches.243 The FBI has further recommended that parents examine “the toy’s Internet and device connection security measures” and probe “any known reported security issues,” “use toys in environments with trusted and secured Wi-Fi Internet access,” “[r]esearch where user data is stored . . . and whether any publicly available reporting exists on their reputation and [stance on] cyber security,” and “[e]nsure the toy is turned off . . . when not in use.”244

Prima facie, IoToys manufacturers and OSPs would wish to invest in measures to protect their products, services, reputation, share price, and customers from harm. As this market-based approach suggests, with proper incentives, the modality of law is not needed—absent substantial market failures.

239 For more on surveillance in the digital age, see generally BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD (2015); Niva Elkin-Koren & Eldar Haber, Governance by Proxy: Cyber Challenges to Civil Liberties, 82 BROOK. L. REV. 105 (2016).
240 16 C.F.R. §§ 312.3(e), 312.8 (2012).
241 CHILDREN’S CONNECTED TOYS, supra note 57, at 2, 16.
242 This assumption is often attributed to Adam Smith’s coining of the “invisible hand,” i.e., that market players acting in their own self-interest will react to demand, which reflects the preferences of members of society and thus promotes the social good. See ADAM SMITH, AN INQUIRY INTO THE NATURE AND CAUSES OF THE WEALTH OF NATIONS (Sálvio Marcelo Soares ed., 4th ed. 2007) (1776).
243 See CHILDREN’S CONNECTED TOYS, supra note 57, at 2, 15 (recommending FTC advice to parents).
244 FED. BUREAU OF INVESTIGATION, supra note 199.
that would prevent the market from reaching its anticipated equilibrium point. But as shown next, while the market as a modality to regulate cybersecurity could be an important component of any solution,\textsuperscript{245} it is insufficient on its own to regulate IoToys properly due to the existence of market failures.

First, the market-based approach’s reliance on consumers’ discontent with security measures is due to failures. It presumes no cognitive failures, no information gaps, and the presence of expertise to evaluate security measures properly. Even if the state adds regulatory requirements of disclosure like security standards or data breach notifications\textsuperscript{246} to reduce information gaps—commonly termed the regulation through disclosure approach\textsuperscript{247}—this will not necessarily lead to a market response.\textsuperscript{248} It might be too vague for consumers to fully understand because of the aforementioned cognitive biases or simply not be fully comprehensible without substantial expertise in cybersecurity.

In addition, consumers may lack the ability to indicate their discontent with cybersecurity measures in the IoToys market as it is not fully competitive. This market currently operates with limited competition—controlled by key market players like Mattel and ToyTalk. Their products and services are not necessarily similar to their competitors’, hence are not fully substitutive. From a child’s perspective, it is fairly intuitive that not all children will view Hello Barbie as equivalent to Cayla. So without a fully competitive market it is difficult to assume that consumers could markedly alter these companies’ security policies.\textsuperscript{249} Notably, however, IoToys devices are certainly not a necessity, and parents’ discontent could be realized simply by their not purchasing any IoToys device.

As the market in itself will be insufficient to promote optimal cybersecurity measures, legal intervention is most likely required. Recalibration of COPPA must begin by expanding beyond maintaining reasonable procedures to protect the confidentiality, security and integrity of personal information collected from

\textsuperscript{245} Professor Lawrence Lessig suggested four modalities that could regulate behavior: market, social norms, technology (code), and law. \textsc{Lawrence Lessig, Code: Version 2.0} 120–37 (2006); \textit{see also} \textsc{Lawrence Lessig, Free Culture} 116–73 (2004).

\textsuperscript{246} Data breach notifications statues in the United States are currently state legislated and usually require private and government entities to notify individuals of security breaches of information involving personally identifiable information with notable exceptions like encrypted data. \textit{See} David Thaw, \textit{The Efficacy of Cybersecurity Regulation}, 30 GA. ST. U. L. REV. 287, 297 (2014).


\textsuperscript{249} \textit{See, e.g.}, Nathan Alexander Sales, \textit{Regulating Cyber-Security}, 107 NW. U. L. REV. 1503, 1517 (2013) (“[S]trategically significant firms in uncompetitive markets are less likely to adequately invest in cyber-security than ordinary firms in competitive markets.”).
children. Policymakers must set a higher threshold than “reasonable” and demand that toy manufacturers and OSPs comply with high security standards for the IoToys device and the stored data. They must establish security standards that OSPs and third parties must meet to be able to collect and retain data. These measures must also address the threat of real-time interception of data, not merely its collection and storage. OSPs must be obliged to use cutting-edge security measures that will stop—or at least substantially reduce—the possibility of hacking the toy and the stored data.

Inter alia, these measures might include requirements to meet predetermined security standards, conduct security audits, implement bug bounty programs, use strong encryption standards, and actively update security measures. The Senate Committee on Commerce, Science, and Transportation Office of Oversight and Investigations has in fact suggested that toymakers build in effective security from the start. These suggestions should become obligatory, but also be further clarified. Policymakers must clarify exactly what robust security means and make sure that companies are subjected to periodic external audits as part of the suggested oversight. Beyond the use of strong encryption, they should incentivize toymakers to implement anonymization measures, differential privacy, and any other PET tools as long as the FTC can verify their applicability to safeguarding children’s privacy.

251 See KIDS & THE CONNECTED HOME, supra note 4, at 15; CHILDREN’S CONNECTED TOYS, supra note 57, at 2.
252 See CHILDREN’S CONNECTED TOYS, supra note 57, at 15.
253 Realizing that speech recognition must obtain large quantities of data to improve, regulators could allow data collection and retention only when children are not linked with the data after its processing. That would mean that the data could still exist, but linking it to a specific user would be highly difficult. Notably, at least one IoToys OSP declares that it anonymizes the data and further ensures it is stored in multiple different places. See Sara Sorcher, The Internet of Toys Raises New Privacy and Security Concerns for Families, CHRISTIAN SCI. MONITOR: PASSCODE (July 22, 2016), https://www.csmonitor.com/World/Passcode/2016/0722/The-Internet-of-Toys-raises-new-privacy-and-security-concerns-for-families [https://perma.cc/AZY4-QU22] (reporting that Elemental Path, which makes a talking dinosaur toy, says it works to anonymize data, while other companies do not).
254 Differential privacy relates to a method by which noise is added systematically to results of data queries so “no single person’s inclusion or exclusion from the database can significantly affect the results of queries.” Jane Bambauer et al., Fool’s Gold: An Illustrated Critique of Differential Privacy, 16 Vand. J. Ent. & Tech. L. 701, 703 (2014). Using differential privacy correctly should assure that no user could infer anything about another user. Id. For an analysis and critique of differential privacy, see id.
255 See, e.g., Platform for Privacy Preferences (P3P) Project, supra note 174 (detailing a PET that allows companies to “express their privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents”).
5. Effective Enforcement

The FTC’s option to sanction COPPA violations is in itself insufficient to be considered effective enforcement. The FTC must be more involved in *ex ante* and *ex post* enforcement practices. From an *ex ante* perspective, the FTC must closely oversee the implementation of privacy policies in practice, and not merely rely on OSPs’ statements. This became evident with the data breach of VTech: the FTC learned *ex post* that the company did not comply with its own privacy policy, which falsely stated that it used encryption when in fact it did not encrypt any information. Even without adhering to direct oversight, at the very least the FTC must investigate and rectify instances where reporters show that an IoToys device is not secure enough. They must use reliable mechanisms to provide substantial sanctions against noncompliance with regulations or simply not approve marketing or sale on the grounds of children’s safety.

These measures must be complemented with *ex post* measures such as imposing steep fines as a potential deterrent. True, the effect of deterrence might be disputable in general; nonetheless, the FTC should exercise its vested powers of enforcement to impose the highest fines possible. Sanctioning companies like VTech to the tune of $650,000 for a substantive data breach is unlikely to advance the deterrence rationale, considering its $689.4 million gross profits in 2017. OSPs must not see fines as costs of doing business and

---

256 The FTC acknowledged this ability to effectively enforce COPPA as a critical component to protecting privacy online. See *Fed. Trade Comm’n*, *supra* note 90, at i.

257 See *Electronic Toy Maker VTech Settles FTC Allegations That It Violated Children’s Privacy Law and the FTC Act*, *supra* note 163.


261 The FTC fines are often quite low in relation to the gravity of the violations and the overall net profit of the violators. Nevertheless, COPPA violations sometimes draw rather large fines, ranging from $250,000 to $3,000,000. Solove & Hartzog, *supra* note 83, at 605, 647.

262 See *Electronic Toy Maker VTech Settles FTC Allegations That It Violated Children’s Privacy Law and the FTC Act*, *supra* note 163.

should reflect further on the gravity of poor security measures. Policymakers should thus implant in the FTC more substantial regulatory teeth. This would enable the Commission’s fines not merely to reflect the level of consumer loss but rather to sanction violations, with fines as percentages of annual global turnover.\footnote{This approach was recently chosen by the European Union in its General Data Protection Regulation (GDPR). \textit{See} Regulation 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, Art. 83, 2016 O.J. (L 119) 1.} If the FTC continues to act as a data protection authority, policymakers must further invest in and expand the purview of the Division of Privacy and Identity Protection—the body devoted to privacy issues—to issuing high fines and conducting meaningful oversight of OSP practices.\footnote{See Solove & Hartzog, \textit{supra} note 83, at 600–01 (noting that the FTC’s staff devoted to privacy issues is relatively small).}

Legal intervention is thus greatly needed to better secure informational privacy of children in the IoToys market. COPPA regulation must frequently be updated to better address the risks that IoToys entails, and frequently revisited in view of technological changes that could affect the risks in these toys. For example, the future IoToys market might expand the current children-to-toy interaction to children-to-children. If, for instance, Hello Barbies begin exchanging information, children might also be exposed to harassment in the form of cyberbullying, along with further dangers to their privacy.\footnote{See Kay Mathiesen, \textit{The Internet, Children, and Privacy: The Case Against Parental Monitoring}, 15 ETHICS & INFO. TECH. 263, 263 (2013) (describing children’s privacy risks on the internet).}

All in all, COPPA should become more oriented to the privacy risks of IoToys, and policymakers must not presume that the potential risks to children’s privacy from being online do not change over time. Children’s privacy must be taken more seriously, and the ways technological developments could negatively affect it must be acknowledged. If an IoToys device increases the risks to children’s privacy, parents must also become more involved in safeguarding their children.\footnote{McReynolds et al., \textit{supra} note 234.} Their involvement, however, should not be treated lightly, as it bears on important normative questions that must be further addressed: what are the implications of the tradeoff between children’s security and children’s privacy—or stated differently—between parents’ empowerment and children’s protection?\footnote{See Milda Macenaite, \textit{From Universal Towards Child-Specific Protection of the Right to Privacy Online: Dilemmas in the EU General Data Protection Regulation}, 19 NEW MEDIA & SOC’Y 765, 766 (2017) (discussing the “empowerment versus protection” dilemma in child rights debates).} More particularly, should children’s right to privacy be viewed only as a right from third-parties or also from their parents?\footnote{See id.} In other words, how can we ensure children’s privacy outside their...
household but also not completely abolish it within what they view as their safe place?

V. TAKING CHILDREN’S PRIVACY SERIOUSLY

Parents have the responsibility to safeguard their offspring from dangers. They must make decisions regarding various aspects of their children’s lives, especially their health, development, and safety. To do so, parents might oblige children, inter alia, to “play in rubber-cushioned playgrounds, use sanitizing gel, sit in car seats, and wear helmets and kneepads while riding their bicycles.” 270 They might also become closely involved in their lives and even use sensors and monitors to assure their safety.271 While parents might always have been involved in their children’s lives to some extent, researchers have witnessed an increase in parents’ involvement since the mid-1980s. To date, it has developed into a phenomenon dubbed helicopter parenting, smothering mothering, or child-centered parenting, among other proposed names.272 Essentially, children today are probably “the most watched over generation” in history.273

The notion that parents nowadays should be more protective could be important and perhaps challenged—but nonetheless beyond the scope of this Article. The purpose of this part is rather modest. It seeks to identify how the regulatory framework that governs IoToys subjects children to this form of parenting and even takes it a step farther than the regulation of online activities through websites. It discusses the tension between children’s protective rights, like the right to be safeguarded from harms, and their participatory rights to make decisions.274 It also further seeks to discuss the privacy protection paradox, 275 namely that children’s privacy cannot be safeguarded properly when parents obtain tools—that IoToys makers are encouraged to provide—to constantly spy on them, when the rationale behind such tools is outside the regulatory framework.

---

271 Id.
272 This phenomenon generally describes parents that are “obsessed with their children’s success and safety [and] vigilantly hover over them, sheltering them from mistakes, disappointment, or risks.” Kathleen Vinson, Hovering Too Close: The Ramifications of Helicopter Parenting in Higher Education, 29 GA. ST. U. L. REV. 423, 424–25 (2013). It had also been characterized, inter alia, as “‘invasive parenting’, ‘overparenting,’ ‘aggressive parenting,’ ‘ modem parenting,’ and ‘snowplow parenting.’” Id. at 424 n.4 (citing Nancy Gibbs, The Growing Backlash Against Overparenting, TIME (Nov. 20, 2009)); Bernstein & Triger, supra note 270, at 1225; Lisa Belkin, Let the Kid Be, N.Y. TIMES MAG. (May 29, 2009), https://www.nytimes.com/2009/05/31/magazine/31wwln-lede-t.html [https://perma.cc/EYX4-SY6R].
273 See Neil Howe & William Strauss, Millennials Rising 9 (2000) (arguing that the millennials’ generation is “the most watched over generation in memory”).
274 See Macenaite, supra note 268, at 766–67.
275 See The Protection of Children Online, supra note 49, at 37.
A. Parenting in the IoToys Era

Parenting generally involves a balance of risk management.276 Many parents might view good or responsible parenting as being all-knowing, which requires them to monitor their children’s behavior.277 They might monitor their children even before birth, using ultrasound screening to detect fetal anomalies, see their unborn baby’s movements, and hear its sounds.278 After birth, parents will often monitor their children’s behavior and development directly, by watching and listening to them, or indirectly, by means of technology, such as wearable devices and various types of sensors and monitors.279 Parents might even monitor their children when another caregiver is present by using, inter alia, cameras hidden inside another object (“nanny cams”).280 When their children are old enough to interact with the digital world, parents might monitor their conduct by various methods. Parents’ consent to their children using the internet, for instance, might require imposing rules and restrictions such as placing the computer in a shared space281 or obliging their children to share the content of their conversations and even their usernames and passwords.282 Parents might also embrace social approaches, like by educating children to share what they are doing or by using technical tools like monitoring software.283 Essentially, many parents will attempt to strengthen their control and track almost everything their children do offline and online.284

It is generally uncontested that keeping an eye on children, especially young ones, is extremely important at any time, let alone in the digital age.285 Parents might fear that their children’s data will be misused and might also be alert to

278 See Bernstein & Triger, supra note 270, at 1232; Deborah Lupton & Ben Williamson, The Datafied Child: The Dataveillance of Children and Implications for Their Rights, 19 NEW MEDIA & SOC’Y 780, 783 (2017).
281 See BOYD, supra note 277, at 72–73.
282 Id. at 72–73.
283 See Jos de Haan, Maximising Opportunities and Minimising Risks for Children Online, in KIDS ONLINE: OPPORTUNITIES AND RISKS FOR CHILDREN 187, 192 (Sonia Livingstone & Leslie Haddon eds., 2009).
284 See BOYD, supra note 277, at 70–74.
285 Warmund, supra note 101, at 190.
their exposure to harmful content, cyberbullying, and inappropriate contact. These fears might be further enhanced by perceiving their children’s interactions as less visible to them online than in the kinetic world. Under this assumption, parents will use technology to monitor their children online as a responsive measure against the risks of technology.

While parents’ mediation is effective in reducing online risks to their children is disputable, these fears are real, and children’s safety should be on the agenda of any parent. As discussed throughout this Article, IoToys could clearly expose children to various risks, and parents might wish to intensify control over their children’s play because of these risks and the invisibility of their actions from their point of view. COPPA regulation deals directly with protecting children’s privacy from third parties misusing their data. With the privacy risks of the internet in mind, American regulators obliged OSPs to provide a right of parental review, which includes granting parents the right to review the collected information.

Some OSPs took the right of parental review a step further in IoToys, by providing parents real-time access to their children’s recordings. In some instances they could even be notified when a new recording was made. At first sight, this move seems to strengthen parents’ control in the IoToys context, and therefore should be encouraged, as it acknowledges the potential risks to the sensitive information that children might convey to third parties. The FBI even publicly recommended that parents closely monitor their children’s activity with the toys. However, this form of monitoring is troubling from a privacy perspective.

While COPPA regulation supposedly increases children’s privacy by strengthening parents’ control over the disclosure of sensitive information, it might further jeopardize children’s privacy from a different perspective: the children’s. Due to the characteristics of many IoToys devices, children might become convinced that the IoToys device is their best friend—even anthropomorphize it—and consequently share their deepest secrets with it. Perhaps obviously, the regulatory framework does not deem such secrets

286 See generally Mathiesen, supra note 266 (discussing cyberbullying and harmful content).
287 See id. at 266.
288 Id. at 267.
289 For an empirical work on reducing online risks by parental mediation, see generally Sonia Livingstone & Ellen J. Helsper, Parental Mediation of Children’s Internet Use, 52 J. BROADCAST ELECTRONIC MEDIA 581 (2008).
291 See TOYTALK, Privacy, supra note 54 (“You may review and delete voice recordings that are in your parent account via the Settings page when you log in to ToyTalk’s website. To review or delete such voice recordings, click on the ‘Conversation Link.’”).
292 Id. (“We may periodically contact parents to inform them when a voice recording is available under their account.”).
293 FED. BUREAU OF INVESTIGATION, supra note 199.
294 See supra Part 0.
sensitive information per se, as safeguarding this information from third parties might not seem important. OSPs that sometimes make it easy for parents to share IoToys devices’ recordings through social media like Facebook, YouTube, and Twitter further demonstrate the secrets’ proclaimed non-sensitive nature. 295 From the children’s perspective, however, their secrets are probably the most valuable privacy rights they own. 296

Children’s view of privacy will probably not change how policymakers conceive personal information. It should not, however, promote parental monitoring when such behavior could further risk children’s conception of privacy. The main rationale behind COPPA was not to foster parental surveillance of their children online but to aid parents who wanted their children to take advantage of the internet, while obtaining better control of the practices of the websites they visited and the information requested from them. 297 IoToys essentially could become a powerful surveillance device for parents, who could now extract all their children’s secrets without their knowledge or consent. It designates parents as surveillance officers and normalizes such conduct for both parents and their children—when they become aware of it in the future. It further illustrates important normative questions in the realm of children’s privacy that are usually less discussed in the literature: What are the implications of constantly monitoring children’s privacy? Should children possess the right to privacy from their parents? Children lack autonomy over most aspects of their lives, so why should IoToys differ?

B. Child Development and Privacy

While monitoring children’s play in IoToys could be important in lessening the privacy risks they entail, ubiquitous parental surveillance carries potentially negative consequences closely linked to their development and well-being. At early stages of life like infancy, this might be less evident, as children lack a “theory of mind”; namely, they are unable to distinguish self from other. 298 After that stage at approximately age four, children learn that they can keep secrets from their parents. 299 That is when the potentially negative effect of ubiquitous surveillance begins.

295 See TOYTALK, Privacy, supra note 54.
296 See infra Part III.A.
297 It is notable that COPPA was partially designed to enhance parental involvement in a child’s online activities. This, however, is not the rationale behind COPPA per se, but rather a tool for parents to achieve the goals of COPPA, i.e., to help protect the safety of children, maintain the security of children’s personal information collected online, and limit the collection of personal information from children without parental consent. See 144 CONG. REC. 23,926 (1998) (statement of Sen. Bryan).
298 See David Premack & Guy Woodruff, Does the Chimpanzee Have a Theory of Mind?, 1 BEHAV. & BRAIN SCI. 515, 515 (1978).
The world’s perception of children has been the subject of many scholarly debates, from Jean Piaget’s development stages and process to Donald Winnicott’s monumental work on stages of child development and practice of childhood play. A key example is Erik Erikson’s work, which stresses the importance of the years from middle childhood (approximately ages six to ten) to early adolescence (approximately ages eleven to fourteen) for children’s development. Erikson argued, inter alia, that these stages are important for developing a sense of self-esteem and individuality. Within these psychological assessments, play itself is also an important part of how children learn about the world, and parents’ intrusion could impede their learning. Control over personal information is also crucial for children’s development, as its absence could affect the adolescent’s dignity and personhood and the development of intimate relationships. Especially regarding IoToys, acknowledging the psychological importance of keeping secrets should not be easily dismissed.

Regardless of IoToys, one might argue that it is within the parents’ prerogative to determine the extent to which they protect their children’s privacy. Parents, for instance, could limit their children’s privacy in various ways, such as intruding in their personal space; knowing their personal interactions and associations, such as where and with whom they meet; and even requiring them to share their daily activities or their hopes, dreams, and fears. Arguably, the perceived risks of the digital world do not change the scope of

---

303 Id.; see also Jacquelynne S. Eccles, The Development of Children Ages 6 to 14, 9 FUTURE CHILD. 30, 32–34 (1999).
304 See Emmeline Taylor & Katina Michael, Smart Toys That Are the Stuff of Nightmares, 35 IEEE TECH. & SOC’Y MAG. 8, 9 (2016).
306 Id. at 488.
this prerogative, they indeed even intensify this need. By this approach, parents must be in greater control, especially in the digital world.

From a legal perspective, parents are not normally prohibited from recording their children or even reading their secret diaries. Parents’ fundamental right to make decisions regarding the “care, custody, and control of their children” is even protected by the Due Process Clause of the Fourteenth Amendment. Parents decide what is best for their children and whether to tell their children that parents can access their children’s conversations. Under some circumstances, parents could even be immune to tort liability under the parental immunity doctrine. As a result, children do not possess the right to conceal information from their parents. COPPA regulation is troubling not because parents are generally entitled to spy on their children but because the regulatory framework encourages OSPs to furnish such measures. When parents buy their children an IoToys doll that is supposedly their children’s new best friend, the children may not suspect that their parents can eavesdrop on every conversation they have with the doll.

Equally troubling is that parents’ depriving their children of privacy is becoming more invisible to their children than ever. Children are usually well aware of their parents’ control over their personal space. For instance, if parents decide that their children should not have privacy in their room, the children see at once that there is no door, and this might affect their behavior.

---


308 Id. (“[P]arents want to know they’re in control. They want a level of control over their kids’ digital world that is similar to the level they have in the real world.”).

309 See Mathiesen, supra note 266, at 264.


311 See U.S. CONST. amend. XIV § 1. For the Supreme Court ruling on parents’ discretion over their own children, see Troxel v. Granville, 530 U.S. 57, 78 (2000). For further information on the history of parental autonomy in common law jurisdictions, see McCarthy, supra note 310, at 975–84.

312 Under the parental immunity doctrine, children were unable to sue their parents for tort claims. For more on the demise of the parental immunity doctrine, see, for example, David Pimentel, Fearing the Bogeyman: How the Legal System’s Overreaction to Perceived Danger Threatens Families and Children, 42 PEPP. L. REV. 235, 241–42 (2015); Pimentel, supra note 276, at 954–55. For a discussion on children’s rights to sue their parents in the context in tort for their child’s injury, see, for example, Maureen S. Binetti, The Child’s Right to “Life, Liberty and the Pursuit of Happiness”: Suits by Children Against Parents for Abuse, Neglect, and Abandonment, 34 RUTGERS L. REV. 154, 156–57 (1981).


314 COPPA Rule, supra note 82.

315 McReynolds et al., supra note 234, at 2.

316 A fairly known example of behavioral shaping by surveillance is the toy based on the Christmas book Elf on the Shelf. Alex Steed, No to ‘Elf on the Shelf’: Christmas Shouldn’t
then seek ways to compensate for their privacy loss by a variety of methods, like keeping a secret journal. The interpretation of COPPA regulation in the realm of IoToys effectively ends the children’s privacy boundary management by making interference invisible to them. It tricks them into believing that they can manage their privacy boundaries, while their parents constantly betray their trust.

Such a form of invisible monitoring could have dire consequences for children’s trust and development and could also further shape their conception of privacy. One might argue that data collection and various forms of monitoring are mostly invisible to adults too, and perhaps these mechanisms actually better prepare children for the “real world.” This notion augments a well-known idiom about the demise of privacy in the digital age. This Article, however, posits differently. Privacy still matters, perhaps even more in the digital era. That children use the digital world does not imply that they do not care about their privacy. They simply view it differently from adults. For instance, children could view privacy simply as “aloneness,” “to hide secrets or special


319 *See generally* BOYD, supra note 277, at 54–55 (“Social media has introduced a new dimension to the well-worn fights over private space and personal expression.”).

320 *See, e.g.*, Sonia Livingstone, *Children’s Privacy Online: Experimenting with Boundaries Within and Beyond the Family*, in COMPUTERS, PHONES, AND THE INTERNET: DOMESTICATING INFORMATION TECHNOLOGY 130, 132 (Robert Kraut et al., 2006) (“Children seek privacy, but as a means to an end not an end in itself.”).

321 *See Melton, supra* note 305, at 488. They might also view privacy as “being alone, managing information, being unbothered, and controlling access to places.” Maxine Wolfe, *Childhood and Privacy*, in CHILDREN AND THE ENVIRONMENT 175, 190–96 (Irwin Altman & Joachin F. Wohlwill eds., 1978) (surveying children’s definitions of privacy).
things,” “to keep things to yourself,” or “not to talk to strangers.” 322 They might value privacy as an enabler tool “to engage in identity play, seek advice, form relationships, and immerse themselves in peer communication.” 323 When children experience constant surveillance by their parents, it shapes their understanding of privacy and limits their ability to make independent choices. 324 Surveillance becomes even more important when their lives are already largely monitored by their parents, 325 and further strengthens the traditional power structure of the “all-knowing” adult over the “all-learning” child. 326

Parents should be generally aware of what their children do with IoToys devices, but this should also be balanced properly by the child’s right to privacy. 327 Their privacy rights—including from their parents—should not be easily discarded. Parents must take into account how these practices could affect their child’s well-being. Certainly, most children will not be able to comprehend the privacy risks of IoToys, as they are too abstract. Children might not even care if OSPs mine their data or use it for various purposes. This is why parents are tasked to consent on their child’s behalf. But being unaware that IoToys devices record their conversations 328 and that their parents have access to them, might change children’s attitudes toward their parents upon discovering the monitoring and the meaning of privacy. 329

To clarify, this Article does not pretend to prefer one form of parenting over another. Perhaps personal safety almost always triumphs over privacy, in which case parental autonomy should be almost absolute. If parents wish to constantly monitor their children’s behavior, with proper analysis of the tradeoff between their safety and their well-being, perhaps they should be allowed to. On the other hand, the constitutional right to parental autonomy is not absolute. Even today, along with cracks in the parental immunity doctrine, parents’ privilege to raise children as they see fit could sometimes be challenged when child protection

323 Priya Kumar et al., ‘No Telling Passcodes out Because They’re Private’: Understanding Children’s Mental Models of Privacy and Security Online, 1 PACM ON HUM.-COMPUTER INTERACTION 64, 64:2 (2017); Livingstone, supra note 320, at 152.
324 See Boyd, supra note 277, at 74.
325 Id. at 76 (“Privacy is especially important for those who are marginalized or lack privilege within society.”).
327 See de Haan, supra note 283, at 193 (“Parents should be broadly aware of what their children do online, although this should be balanced by the child’s right to privacy.”). For an analysis on why children should have a right to privacy, see Mathiesen, supra note 266, at 269–72.
328 McReynolds et al., supra note 234, at 2.
and safety concerns arise.\textsuperscript{330} The state could in fact triumph over parental autonomy under some circumstances by regulating the parent–child relationship.\textsuperscript{331} Accordingly, children’s privacy rights should be treated as part of their welfare and thus not be easily waivable by their parents as a default.\textsuperscript{332}

At the very least, COPPA should not promote such potentially deceptive practices without the child’s involvement in the process. If designed to safeguard children’s privacy, COPPA must not further foster violating that privacy by granting parents better tools to do so. It must not designate parents as surveillance officers. Policymakers should further address the parent–child dimension within the notions of notice and consent. By doing so, they can make children part of the solution to the risks of the digital era rather than reinforce an existing problem.

\textbf{C. Children’s Choice?}

Accepting the potential arguments against this form of parental mediation does not necessarily lead to regulating IoToys. The sanctity of the family unit is important, and interference should be generally limited.\textsuperscript{333} Even if delicate regulation takes place, COPPA might not be the right tool for it. Still, regulators should at least acknowledge children’s privacy interests, in contrast to the concept of privacy as portrayed by parents. Not only does COPPA disregard children’s view of privacy, it indeed enhances the violation of that privacy, as children perceive it. It takes away children’s freedom to decide what to disclose to their parents, as it promotes their full access to stored content. Essentially, COPPA fails to internalize the complexity of the child–parent relationship.\textsuperscript{334}

Promoting the use of sophisticated spying devices for parents to discover their children’s secrets is not among the values embedded in COPPA regulation and should therefore be minimized through other factors. The parent–child relationship should not be set aside, and children’s trust in their parents should

\textsuperscript{332} For an argument that privacy is not always a waivable right, see JULIE E. COHEN, \textit{CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE} 148 (2012).
\textsuperscript{333} See The Family Educational Rights and Privacy Act (FERPA), 20 U.S.C. § 1232g (2012) (instituting federal law that protects the privacy of student educational records and allows parents the right to “inspect and review” them).
be taken seriously. Involving children in IoToys decisions could benefit their technological education and improve the parent–child relationship, and the understanding of privacy by both sides. Increasing children’s participatory rights, viewed as a positive liberty, could enhance children’s liberty and provide considerable privacy protection while affording their independence.

Raising children’s awareness of IoToys devices’ ability to share their data with their parents should not be generally contested. There is no rationale behind parents knowing children’s secrets per se—such knowledge is meant only to safeguard children from revealing personal information that could be misused. Parents could achieve this purpose simply by listening to the communication from the IoToys device—without hearing their child’s answer. Also, children must be made aware of the practical—not merely abstract—risks of telling their toy everything. To ensure trust, parents should simply talk to their children and explain that they might access their conversations. The “digital talk” could be important in this context. The participants could together decide, for instance, how to adjust the IoToys device’s privacy settings, when applicable, in ways that would best reflect both sides’ conceptions of privacy.

Unfortunately, this rather intuitive solution will probably not be achieved easily, as it depends, inter alia, on diverse approaches to parenting. Some parents might disregard their children’s notion of privacy and choose not to share such information with them. That is why awareness should be raised not simply by parents but also by the state. Policymakers can raise awareness by design. They can oblige OSPs and toy manufacturers to communicate this information through the IoToys device throughout its use, especially in a toy’s first communication with a child. They could also oblige OSPs and toy manufacturers to grant children better control over their shared data by enabling them to listen to and delete their own recordings.

Other regulatory ways of raising awareness could be achieved by investing in informative state-sponsored advertisements directed at children or obliging

---

335 See Davis, supra note 307; Leta Jones & Meurer, supra note 329.
337 Under a negative liberty approach, privacy should be viewed as a form of exercising personal choice. See Cohen, supra note 190, at 1907.
339 See, e.g., Leta Jones & Meurer, supra note 329 (“ToyTalk could display Barbie’s side of the conversation to parents without revealing their child’s responses.”).
341 See McReynolds et al., supra note 234, at 8.
toy manufacturers or IoToys OSPs to include this information in their advertisements. Thereafter the state could also invest in more general awareness-raising campaigns or even promote awareness through the education system.\footnote{See de Haan, supra note 283, at 193 (“Parental mediation might be stimulated by awareness-raising campaigns or by meetings at schools.”).} Along with awareness, policymakers must consider the notion of children’s autonomous choice within the concept of privacy and include them in the consent process. To this end, policymakers could oblige OSPs to obtain verifiable consent from the parents, but also from the children. Only on fulfilment of this dual-consent requirement could IoToys devices be activated. This consent model, while potentially objectionable to many parents, could further foster the protection of children’s liberty and autotomy. Children do have legal rights;\footnote{For a discussion on the possession of rights by minors in the United States, see Michele Goodwin & Naomi Duke, Capacity and Autonomy: A Thought Experiment on Minors’ Access to Assisted Reproductive Technology, 34 HARV. J.L. & GENDER 503, 508, 521–33 (2011).} in the context of privacy and IoToys, they should at least have the right to roll back the invisible boundaries of parental surveillance.

VI. CONCLUSION

IoToys might call for a shift in the perception of the collection and retention of children’s information online. These forms of regulation will most likely shape children’s conceptions of privacy. Essentially, children need not merely a right to privacy or to be let alone but simply the freedom to play with toys, without realizing that it is actually their parents who are toying with their privacy. Children need a liberty simply to be themselves. To properly mitigate the privacy risks that IoToys entails, policymakers must reevaluate the potential risks of IoToys to children’s privacy, including their need to keep secrets from their parents, and strike a proper balance between parents’ safeguarding their children from these risks while maintaining children’s autonomy. COPPA regulation must therefore be revisited and recalibrated to properly meet the challenges of IoToys. This Article suggests such a form of recalibration by revisiting COPPA’s requirements and adjusting them to IoToys. It surveys various methods to promote awareness of the risks of IoToys: redefining the choice mechanism; requiring data minimization and transparency; increasing cybersecurity and enforcement; and finally, acknowledging children’s privacy interests by involving children in the process.

Clearly, these practices may merely be a temporary solution for protecting children online and could become obsolete due to technological developments. If we consider IoToys in the broader context of IoT, we might argue that any attempt to safeguard children’s privacy in a society racing into a ubiquitous surveillance era would be futile. When children are surrounded by IoT devices that constantly gather data from them, sectoral regulation of devices that target children is perhaps no longer practical. Potentially, IoToys necessitates...
rethinking the legal framework altogether, not simply recalibrating it. But until such potential reform takes place, children’s privacy rights should not be forsaken. At the very least, the implications of IoToys and the internet of children has to be on the agenda of governmental or regulatory entities now, not in the future. Children should play with toys. But these toys should not play with their privacy.
Freedom to Hack

IDO KILOVATY*

The proliferation of Internet-connected smart devices, also known as the “Internet of Things,” has become a major threat to privacy, user security, Internet security, and even national security. These threats are manifestations of externalities primarily resulting from a market failure in the Internet of Things industry, in which vendors do not have an incentive to implement reasonable security in the software embedded in devices they produce, thus creating cheap and unsecure devices. This Article argues that law and policy have a central role to play in making this digital ecosystem more secure—not only through direct regulation of this industry, but primarily through allowing individual security researchers to hack for security—or “ethical hacking.” At present, contractual obligations and laws that prohibit hacking, such as the Computer Fraud and Abuse Act and the Digital Millennium Copyright Act, are adopting a strict liability approach, which criminalizes almost any form of hacking, regardless of motivation or potential benefits. This Article rejects this outdated approach in the wake of ubiquitous cyber-attacks, imperfect software, and the emerging Internet of Things ecosystem.

This Article argues that law and regulatory agencies should accommodate hacking for security purposes to allow security researchers to discover possible vulnerabilities, while shielding them from copyright infringement or criminal liability. While security research into software and hardware is desirable, the law by and large restricts such research. This results in a reality of highly unsecure Internet of Things devices and could potentially lead to serious harms to security and privacy. Such a legal accommodation should be supported by other legal adaptations, mainly involving regulatory oversight and enforcement, consistent rules for vulnerability disclosure, and clear distinctions between ethical and malicious hackers.

TABLE OF CONTENTS

I. INTRODUCTION ............................................................................457

* Frederic Dorwart Endowed Assistant Professor of Law, University of Tulsa, College of Law; Cybersecurity Policy Fellow, New America; Visiting Faculty Fellow, Center for Global Legal Challenges, Yale Law School; Affiliate Fellow, Information Society Project, Yale Law School; I would also like to thank Rosa Brooks, Oona Hathaway, Scott Shapiro, Robin West, Taisu Zhang, Molly Brady, Niva Elkin-Koren, Tal Zarsky, Robert Spoo, Rebecca Crotoof, Claudia Haupt, Amit Elazari, ISP fellows workshop participants, Data & Society fellows, the Georgetown Law fellows workshop participants, and the Center for Cyber Law and Policy at the University of Haifa.
II. Internet of Hackable Things .................................................. 464
   A. The Economics of IoT ...................................................... 467
   B. The Technology of IoT .................................................... 469
      1. The Ubiquity of Sensors ............................................. 471
      2. Physicality .................................................................. 472
      3. Software and Hardware Distinction ............................ 473
   C. The Threats of IoT .......................................................... 474
      1. User Privacy ............................................................. 476
      2. User Security ........................................................... 477
      3. Third-Party Security .................................................. 479

III. The Security Research Environment ...................................... 480
   A. White Hat ...................................................................... 481
   B. Black Hat ...................................................................... 482
   C. Gray Hat ..................................................................... 483
   D. The Vulnerability Market ............................................. 483
   E. Accountability in the IoT Industry ................................. 484

IV. The Freedom to Hack .......................................................... 485
   A. The Digital Millennium Copyright Act (DMCA) ............. 489
      1. The DMCA Exemption for Security Research ............. 491
         a. Good Faith .......................................................... 495
         b. Opposition by U.S. Regulatory Agencies ............... 497
   B. The Computer Fraud and Abuse Act (CFAA) ................. 498
      1. U.S. Sentencing Guidelines ..................................... 503
   C. Contractual Prohibitions ............................................. 504

V. Creating a Secure Hyperconnected World Through Law ........ 504
   A. Distinguishing Malicious from Benign Hackers .............. 506
   B. Legislative and Administrative Efforts to Date .............. 507
   C. Clarifying CFAA and DMCA Boundaries ........................ 509
   D. Requiring Built-In Patchability in IoT Devices ............. 511
   E. Privacy Tort Law Solutions ......................................... 512
   F. Vulnerability Disclosure Procedure ............................... 513
      1. Responsible Disclosure ........................................... 514
      2. Full Disclosure ...................................................... 516
      3. The Road Forward on Vulnerability Disclosure .......... 517
   G. Transnational Law Enforcement and Reducing National
      Security Threats ......................................................... 517
   H. Tackling Security by Obscurity ..................................... 518

VI. Conclusion .................................................................. 520
I. INTRODUCTION

Everyday devices and appliances are becoming more sophisticated, computerized, and software-backed.1 Cars, thermostats, door locks, smart watches, and even toasters are now powered by code and connected to the Internet, which offers a variety of online features that allow users to remotely monitor and control their devices.2 These objects are collectively referred to as the “Internet of Things” (IoT) to denote that Internet is no longer exclusively a platform for people to communicate with each other; it is now a “physical” Internet,3 a network of “things” communicating amongst themselves while also collecting and transmitting user data collected by their sensors to corporations and state authorities.4

The proliferation of IoT devices in personal, business, and public environments is part of a technological shift from hardware to software.5 Physical objects are being supplemented, and even replaced, by software. By 2020, it is expected that IoT will reach as many as 20 billion connected devices, compared to 8 billion today,7 with other estimates extending to as much as 50 billion devices.8 The future worth of the IoT industry is also estimated in the hundreds of billions of dollars, should its trajectory remain as projected.9 This shift is preceded by a phenomenon of embedding processors into everyday “things.”10 In the past, this would have been immensely expensive and inefficient, whereas today, microprocessors are widely available and affordable,
and Internet speeds are constantly increasing, meaning that it is easier to manufacture “smart” objects that operate smoothly.  

Software, however, is not the only emerging technological feature in everyday objects. The uniqueness of IoT is its Internet connectivity, which makes it part of the global network grid, with all the pertaining conveniences and dangers. The IoT trend will most likely continue to grow and pose serious challenges in the future, both legally and technically. Some argue that the IoT development may signal “the end of ownership,” since copyright may stifle any modification to the software of these devices, but copyright law is also, in a way, a form of information censorship.

However, I argue that unless a broad freedom to hack these devices for security purposes is recognized, at least until regulatory agencies catch up, IoT technology could also be the end of security and privacy, broadly speaking. This is particularly true considering that the complexities of IoT software will necessarily mean tradeoffs in terms of security, and vendors creating complex IoT software will have to test it for every possible attack or compromise, which is essentially impossible. Even if it were possible, experts argue that software engineers cannot predict future methods of attack, and software testing would  


12 See Maria Farrell, The Internet of Things—Who Wins, Who Loses?, The Guardian (Aug. 14, 2015), https://www.theguardian.com/technology/2015/aug/14/internet-of-things-winners-and-losers-privacy-autonomy-capitalism [https://perma.cc/9UTD-EK6K] (“With its insecure devices with multiple points of data access, user applications that routinely exfiltrate our sensor data, activity logs and personal contacts, and a Sisyphean uphill struggle required to exert any control over who knows what about us, the internet of things does more than create whole new cyber-security attack surfaces. It is so riddled with metastasising points of vulnerability that you begin to sense that these are not bugs, but features.”).


15 See Samuelson, supra note 13, at 598.


17 See id. at 545–47 (“Even when software performs as intended, software cannot fully protect users from themselves.”); see also Capers Jones, Software Defect-Removal Efficiency, 29 COMPUTER 94, 94–95 (1996); Note, Immunizing the Internet, Or: How I
also not solve the social engineering threat that targets the unwitting cooperation of users,18 which involves “opening an infected file, clicking on a malicious hyperlink, sending personal information to a phishing Web site, or manually adjusting security settings.”19 However, it is still believed that the vast majority of security breaches are caused by flaws in software.20

While embedding access to the global network within ordinary objects offers many advantages—it makes devices more dynamic, customizable, user-friendly (to an extent), and, generally, smarter21—it also poses a series of security challenges that, if they remain unaddressed, may represent actual threats to the “digital order” in the form of rampant security breaches and privacy violations.22

The major problem with today’s unsecure IoT environment is that it is largely a result of a market failure.23 The market failure manifests itself in multiple ways. First, the industry is not legally bound by any particular guidelines on security and privacy;24 a sizable number of devices are therefore unsecure, offering an opportunity for criminals and other exploiters to commit malicious cyber-attacks against innocent users.25 Further, IoT can also be used as a proxy for larger attacks against critical infrastructure, including the very backbone of the Internet—an externality that neither vendors nor IoT users necessarily care about, because they do not directly experience the adverse effects of those externalities.26 Second, IoT vendors have no economic incentive

Learned to Stop Worrying and Love the Worm, 119 HARV. L. REV. 2442, 2449 (2006) [hereinafter Immunizing the Internet] (“[I]t is much harder to ‘patch’ a person than a computer.”).

18 See Thompson, supra note 16, at 545.
19 See id. at 547.
20 See Derek E. Bambauer & Oliver Day, The Hacker’s Aegis, 60 EMORY L.J. 1051, 1060 (2011) (“Gartner calculates that 75% of security breaches result from software flaws.”).
21 See Minerva et al., supra note 10, at 27.
22 See Bambauer & Day, supra note 20, at 1058.
23 See Schneier, supra note 3.
26 See York, supra note 25 (explaining how an IoT-enabled denial-of-service attack against DNS provider Dyn made it impossible for Internet users on the East Coast to reach various websites); see also Bruce Schneier, Your WiFi-Connected Thermostat Can Take Down the Whole Internet. We Need New Regulations, WASH. POST (Nov. 3, 2016),
to offer security as a feature in their products, primarily because consumers are not showing strong preferences toward security and privacy as higher priorities than lower prices. At the very least, informational gaps between vendors and consumers lead to an uninformed and inefficient choice by consumers. The Senate has recently recognized this particular market failure and has proposed IoT industry-focused legislation.

Ransomware attacks are only one example of malicious activity that criminals or nation-states may use against unsecure IoT devices, and reports indicate that ransomware attacks against IoT are already taking place at present. Distributed denial-of-service (DDoS) attacks, data breaches, and

---


28 See Richard A. Spinello, CyberEthics: Morality and Law in Cyberspace 151–53 (2011) (explaining that the loss of privacy is a market failure).


30 See Kim Zetter, What Is Ransomware? A Guide to the Global Cyberattack’s Scary Method, Wired (May 14, 2017), https://www.wired.com/2017/05/hacker-lexicon-guide-ransomware-scary-hack-thats-rise [https://perma.cc/4ZPC-4WAX] (explaining that ransomware is malware that prevents access to data resident on a target computer by encrypting data files, without the user being able to access them until he or she pays the ransom).

31 See Bilefsky, supra note 25 (explaining that computer systems responsible for the electronic key system was hit with ransomware); cf. Nathaniel Mott, Ransomware Didn’t Lock People in Their Hotel Rooms, Tom’s Hardware (Jan. 30, 2017), http://www.tomshardware.com/news/ransomware-didnt-lock-hotel-rooms,33528.html [https://perma.cc/7QNT-2D4X] (claiming that the Austrian hotel ransomware was not quite as reported, but a regular ransomware affecting generation of new keys).

32 See Immunizing the Internet, supra note 17, at 2444 (DDoS attacks are “self-propagating worms [who] take control of vulnerable computers . . . the attackers then command the computer to flood targeted systems with requests for information, preventing legitimate traffic from getting through.”).
surveillance are all possible threats to IoT users if its security problem remains unaddressed.

Recently, Bruce Schneier, a (arguably the) leading cybersecurity and cryptography expert, referred to the increasing prevalence of IoT devices as a “World-Sized Web,” denoting that this ubiquitous network of devices will benefit corporations seeking to maximize profits, open new vulnerabilities for criminals to exploit, and aid totalitarian regimes throughout the world. It is almost a cliché in the information security community that IoT devices are very often unsecure and relatively easy to hack due to an abundance of software flaws, unpatched vulnerabilities, and even an inability to “patch” these devices’ flaws once they are discovered. This is largely enabled by market forces, which pressure vendors to create cheaper devices at the cost of disregarding security and privacy. In other words, this reality is enabled by the tech industry’s drive to innovate at an accelerated pace, while working under the

---

33 See generally Andrew Guthrie Ferguson, *The Internet of Things and the Fourth Amendment of Effects*, 104 CALIF. L. REV. 805, 805 (2016) (arguing that the Internet of Things present new possibilities for surveillance thus challenging established Fourth Amendment doctrine).


36 For the purposes of this Article, “vulnerability” is broadly defined as “a set of conditions that may compromise the confidentiality, integrity, or availability of an information system. It is often a simple oversight or weakness in a computer’s software that lets a hacker manipulate computer data.” Edward H. Freeman, *Vulnerability Disclosure: The Strange Case of Bret McDanel*, 16 INFO. SYS. SECURITY 127, 127 (2007).

37 See Schneier, supra note 35.


40 See The Connected World: Examining the Internet of Things: Hearing on S. Hrg. 114–237 Before the S. Comm. on Commerce, Sci., and Transport., 114th Cong. 119 (2015) (“The computer chips that power these systems are often cheaply produced, rarely updated or patched, and highly susceptible to hacks.... These devices will be cheap, even disposable, and the incentives for the manufacturer to provide regular security updates will be minimal.”).

41 See Schneier, supra note 39 (For example, “The chip manufacturer is busy shipping the next version of the chip, and the ODM is busy upgrading its product to work with this next chip. Maintaining the older chips and products just isn’t a priority. And the software is
assumption that embedding cybersecurity could stifle this rapid innovation rate.42

To address the abovementioned market failure, this Article argues that outsourcing some of the vulnerability discovery to third-party actors—security researchers—would bolster IoT security. These researchers essentially employ hacking techniques for the purpose of enhancing security—in other words, they think and act like a hacker for the company in order to ward off future criminal hacking.

Currently, federal law imposes significant limitations on unsolicited hacking for security research through both civil penalties and criminalization of certain hacking activities,43 leading to fears of legal jeopardy among members of the cybersecurity community.44 Exceptions to these legal sanctions, if they exist, are typically very narrow and would still put benign actors under the threat of legal consequences from vendors, thus limiting the amount of overall security research as well as the ability to present such research in an academic setting for further study and development.45

In order to enhance IoT security, the law, as well as the institutions creating, interpreting, and applying the law, should allow hacking for the purpose of security research. Such “benign” hacking would reveal flaws and weaknesses in software that, if exploited by malicious actors, could affect not only individuals’ personal security and privacy, but even U.S. national security.46 This approach will increase the efficiency of vulnerability disclosure and patching because there will be no chilling effect on the activity of revealing software old, even when the device is new. For example, one survey of common home routers found that the software components were four to five years older than the device.”).


43 See Samuelson, supra note 13, at 568.


45 See Bambauer & Day, supra note 20, at 1054 (arguing that IP laws stifle critical security research and blocks or limits the ability to share information relating to security flaws) (citing Jonathan L. Zittrain, The Generative Internet, 119 HARV. L. REV. 1974, 1974 (2006)).

To be clear, security research is only one part of the overall cybersecurity concoction, which should include, in Lawrence Lessig’s words, an optimal balance between “public law and private fences.” There is a race between benevolent and malicious actors in cyberspace, and the argument advanced by this paper seeks to empower actors who wish to improve the overall security and privacy of IoT.

The underlying hypothesis of this paper is that advancing IoT technologies will transform our lives entirely by becoming a substantial part of our society. The ubiquity of sensors, the physicality of most IoT devices, and the absence of reasonable default security standards could lead to major threats to individual and collective security and privacy. The rapid development of this field has already led to regulatory inefficiency and a serious market failure, enabling vendors to manufacture and sell unsecure IoT devices globally. Providing an incentive for the broader security community to become involved in fixing this ecosystem without fear of legal jeopardy will make individual users safer while also protecting critical infrastructure, such as hospitals, power plants, and the Internet backbone, from IoT externalities.

This paper will proceed in four parts. In Part I, I will discuss the phenomenon of IoT—“the world of hackable things”—and provide an overview of the market failures at play. These market failures are at the crux of this Article’s argument because they allow threats to individual users and third-parties to flourish as a result of unsecure IoT devices. Part II will be dedicated to introducing the security research environment, in which different types of hackers and motivations are shaping reality. In Part III, I will focus on the legal hurdles impeding “the freedom to hack”—mainly contractual provisions, federal prohibition of circumvention of technological protection measures (TPMs) in the Digital Copyright and Millennium Act, and criminal liability for unauthorized access to protected computers within the Computer Fraud and Abuse Act. Finally, Part IV will propose a concrete framework for creating a normative, technical, and institutional environment in which security researchers can achieve their goal of making software more secure by distinguishing benevolent from malicious actors, strengthening regulatory oversight and enforcement, clarifying statutory boundaries, regulating

---

47 See Malena Carollo, Influencers: Lawsuits to Prevent Reporting Vulnerabilities Will Chill Research, CHRISTIAN SCI. MONITOR (Sept. 29, 2015), https://www.csmonitor.com/World/Passcode/Passcode-Influencers/2015/0929/Influencers-Lawsuits-to-prevent-reporting-vulnerabilities-will-chill-research [https://perma.cc/7HSK-MLGB] (providing data that 74% of leading experts (referred to as “the Influencers”) believe that lawsuits against vulnerability disclosure in public will have chilling effects on security research).


49 See Schneier, supra note 3.

50 See Immunizing the Internet, supra note 17, at 2443 (2006) (“Not only does current policy create the wrong incentives regarding cybercrime, it does too little to encourage computer hackers and computer users to contribute actively to Internet security.”).
patchability, creating a consistent procedure for disclosure of vulnerabilities, and tackling security by obscurity.

II. INTERNET OF HACKABLE THINGS

It was probably unimaginable at the conception of the Internet that one day it would be used to connect everyday “things” to it. The development of this phenomenon allowed for machine-to-machine communication, the “communication between . . . entities that do not necessarily need any direct human intervention.”\(^\text{51}\) Whether through a smart thermostat that learns a user’s temperature-setting patterns,\(^\text{52}\) a bracelet that tells a user how well she exercises and sleeps,\(^\text{53}\) a webcam that can wirelessly transmit photos and videos,\(^\text{54}\) a smart toaster offering the perfect toast,\(^\text{55}\) or a car that has the ability to connect to the Internet and offer navigation services, self-diagnosis tools, and remote control through widely used smartphones,\(^\text{56}\) such machine-to-machine networks abound.

There is a growing understanding that “things with computers embedded in them” are becoming “computers with things attached to them.”\(^\text{57}\) This means that a whole set of legal issues traditionally pertaining to computers are transposed into the area of ordinary daily objects, but those ordinary daily objects now have a few extra features that make questions of legality tremendously challenging.\(^\text{58}\) For example, previously, if a toaster malfunctioned, it would have been mainly a consumer protection problem, whereas today, it might as well be a telecommunications problem, involving a

\(^\text{51}\) Minerva et al., supra note 10, at 12.

\(^\text{52}\) Meet the Thermostat, NEST, https://nest.com/thermostat/meet-nest-thermostat [https://perma.cc/2YP2-QPPW].


\(^\text{55}\) See Joel Hruska, The Internet of Things Has Officially Hit Peak Stupid, Courtesy of This Smart Toaster, EXTREME TECH (Jan. 5, 2017), https://www.extremetech.com/electronics/242169-internet-things-officially-hit-peak-stupid-courtesy-smart-toaster-griffin-technology [https://perma.cc/7XE8-CFJK].


\(^\text{57}\) See Schneier, supra note 3.

whole set of challenges pertaining to privacy and security and, in more extreme circumstances, national security.59

While the general phenomenon of IoT is somewhat intuitive in today’s hyperconnected world, there is no official or widely adopted definition of the technology.60 One definition is “the ability of everyday objects to connect to the Internet and to send and receive data,”61 a feature that was previously nonexistent in everyday things. Another definition provides that IoT is “a network of items—each embedded with sensors—which are connected to the Internet”;62 another similar definition characterizes IoT as a “[s]ystem where the Internet is connected to the physical world via ubiquitous sensors.”63 While Internet connectivity is itself quite intuitive, often missing in defining IoT is an emphasis on the sensors, actuators, and central processing units (CPUs), or cloud computers,64 that often comprise the IoT ecosystem.

Unlike personal computers (desktop, laptops, smartphones, and the like), IoT devices often lack a user interface, or at least one that allows control over security and privacy features.65 IoT should also be contrasted from popular operating systems, which are supported by large tech companies who constantly offer updates to the software.66 This largely means that the degree of user control over the configuration of a device is significantly limited and is usually controlled by the vendor, if at all.67 It is expected that the vendor will provide reasonable security already built into the device—“security by design”—but unfortunately, the current state of affairs in IoT has proven otherwise.68

60 Minerva et al., supra note 10, at 6.
61 See FTC STAFF REPORT, supra note 8, at i.
63 Minerva et al., supra note 10, at 21.
64 The fact that many IoT devices are supported by cloud computing creates and additional risk to privacy, since data stored on the cloud could potentially become the target of a data breach against the cloud itself. See Bambauer & Day, supra note 20, at 1059 (providing an example of cloud weakness that led to a security breach against Twitter).
65 FTC STAFF REPORT, supra note 8, at v–vi.
68 See id. (“Most IoT devices are ‘closed.’ Customers can’t add security software after devices ship from the factory. Often, such tampering voids the warranty. For such reasons, security has to be built into IoT devices so that they are ‘secure by design.’ In other words, for IoT, security must evolve from security just ‘bolted onto’ existing systems such as servers
Understanding the physicality of IoT is crucial if we are to create solutions to the wide range of resulting legal challenges. IoT insecurity is not merely a theoretical threat—it is an actual danger to our very homes.\(^6^9\) Typically, an IoT device is comprised of three components—a sensor, a CPU (or cloud computer), and an actuator.\(^7^0\) While a sensor collects data about its users and environment,\(^7^1\) the CPU (or “the cloud”) processes that data and potentially commands the actuator to take appropriate actions.\(^7^2\) These two components are essential for controlling the actuator, which is an “output device[] that implement[s] decisions.”\(^7^3\) For example, a sensor could be a thermostat used to monitor the temperature, with a connected CPU tasked with determining whether the air conditioner should be turned on or off, which would be accomplished through the actuator, the actual object that this whole system was built to control.\(^7^4\) In a way, sensors are the “eyes and ears” of the Internet, and the actuators are “hands and feet.”\(^7^5\) The CPUs, in this analogy, would be the brain, since they process data and react to it according to certain predetermined software-based rules.\(^7^6\)

Since a typical user has little to no control over the security features (and many other features) of their specific device, enhancing the security of the device will necessarily require the user to tinker with the software, which could breach contractual obligations contained within End-User License Agreements (EULA), violate the anti-circumvention rules of the Digital Millennium Copyright Act (DMCA),\(^7^7\) or trigger criminal liability and prosecution if the manner in which they access these devices is seemingly unauthorized—which includes virtually any form of hacking.\(^7^8\)

69 See Schneier, supra note 3.
70 See id.
71 Id.
72 Id.
73 See Poudel, supra note 9, at 1003.
74 See Schneier, supra note 3.
75 Id.
76 See id.
78 See 18 U.S.C. § 1030(a)(2) (2012); see also Erin Fleury, Is It Illegal to Test Websites for Security Flaws? Heartbleed & the CFAA, MINN. J. L. SCI. & TECH. F. (Dec. 30, 2014), http://editions.lib.umn.edu/mjlst/is-it-illegal-to-test-websites-for-security-flaws-heartbleed-the-cfaa [https://perma.cc/PS9S-RJX8] (arguing that the discovery of the OpenSSL Heartbleed security flaw, which allowed intercepting encrypted information, caused systems “to send back far more than what is intended. Of course, the CFAA is meant to target people who use exploits such as this to gain unauthorized access to computer systems, so it would seem that using Heartbleed is clearly within the scope and purpose of the CFAA. The real
Therefore, users often have to rely on vendors’ practices of vulnerability patching and security by design, which do not always exist in a market of accelerated innovation and competition, particularly in cheaper devices. In many instances, a vendor’s decision whether to provide vulnerability patches is a question of risk assessment and market forces—and market forces, particularly in the tech industry, do not always work in favor of consumers (if we assume that privacy and security are in the interest of consumers). This is perhaps more alarming considering that the cost of security breaches to users in aggregate is significantly higher than the cost to vendors, which could explain the gap in expectations between vendors and users. In other words, “[s]ystems are particularly prone to failure when the person guarding them is not the person who suffers when they fail.”

A. The Economics of IoT

Many assume that the market will eventually solve the security and privacy problems of the IoT ecosystem. But this may not be accurate given that these problems are themselves a result of a market failure. The unlikelihood of a market solution is particularly stark when examined in terms of the costs problem arises, however, for people interested in independently (i.e. without authorization) testing a system to determine if it is still susceptible to Heartbleed or other vulnerabilities.”).

79 See Rapid7, Comments in Response to the Notice and Request for Comments on “The Benefits, Challenges, and Potential Roles for the Government in Fostering the Advancement of the Internet of Things,” NAT’L TELECOMM. & INFO. ADMIN. (June 1, 2016), https://www.ntia.doc.gov/files/ntia/publications/rapid7_comments_to_ntia_iot_rfc_-_jun_2_2016.pdf [https://perma.cc/3F8W-57NT] (“Since IoT devices are highly diversified and include very inexpensive items manufactured by companies with limited security experience, the result can be a considerably more exploitable environment than the status quo.”).

80 See Terrell McSweeny, Comm’r, Fed. Trade Comm’n, Keynote Address at the New York Law School: Consumer Protection in the Age of Connected Everything 3–4 (Feb. 3, 2017), https://www.ftc.gov/system/files/documents/public_statements/1070193/mcsweeny_nysioio_2016.pdf [https://perma.cc/VY6E-JAFJ] (“Consumer concern is heightened by business practices that often leave them in the lurch: IoT products may not have patch support or the same life expectancy as other connected products, and these limitations are not always communicated clearly to consumers. . . . Consumers are repeatedly saying that data security is a top barrier to purchasing connected devices.”).

81 See Bambauer & Day, supra note 20, at 1059 (“[U]sers face greater harm than vendors do, especially overall. While precise figures are difficult to ascertain, reliable estimates of the worldwide economic damage caused by digital attacks in 2003 range from $12.5 billion for worms and viruses, and $226 billion for all attacks, to $157-$192 billion on Windows PCs alone in 2004. Losses to vendors from security breaches, such as from increased support costs, reputational harm, and declines in share price, are also uncertain, but likely considerably smaller. Vendors, therefore, have less incentive to fix bugs than is socially optimal.” (internal citations omitted)).


83 See Schneier, supra note 3.

84 See id.
associated with cyber-attacks on IoT, which are often experienced by third parties and are therefore considered externalities. 85 Because such externalities involve a wide variety of sectors and actors, with varying degrees of costs and benefits, the prospect of an efficient transaction is unlikely. 86

When it comes to externalities in software, it is often believed that software vulnerabilities are “inevitable externalities” because flawless software does not yet exist. 87 This is further exacerbated by the pressure placed on vendors by competition to release software to the market as fast as they can. 88 While this trend is generally true, it is still possible to make software better through constant fixing of vulnerabilities, therefore reaching a socially optimal level of security. 89

Furthermore, companies who decide to enter the IoT market do not always have the experience needed to implement security features in their devices. 90 There is a sizable degree of opportunism when it comes to new players in the IoT industry, making unsecure IoT devices pervasive. 91

In addition, IoT devices are largely inexpensive and disposable, which precludes most costly security features. 92 The literature identifies additional reasons for ubiquitous unsecure IoT devices—lack of experience in data security among vendors, absence of processing power in most IoT devices for “robust security measures such as encryption,” and unforeseen threats, 93 given that the attackers are humans who constantly adapt and change their methods. 94 The recurring theme is the inability of vendors to fully solve the potential security flaws in IoT devices on their own.

At the same time, the users themselves are often unaware of the risks; IoT architecture is often driven by vendors attempting to reduce costs, and the individual consumer is typically interested in a product’s features, rather than

---

85 See id.
87 See id. at 142–44; see also Jay Pil Choi et al., Network Security: Vulnerabilities and Disclosure Policy, 58 J. Indus. Econ. 868, 869 (2010) (“[I]t is virtually impossible to design software that is free of vulnerabilities.”).
89 See Choi et al., supra note 87, at 869 (“[The software industry has made significant investments in writing more secure code . . .”).
90 FTC Staff Report, supra note 8, at 13.
92 FTC Staff Report, supra note 8, at 13.
its security settings. 95 Whereas computers have been hackable since their conception, the IoT ecosystem increases the stakes to a far greater state of urgency. 96 This is largely enabled by the physicality of IoT, which can cause serious physical harms, and the ubiquitous sensors, which pose a privacy concern to users. 97 This notion is further supported by the unwillingness of certain tech companies to patch their software if it does not yield an effective cost-benefit analysis. 98 Furthermore, while security and privacy are certainly important to consumers, it is unclear whether consumers will agree to pay more for a product that is more secure, even if current vendor-user informational gaps are decreased. 99 This suggests that even informing users of the risks is unlikely to solve the problem of unsecure IoT.

The classic solution to externalities resulting from market failures is government intervention in the form of legislation and regulation. 100 This Article takes another approach—legislation and regulation of the IoT industry are certainly required, but they could be far more efficient in conjunction with the lifting of burdens constraining security researchers. In other words, the market failure described in this subchapter can be mitigated by security researchers improving software quality through ethical hacking.

B. The Technology of IoT

IoT offers a convenience not previously available in offline objects. First, the user has some remote control over certain features of the device, often from

---

97 See Schneier, supra note 3, at 1 (“All computers are hackable. This has as much to do with the computer market as it does with the technologies. We prefer our software full of features and inexpensive, at the expense of security and reliability. That your computer can affect the security of Twitter is a market failure. The industry is filled with market failures that, until now, have been largely ignorable. As computers continue to permeate our homes, cars, businesses, these market failures will no longer be tolerable. Our only solution will be regulation, and that regulation will be foisted on us by a government desperate to ‘do something’ in the face of disaster.”).
99 See Kesan & Hayes, supra note 27, at 781–82.
100 See Eli Dourado & Jerry Brito, Is There a Market Failure in Cybersecurity?, 106 MERCATUS ON POL’Y GEO. MASON UNIV. 1, 2 (2012).
a smartphone or personal computer. She has the ability to customize and monitor the functionality of her appliances, though this is often limited through the user interface provided by the vendor. Second, IoT technology equips vendors with the ability to optimize and improve their products through processing user data generated by the devices. However, this comes at a cost, since consumer data may also be used in negative ways, such as aggressive advertising, sale to third parties, or enhancement of surveillance capabilities. Third, IoT technology offers interoperability between devices, which, though it is yet to be fully developed, allows devices to communicate with each other. These benefits may sometimes even relate to the health, quality of life, and wellbeing of the user. Insulin pumps and pacemakers are examples of IoT applications in healthcare that revolutionized diagnosis and medical treatment, making patients’ health much more manageable.

Cybersecurity risks and threats existed long before the advent of IoT, and the argument made by this Article could apply equally to IoT and non-IoT environments, since software will have flaws regardless of the platform on which it runs. However, the IoT ecosystem creates a serious challenge and shakes up some basic cybersecurity assumptions—it significantly broadens the attack surface that hackers can use, and the level of harm to autonomy is also

---


102 See Nick Feamster, Who Will Secure the Internet of Things?, FREEDOM TO TINKER (Jan. 19, 2016), https://freedom-to-tinker.com/2016/01/19/who-will-secure-the-internet-of-things [https://perma.cc/8B6Y-NL35] (“Manufacturers of consumer products have little interest in releasing software patches and may even design the device without any interfaces for patching the software in the first place.”).

103 See Ferguson, supra note 33, at 807–08.


106 See Ferguson, supra note 33, at 811.


108 See FTC STAFF REPORT, supra note 8, at i–ii.

109 See id. at 7–8 (“[C]onnected health devices can ‘improve quality of life and safety by providing a richer source of data to the patient’s doctor for diagnosis and treatment[,] . . . improve disease prevention, making the healthcare system more efficient and driving costs down[,] . . . [and] provide an incredible wealth of data, revolutionizing medical research and allowing the medical community to better treat, and ultimately eradicate, diseases.’”).

far greater, thus trivializing hacking in general but also making it more personal.\textsuperscript{111} This will result in more opportunistic hacking, whereby users’ security or privacy may be compromised for potential criminal ends.\textsuperscript{112}

Law and regulation will find it increasingly difficult to address IoT hacking, due to its immense pervasiveness, volume, and trans-border effects and origins.\textsuperscript{113} This will leave the most trivial hacking activities unaddressed from a law enforcement perspective.\textsuperscript{114} The argument in this Article, therefore, proposes to enhance security by fixing vulnerabilities through a legal system that legitimizes the activities undertaken by security researchers. These researchers employ hacking and reverse-engineering techniques for the purpose of identifying security flaws and reporting them to the respective vendor and, eventually, the public.

The following subparts elaborate on why the IoT ecosystem is particularly challenging in the cybersecurity context—sensors are everywhere, processors are operating physical objects, and the distinctions between software and hardware are eroding. These IoT-specific challenges are creating a particularly vulnerable environment.

1. The Ubiquity of Sensors

The IoT ecosystem is creating a world of ubiquitous sensors.\textsuperscript{115} These sensors are the eyes and ears of the Internet, collecting data about the

\textsuperscript{111} Oliver Tavakoli, \textit{The Unintended Attack Surface of the Internet of Things: How a Vulnerability in a Common Consumer WiFi Device Is Challenging Today’s Enterprise Security}, \textit{Dark Reading} (Sept. 29, 2015), www.darkreading.com/vulnerabilities---threats/the-unintended-attack-surface-of-the-internet-of-things/a/d-id/1322393 [https://perma.cc/R9CS-EBME] (“[T]he combination of poorly written code and infrequent updates will surely lead to a broader and less manageable attack surface.”); \textit{see also FTC Staff Report, supra} note 8, at 11 (“[A]s consumers install more smart devices in their homes, they may increase the number of vulnerabilities an intruder could use to compromise personal information.”); Mauricio Paez & Mike La Marca, \textit{The Internet of Things: Emerging Legal Issues for Businesses}, 43 N. Ky. L. Rev. 29, 46 (2016) (“As the number of Internet-connected objects expands, so too does the potential attack surface. The IoT faces serious security issues because it is based on interoperability and interdependence: more interactions among devices lead to more areas of vulnerability.”).


\textsuperscript{113} \textit{See Immunizing the Internet, supra} note 17, at 2446–47.

\textsuperscript{114} Scholars recognize the limits of law enforcement in the world of computer crime. \textit{See id.} at 2445 (2006) (“[C]ybercrime cannot be effectively combated solely with traditional law enforcement tools.”).

\textsuperscript{115} \textit{See Arkady Zaslavsky, Internet of Things and Ubiquitous Sensing, Computing Now} (Sept. 2013), https://www.computer.org/web/computingnow/archive/september2013 [https://perma.cc/M787-X9FD] (“With billions of ICOs [Internet-connected objects] and a diverse abundance of sensors, the IoT will be an enabler of ubiquitous sensing.”).
environment and processing and possibly transmitting that data elsewhere. These sensors are working continuously, and they are everywhere. IoT devices enable not only data about direct computer use but also data about driving, home heating and cooling, food stored in a refrigerator, pulse and blood pressure, sleep patterns, and much more.

These distributed data can tell a lot about a specific person. The most private and nonintuitive pieces of information about a user are constantly collected by IoT devices and may enable misuse for criminal, business, law enforcement, and other purposes. The richness of data within the IoT ecosystem has also led to law enforcement finding this space appealing for surveillance.

2. Physicality

A significant characteristic of IoT is its physicality. Processors embedded in IoT devices are tasked to operate actual, physical equipment, with tangible consequences in the physical world. Think of a smart thermostat, which learns about the preferences of the user but is also tasked to turn on or off a piece of equipment—the AC or furnace—when certain conditions are met. In this way, the IoT device commands the actuator, meaning that any meddling with IoT could have physical ramifications due to actuators malfunctioning, at times posing danger to physical security. Examples include a vehicle not responding to its driver’s actions, a disabled insulin pump, and a garage door that won’t open.

---

116 See Hakima Chaouchi & Thomas Bourgeau, Internet of Things: From Real to Virtual World, in NEXT-GENERATION WIRELESS TECHNOLOGIES: 4G AND BEYOND 161, 173 (Naveen Chilamkurti et al. eds., 2013) (listing some examples of data collected by sensors—“mechanical data (position, force, pressure), thermal data (temperature, heat flow), electrostatic or magnetic field, radiation intensity (electromagnetic, nuclear), chemical data (humidity, ion, gas concentration), and biological data (toxicity, presence of bioorganisms”).

117 See Rapid7, supra note 79.

118 Ferguson, supra note 33, at 807–08; Poudel, supra note 9, at 1013; Schneier, supra note 35.

119 Schneier, supra note 35, at 2; Ferguson, supra note 33, at 819.

120 See FTC STAFF REPORT, supra note 8, at 5, 12.


122 See id.

123 See FTC STAFF REPORT, supra note 8, at 12.

In other words, today’s everyday objects are creating telecommunications problems that challenge notions of security and privacy. These challenges are similar whether we talk about healthcare equipment, household objects, or transportation. The effects, however, may be tremendously different—a malfunctioning pacemaker could lead to death, whereas a disabled wearable smartwatch is a matter of inconvenience or, at most, a privacy violation.

3. Software and Hardware Distinction

Although the growing role and share of software in the overall IoT environment cannot be overstated, hardware also poses a host of challenges to the security and privacy associated with IoT. For example, researchers at the University of Michigan have recently learned that a CPU manufactured overseas had a backdoor built by design into the CPU. This enables a small portion of the CPU to be used as an entryway for malware, which can then obtain control over the device. Since IoT devices have CPUs embedded in them, this represents an actual threat to the integrity and resilience of IoT.

From a security and privacy perspective, both the software and the hardware need to be regulated and monitored for potential vulnerabilities that could affect the normal functioning of a device. Regulatory agencies in the United States are increasingly focusing their efforts on software, which many believe will be “eating the world” and taking over the digital sphere. But even if this prediction is accurate, hardware may still be designed in a way that allows exploitation, particularly if it is under-regulated due to the appeal of software regulation. Hardware represents an even bigger “black-box” problem, since it is extremely time consuming and complicated to determine how a specific computer component works, whereas software is relatively easier to grasp—as

126 See Andy Greenberg, Forget Software—Now Hackers Are Exploiting Physics, WIRED (Aug. 31, 2016), https://www.wired.com/2016/08/new-form-hacking-breaks-ideas-computers-work [https://perma.cc/DVN6-KQML] (“The trick works by running a program on the target computer, which repeatedly overwrites a certain row of transistors in its DRAM flash memory, ‘hammering’ it until a rare glitch occurs: Electric charge leaks from the hammered row of transistors into an adjacent row. The leaked charge then causes a certain bit in that adjacent row of the computer’s memory to flip from one to zero or vice versa. That bit flip gives you access to a privileged level of the computer’s operating system.”).
128 Id. at 19.
129 Id. at 36.
security researchers have demonstrated recently.\textsuperscript{131} Therefore, the analysis provided by this Article, while focusing mostly on software, could still be applicable to security research into hardware.

C. The Threats of IoT

The characteristics of sensor abundancy and general physicality of IoT lead us to a third attribute, which is particularly alarming. IoT devices are not typically manufactured with robust or even minimal security standards (technical, and possibly mechanical).\textsuperscript{132} The IoT market failure results in vendors not implementing security in their IoT devices, mostly due to competition—in other words, in order to reduce manufacturing costs and offer a cheaper product.\textsuperscript{133} On the other hand, the average consumer does not typically demand strong security features, most likely due to informational gaps.\textsuperscript{134}

This suggests that lack of IoT security is a global problem, since the same security-lacking devices would be present in the United States just as in other parts of the world. Regardless, the United States has an important role to play from a legal perspective by setting robust standards and best practices for the rest of the world to follow, including the ethical hacking of IoT devices advanced by this Article. In addition, many IoT vendors are based in the United States and fall under the jurisdiction of U.S. laws and regulations,\textsuperscript{135} and so ethical hacking within the United States would secure both domestic devices as well as those that are exported to elsewhere in the world.

The IoT revolution comes with a price. While the ability of everyday objects to connect to the Internet offers a broad range of advantages, it also poses a set of specific challenges, stemming from the vulnerabilities that these devices have almost by default. The literature generally identifies three major threats with today’s IoT ecosystem—privacy, individual user security, and third-party security.\textsuperscript{136}

\textsuperscript{131} See Ohm & Reid, supra note 5, at 1675–79 (describing the shift from hardware to software).
\textsuperscript{132} See Immunizing the Internet, supra note 17, at 2444.
\textsuperscript{133} See Lazarescu, supra note 112.
First, since IoT sensors collect data about their respective users and their environment, unauthorized actors may attempt to access that personal information for a variety of reasons. Having security features within an IoT device could make it much harder for these unauthorized actors to access personal information. However, privacy breaches could then still be committed by vendors and other third parties who seek to monetize the collected data, which could also be labeled as a privacy risk.

Second, malicious actors may try to hack into IoT devices and meddle with the functionality of the device. For example, hackers may decide to shut down a car’s engine, lock a hotel room while demanding ransom, or disable a pacemaker. These are security risks confined to the user.

Third, IoT devices may be used individually (a single IoT device) or collectively (an “army” of compromised IoT devices) to facilitate an attack or breach targeting another computer system. In this case, the IoT is used merely as a proxy, which allows the hacker to have more disruptive power (if multiple IoT devices are used for a specific attack) and to mask her or his identity. This is the manifestation of the externalities discussed supra. For example, a hundred thousand compromised IoT devices were used to mount a distributed denial of service (DDoS) attack against Domain Name System (DNS) provider Dyn. The Dyn attack made it impossible for Internet users to access websites like Twitter, Netflix, and Reddit. This is a security risk against third parties—against the Internet.

137 See Poudel, supra note 9, at 1013.
141 See FTC STAFF REPORT, supra note 8, at 12 (“[A] compromised IoT device could be used to launch a denial of service attack. Denial of service attacks are more effective the more devices the attacker has under his or her control; as IoT devices proliferate, vulnerabilities could enable these attackers to assemble large numbers of devices to use in such attacks. Another possibility is that a connected device could be used to send malicious emails.”).
142 Id.
144 See Schneier, supra note 3, at 1, 5.
1. User Privacy

IoT devices often generate data about the consumer, which raises the risk of these data being compromised.145 Many consumers would not be able to differentiate between an Internet-connected object and its offline counterpart in terms of the potential privacy implications.146 Data collected by IoT devices may pose a host of privacy concerns.147 For example, in the case of an IoT device used to measure blood alcohol—the Breathometer—collected data may impact “employment decisions; criminal liability implications; and health, life, or car insurance ramifications.”148 The data collection, retention, and disposal policies of a specific manufacturer are not always communicated to the consumer in a transparent and accessible manner.149 This is of course not unique to the Breathometer, as other IoT devices collect sensitive personal data as well.

These problematic uses of personal information are not the end of the story. Certain devices might require the use of payment methods and passwords, which could be accessed and misused by cyber criminals seeking financial gain.150 If this sensitive information is not properly secured, the number of vulnerabilities and compromises will increase, exposing personal information to malicious actors.

Another major problem that is currently emerging in the privacy law scholarship is sensor fusion151—when innocuous and seemingly insignificant data collected by an individual IoT sensor could be used to make inferences about the user when paired with data collected from other IoT sensors. Collectively, the data could be used to make near-certain inferences about the user, though the individual pieces of data would have no meaning on their own.152 For example, data from a smartphone’s gyroscope could be used to determine the driving habits of a user; when paired with an IoT pacemaker, the combination of these data can yield an inference about the emotional state and mood of the user.153 Scholars identify a long list of inferences that would be possible under the emerging IoT ecosystem of data collection—“a user’s mood;

145 See Schneier, supra note 35.
146 See Kesan & Hayes, supra note 27, at 781.
147 See Bambauer & Day, supra note 20, at 1058.
148 See Peppet, supra note 93, at 90.
149 Id. at 90, n.18 (“[M]any ‘things’ have little in their external form that suggests they are connected to the Internet. When you grab an Internet-connected scarf from the coat rack or sit on an Internet-connected chair, should you have some obvious sign that data will be transmitted or an action triggered?”) (citing ADRIAN MCEWEN & HAKIM CASSIMALLY, DESIGNING THE INTERNET OF THINGS 294 (2014)).
151 See Peppet, supra note 93, at 118–24 (“Sensor fusion is the combining of sensor data from different sources to create a resulting set of information that is better than if the information is used separately.”).
152 Id. at 120.
153 See Poudel, supra note 9, at 1013.
stress levels; personality type; bipolar disorder; demographics (e.g., gender, marital status, job status, age); smoking habits; overall wellbeing; progression of Parkinson’s disease; sleep patterns; happiness; levels of exercise; and types of physical activity or movement.” Considering how personal and sensitive some of these data are, IoT devices should allow for stronger security to prevent breaches that could be devastating to users.

Daniel Solove calls this problem “data aggregation” and argues that, “[v]iewed in isolation, each piece of our day-to-day information is not all that telling; viewed in combination, it begins to paint a portrait about our personalities.” The bottom line is that malicious actors have many methods of abusing private information they collect without authorization, particularly if they can collect that information across multiple IoT devices.

It must be noted that many of the data described in this subpart would not be considered personally identifiable information (PII), which, if compromised, imposes notification responsibilities on vendors. However, PII does not typically include sensor data, or anonymized data, which is often re-identifiable. This difficulty seems to suggest that the focus at present should be on enhancing IoT security until federal and state regulations address the full breadth of data that ought to be protected by vendors. At present, relying on state laws regulating notification of data breaches would not necessarily solve the problem of sensor fusion.

2. User Security

Vulnerabilities in a specific device may facilitate potential exploitations against that specific device and, consequently, its user. The primary target in this case is not the data in the device but rather the device’s functionality. For example, a hacker may decide to attack a thermostat using a ransomware method, meaning that the user will be unable to use the thermostat until she or he pays the ransom. The data are not the primary interest for the hacker

---

154 See id.
155 See Daniel J. Solove, Access and Aggregation: Public Records, Privacy and the Constitution, 86 MINN. L. REV. 1137, 1185 (2002) (“The aggregation problem arises from the fact that the digital revolution has enabled information to be easily amassed and combined. Even information in public records that is superficial or incomplete can be quite useful in obtaining more data about individuals. Information breeds information.”).
156 See GINA STEVENS, CONG. RES. SERV., RL34120, FEDERAL INFORMATION SECURITY AND DATA BREACH NOTIFICATION LAWS (2010).
157 See Alexander H. Tran, The Internet of Things and Potential Remedies in Privacy Tort Law, 50 COLUM. J.L. & SOC. PROBS. 263, 275–76 (2017) (arguing that many state laws are not dealing with sensor data, which may be re-identifiable, with Texas’ statute being one of the only exceptions, providing a broad definition to “sensitive personal information”).
158 See Lazarescu, supra note 112.
here—whereas disrupting the normal functioning of the device is.\textsuperscript{160} This hack is also enabled by weak security standards and vulnerabilities in software.\textsuperscript{161}

Recently, an Austrian hotel suffered a ransomware attack targeting its smart-locks.\textsuperscript{162} The attack locked up hotel rooms until the hotel gave up and paid the ransom in order to restore the functioning of the locks. In that case, hackers did not care about who used the locks, or how, or when.\textsuperscript{163}

User security may take a more serious form if the target is a life-sustaining IoT device such as the pacemaker. In fact, security researchers revealed recently that pacemakers have nineteen security vulnerabilities and are plagued with as many as 8,600 security flaws.\textsuperscript{164} In addition, security researchers were able to hack into insulin pumps and disable their medicine delivery settings.\textsuperscript{165} Potentially, a hacker exploiting one or more of these vulnerabilities could cause a life-threatening situation, ranging from a serious bodily harm to the user or, in extreme situations, even death.\textsuperscript{166}

Vulnerable IoT devices could also be used to access the network through which they connect to the Internet, which would expose other devices on the network to potential compromise.\textsuperscript{167} Even if a specific vendor employs the strictest security features for their IoT devices, that would not necessarily protect all IoT devices within a household, as there are many vendors with varying degrees of IoT security implementations.\textsuperscript{168} This is analogous in a way to the Target breach, which surprisingly was directed not at Target’s computer network but rather at a contractor who had weaker data-protection standards.\textsuperscript{169}

\begin{footnotesize}
\begin{enumerate}
\item[160] See id.
\item[161] See id.
\item[162] See Wolff, supra note 139.
\item[163] See id.
\item[165] See FTC STAFF REPORT, supra note 8, at 12.
\item[166] See Lily Hay Newman, \textit{Medical Devices Are the Next Security Nightmare}, WIRED (Mar. 2, 2017), https://www.wired.com/2017/03/medical-devices-next-security-nightmare [https://perma.cc/9NM-WE75] (“That in turn could mean the theft of sensitive medical records, or a devastating ransomware attack that holds vital systems hostage until administrators pay up. ‘The entire extortion landscape has changed,’ says Ed Cabrera, chief cybersecurity officer at the threat research firm Trend Micro. ‘You do get into this life or death situation potentially.’”).
\item[167] See FTC STAFF REPORT, supra note 8, at 11.
\item[168] See Poudel, supra note 9, at 1015.
\end{enumerate}
\end{footnotesize}
That hack resulted in forty million credit cards being stolen in one of the biggest data breaches in recent years.\textsuperscript{170} 

The bottom line is that a compromise to user security can range in its effects from inconvenience, such as the device being slowed down, to complete disruption of the device, to a life-threatening situation, depending on the targeted device, motivation, and the method of exploitation employed.

3. Third-Party Security

The proliferation of IoT creates an environment of potentially millions of vulnerable devices. This enables hackers to create enslaved IoT devices that can be used as a proxy for attacking third parties—commonly referred to as “botnets.”\textsuperscript{171} Botnets are essentially armies of Internet-connected devices compromised through a malware that infects them and allows the attacker (the “bot master”) to command that group of devices.\textsuperscript{172} The most intuitive form of third-party security risk due to IoT botnets is a DDoS attack.\textsuperscript{173} The key in a DDoS attack (as opposed to a DoS attack) is in the overwhelming volume of requests, which essentially shuts down the target due to its unavailable bandwidth for responding to legitimate requests of service.\textsuperscript{174}

In October 2016, a malware named Mirai created a botnet out of a hundred thousand compromised IoT devices and used it to mount a DDoS attack against a DNS service provider, Dyn.\textsuperscript{175} DNS is the basic protocol that translates alphanumerical addresses (like 192.168.1.182), which are then translated into a computer’s binary language in blocks of eight bits (11000000 10101000 00000001 10110110).\textsuperscript{176} The Internet’s TCP/IP protocol works with binary addresses, which it “understands,” whereas alphanumerical addresses are a convention that enables humans to conveniently browse the Internet without having to memorize a list of numerical IP addresses.\textsuperscript{177} This structure is an easy target for a malicious actor who wishes to shut down portions of the World Wide Web

\textsuperscript{170}Id.; see also Gregg Scott, commenting on Brian Krebs, Email Attack on Vendor Set Up Breach at Target, \textsc{Krebs on Security} (Feb. 14, 2014), https://krebsonsecurity.com/2014/02/email-attack-on-vendor-set-up-breach-at-target [https://perma.cc/5NT8-JQA2].

\textsuperscript{171}A botnet that recently caused significant unrest is Mirai, which is also the name of the malware that allowed the organization of this botnet. Lily Hay Newman, The Botnet That Broke the Internet Isn’t Going Away, \textsc{Wired} (Dec. 9, 2016), https://www.wired.com/2016/12/botnet-broke-internet-isnt-going-away [https://perma.cc/KE29-8S9M].

\textsuperscript{172}See id.

\textsuperscript{173}See id.

\textsuperscript{174}See id.

\textsuperscript{175}See Mathew J. Schwartz, Botnet Army of ‘Up to 100,000’ IoT Devices Disrupted Dyn, \textsc{Bank Info Security} (Oct. 27, 2016), https://www.bankinfosecurity.com/botnet-army-just-100000-iot-devices-disrupted-dyn-a-9486 [https://perma.cc/C8W5-ZV8H].


\textsuperscript{177}See id.
and make it impossible for the average user to access websites and services online.178

III. THE SECURITY RESEARCH ENVIRONMENT

In cybersecurity, it is essential to understand the enemy in order to resolve the threats and challenges that exist largely due to certain forms of hacking. Hacking tends to have a negative connotation—it frequently implies malevolent, possibly illegal, activity in relation to computers and networks.179 But hacking culture is more diverse than that. Criminally motivated hackers, or “black hat hackers,” are only a subset of the larger group of hackers—in fact, a tiny proportion, only about 1%.180 Hackers tend to have different motivations, purposes, and incentives, ranging from seeking a thrill or challenge, or resolving and fixing vulnerabilities, to extorting a user, disrupting the functioning of computers and networks, stealing data and credentials, and potentially selling the data or vulnerabilities in a designated marketplace on the Internet.181

Similarly, people tinker with their devices for a variety of reasons—for fun, to study, or to fix vulnerabilities and weaknesses, but also for criminal and destructive purposes.182 More importantly, hackers have a clear advantage over vendors when it comes to finding vulnerabilities.183 While a vendor may be focused on other tasks, hackers can dedicate their time to further study a specific system and identify its flaws.184 Hackers also tend to have the cutting-edge knowledge that allows them to reveal vulnerabilities in creative ways.185 Considering that it is far easier to attack than to defend in cyberspace—the attacker needs to know of only one vulnerability, while the defender has to defend against all possible attacks—provides yet another argument in favor of ethical hacking for security purposes.186 Efficient cyber-defense strategies, therefore, have to rely on a robust cybersecurity research environment, which involves hacking.187

This Part will explain the three main categories of hackers, which may assist in the further analysis of the “freedom to hack.” These categories are typically assigned a color—white, gray, or black. These colors reflect the morality of the

178 See York, supra note 25.
181 See id. at 294–98.
182 See Samuelson, supra note 13, at 564.
183 See Bambauer & Day, supra note 20, at 1062.
184 Id. at 1061.
185 Id.
187 See Kesan & Hayes, supra note 27, at 786.
hacking—which may also suggest its legality, though the two are not mutually
dependent. As this Part demonstrates, the boundary between legitimate and
illegitimate hacking is somewhat fuzzy, given that both ethical and criminal
hackers are utilizing the same techniques, and at first blush, in the absence
of context, it is hard to differentiate between the two. Law enforcement and
courts are not always well-equipped to make this normative determination,
and this Article therefore argues that differentiating between ethical and
unethical hackers depends on whether the hacker in question exploited a
vulnerability and whether procedures of vulnerability disclosure were followed.
This will be further discussed in Part IV.

A. White Hat

White-hat hackers are security researchers whose main motivation is to
improve software and hardware by revealing vulnerabilities and security flaws
and disclosing them in a way that will ensure they are patched. White-hat
hackers, when not employed by the vendors themselves, are motivated only
sometimes by financial gain (the expectation of being monetarily rewarded);
more often they are motivated by the challenge, or by the genuine belief that
improving the quality of software and hardware will make Internet security
stronger.

For an illustration of how white hats are improving the security of the
broader Internet infrastructure, look to Mike Lynn, a security researcher then
affiliated with Internet Security Systems, who discovered a serious software
flaw in Cisco’s routers. Although Lynn reported the vulnerability to Cisco,
he was still threatened with legal action because he planned on presenting some
of the information to his peers at a security conference. The gravity of this

---

188 See id. at 769–70 (suggesting ethics and morality axes for hackers).
189 See Thompson, supra note 16, at 556.
191 In Part IV infra, I will propose certain recommendations that could alleviate some of the difficulties introduced in the current Part.
193 See id.
194 See Thompson, supra note 16, at 555.
195 See Bambauer & Day, supra note 20, at 1053.
196 Id. at 1053–54 (citing Bruce Schneier, Cisco Harasses Security Researcher, SCHNEIER ON SECURITY (July 29, 2005), http://www.schneier.com/blog/archives/2005/07/cisco_harasses.html [https://perma.cc/WAQ7-WE57]).
flaw was characterized then as a ticking bomb endangering the very backbone of the Internet.197

Certain commentators believe that the notion of separating white hats from other hackers is that white hats act under authorization.198 Another distinction made in literature is based on disclosure: hackers disclosing vulnerabilities directly to the vendor are white hats, while those publicizing vulnerabilities to the broader public are considered gray hats.199

Given that white hats’ motivation is primarily the drive to enhance security, it seems unreasonable to subject these individuals to legal liability, assuming that cybersecurity is in the interest of the broader public and possibly the international community. It would be best, therefore, to define white hats as hackers who seek to improve security while minimizing possible harm to the vulnerable target by neither exploiting the vulnerability nor selling it to malicious actors.200

B. Black Hat

Black-hat hacking is the exact opposite of the white-hat approach. Indeed, black hats are hackers motivated by mischief or profit rather than by actually fixing vulnerabilities and security flaws.201 The ability to anonymize one’s identity on the Internet allows for the proliferation of black hat hackers (or “cybercriminals”), which lowers the risks of detection and prosecution compared to the physical world.202 Data suggests that law enforcement is usually reluctant to investigate, apprehend, and prosecute cybercriminals, given that hackers often reside overseas, which presents challenges with regard to jurisdiction and gathering evidence.203

Certain commentators make the argument that, even though black hats are essentially cybercriminals, the law should still allow them to operate freely since they can expose flaws and vulnerabilities that could have been exploited in more harmful ways, such as through terrorism or state-sponsored attacks.204 However,


198 See Thompson, supra note 16, at 557.


200 See id. at 558.

201 Hopping & Hellard, supra note 192.


203 Brenner, supra note 202, at 7.

204 Immunizing the Internet, supra note 17, at 2446 (noting that “cybercrime can expose security flaws that, if fixed, can prevent more devastating future attacks”).
the analysis in this Article will exclude black-hat hackers, since their primary intention is not enhancing security.

C. Gray Hat

Hackers’ ethics and motivations are not binary but rather could be placed somewhere on a black-white continuum. The gray area in which hackers operate with unclear motivations is fittingly labeled as “gray hat.” As an example, gray hats will still identify vulnerabilities, but, rather than disclosing them to the vendor, they might sell them to governments, intelligence agencies, or law enforcement authorities. The buyer, in turn, uses the vulnerability for a variety of purposes, such as for espionage, military, or law enforcement ends. It is difficult to tell whether gray hats are included or excluded from the scope of the argument in this Article, since that largely depends on their motivations and the precise nature of their activities. But assuming the gray-hat hacker in question follows the procedure of vulnerability disclosure and minimization of harm to third parties, they ought to be in the clear in terms of legal liability.

D. The Vulnerability Market

When considering a freedom to hack, it is also important to understand the incentives and realities of the “black-hat” vulnerability market. In this market, hackers sell what are typically known as “zero-day exploits,” meaning that vendors are unaware of these vulnerabilities in their systems and, therefore,

---

205 See generally ALLEN HARPER ET AL., GRAY HAT HACKING: THE ETHICAL HACKER’S HANDBOOK, at xxix (Wendy Rinaldi ed., 5th ed. 2018) (a book where the author provides “a holistic review of ethical hacking that is responsible and truly ethical in its intentions and material” which distinguishes gray hats from white hats).


207 See id.

208 See id.

the chance of them getting patched is relatively low.\textsuperscript{210} Governments, intelligence agencies, militaries, and cybercriminals find this black market for vulnerabilities very appealing,\textsuperscript{211} and hackers who end up selling vulnerabilities on that market believe that they are better off doing so rather than disclosing them to the respective vendor.\textsuperscript{212}

In the digital era, knowing of a vulnerability can be either a weapon or a shield. Legalizing ethical hacking could be an incentive to use that knowledge as a shield while reducing the likelihood that researchers will sell vulnerabilities on the black market. In many respects, the legal challenges demonstrated in Part III of this Article create an incentive for researchers to sell vulnerabilities on the black market, rather than to disclose them to the relevant parties, for fear of legal jeopardy.\textsuperscript{213} The result makes individual users less safe and creates a serious danger to the Internet as a whole, considering that critical infrastructure and other public services may be running software with exploitable vulnerabilities of which the vendor has no knowledge.\textsuperscript{214}

At the same time, there are white-hat vulnerability markets, which are often referred to as “bug bounty” programs, facilitated by the vendors themselves.\textsuperscript{215} These markets create incentives for security researchers by offering monetary rewards for reports of vulnerabilities made directly to the vendors under predetermined conditions.\textsuperscript{216} Their purpose is to create a greater incentive for security researchers to cooperate with vendors in order to prevent vulnerabilities from being sold to potentially malicious actors—criminal hackers and hostile governments.\textsuperscript{217}

E. Accountability in the IoT Industry

Allowing ethical hackers to freely snoop for vulnerabilities and flaws could facilitate a more accountable IoT industry: manufacturers will patch reported vulnerabilities and attempt to improve their products in a way that provides reasonable security, and therefore data privacy, in order to avoid negative publicity. The ethical hacking community is usually ahead of regulatory efforts

\begin{footnotes}
\footnotetext{\textsuperscript{210}See Schneier, supra note 209.}
\footnotetext{\textsuperscript{211}See id.}
\footnotetext{\textsuperscript{212}Bambauer & Day, supra note 20, at 1067–68.}
\footnotetext{\textsuperscript{213}Id. at 1054 (“IP law plays a suppressive rather than a generative function—it blocks or limits whether, and how, hackers share their findings.”) (citing Jonathan L. Zittrain, The Generative Internet, 119 HARV. L. REV. 1974 (2006)).}
\footnotetext{\textsuperscript{214}See id. at 1058.}
\footnotetext{\textsuperscript{215}Zetter, Hacker, supra note 206. Google’s bug bounty program offers monetary rewards ranging from $100 to $31,337 to security researchers who identify and report qualifying bugs and corresponding attack scenarios to Google. Google Vulnerability Reward Program (VRP) Rules, GOOGLE APPLICATION SECURITY, https://www.google.com/about/appsecurity/reward-program [https://perma.cc/J95H-58FM].}
\footnotetext{\textsuperscript{216}Zetter, Hacker, supra note 206.}
\footnotetext{\textsuperscript{217}See Kesan & Hayes, supra note 27, at 759 (creating a distinction between white, black, and gray vulnerability markets).}
\end{footnotes}
to set standards for industries, which potentially allows for a more efficient and informed security atmosphere.

Regulatory agencies are slowly beginning to realize the immense potential of exposing IoT vulnerabilities with the help of the hacker community. This allows the industry to patch vulnerabilities before malicious actors can exploit them for criminal, political, or challenge-driven ends. The FTC has recently announced an IoT challenge to “combat security vulnerabilities in home devices,” offering a monetary reward for a tool that would enhance IoT security in the form of a “physical device that the consumer can add to his or her home network that would check and install updates for other IoT devices on that home network, or it might be an app or cloud-based service, or a dashboard or other user interface.” However, this effort is still not actively encouraging ethical hacking; rather, it encourages innovation. At the same time, the FTC has also become an enforcer of cybersecurity and privacy, under Section 5(a) of the FTC Act. In the future, the FTC may play an active part in ensuring that vendors address vulnerabilities reported to them in a reasonable and timely manner.

IV. THE FREEDOM TO HACK

Individuals tinker with their devices for many reasons, including for the challenge, to learn how the system works, or for diagnostic and repair purposes. The freedom to tinker is important for innovation and creativity,
and, as the next Parts will analyze, for the enhancement of security. Ensuring more ownership rights to consumers of otherwise copyrighted objects is not only a legalistic concept but an actual advocacy movement. For example, the Electronic Frontier Foundation (EFF), a nonprofit organization, is a strong proponent of a broad right to tinker, giving consumers more flexibility and autonomy and protecting “civil liberties in the digital world.”

The ideology behind the movement is the belief that technology helps protect civil rights and liberties like freedom of expression, privacy, and activism. Edward Felten notes that tinkering is not only a natural part of property rights, which the owner possesses, but an exercise in defining the relationship between the user and digital devices as “our experience is mediated through these devices.” Although tinkering is seemingly intuitively part of ownership, it has largely not been formally legally recognized. When the law has addressed tinkering, it has mostly been framed under the “permission culture,” which permits tinkering only under very limited and narrow circumstances. Any deviation from this has generally been considered a prohibited criminal activity.

Court cases on the freedom to tinker reach as far as the U.S. Supreme Court, which, in the recent Impression Products v. Lexmark International, allowed consumers to tinker with and reuse their printer cartridges without facing patent infringement charges, highlighting that this freedom is part of “the rights that come along with ownership” and that “the buyer is free and clear of an infringement lawsuit” in such circumstances.

Many have been advocating for a broad freedom to tinker with otherwise copyright-protected hardware and software. The EFF and other non-profit organizations have long pushed for a right to tinker with rightfully owned hardware and software, framing it as a broader “digital freedom.” In the past, consumers could reverse-engineer and research their devices, but nowadays, Section 1201 of the DMCA, which prohibits circumvention of Technical

222 About EFF, ELECTRONIC FRONTIER FOUND., https://www.eff.org/about [https://perma.cc/5SQF-BK9X].

223 See id.


225 See Andrew Torrance & Eric Von Hippel, The Right to Innovate, 2015 MICH. ST. L. REV. 793, 801 (2015); see also Samuelson, supra note 13, at 566–67 (describing the freedom to tinker as “existing largely without a formally recognized legal identity”).

226 See Samuelson, supra note 13, at 566 (citing Felten, supra note 224).

227 See id.


229 Id. at 1534.

230 See Samuelson, supra note 13, at 569–81.

Protection Measures (TPMs), as well as the Computer Fraud and Abuse Act (CFAAA) and wiretap laws have hampered that ability.\textsuperscript{232} Similarly, there is a growing body of research suggesting that companies create contractual “safe harbors” for security researchers, meaning that contracts ought to foster security research rather than stifle it.\textsuperscript{233}

The freedom to tinker encompasses many dimensions—it allows for the intellectual freedom to learn more about different objects in people’s lives.\textsuperscript{234} This Article introduces a subset of the freedom to tinker—\textit{the freedom to hack}.

By \textit{freedom to hack}, I mean that the law, along with the institutions that interpret, apply, and enforce it, should recognize the benefits of security research (or ethical hacking). The old saying goes “given enough eyeballs, all bugs are shallow,”\textsuperscript{235} indeed it is increasingly becoming the new tech wisdom—inviting the security research community to participate in this information security enhancing activity. Empirical evidence suggests that bug bounty programs are in fact a cost-effective mechanism.\textsuperscript{236} This mostly includes research into vulnerabilities in software, hardware, and networks with the intent of fixing these flaws and making the system less susceptible to malicious hacking and more secure overall. Therefore, to some extent, security researchers or hacking-savvy individuals should be able to hack and snoop for vulnerabilities and weaknesses in order to make computer systems and networks stronger by exposing these flaws. There is an ongoing debate over how to disclose vulnerabilities and software flaws, and I will discuss it further in Part IV of this Article.

The freedom to hack, only a small part of the freedom to tinker, focuses on one important dimension—the right to expose and disclose vulnerabilities to the


\textsuperscript{234} See Samuelson, \textit{supra} note 13, at 565–66.

\textsuperscript{235} ERIC S. RAYMOND, \textit{The Cathedral and the Bazaar: Musings on Linux and Open Source by an Accidental Revolutionary} 30 (Tim O’Reilly ed., rev. ed., 1999). This is Eric Raymond’s famous “Linus Law,” one of open-source culture’s cornerstones. \textit{Id.}

\textsuperscript{236} See Elazari Bar On, \textit{supra} note 233 (manuscript at 7) (citing Matthew Finifter et al., \textit{An Empirical Study of Vulnerability Rewards Programs}, 22nd USENIX Security Symposium, at 13 (Aug. 14–16, 2013) (The symposium “presents data from two leading programs (Mozilla and Google) for the period 2010–2013, and reports that the overall cost of bug bounty, per day, is on average $485 (on Chrome) or $658 (on Firefox), compared to the cost of highly-skilled security engineer estimated at $500 per day. As the authors note, while the cost of the entire program resembles the cost of hiring one engineer, ‘the benefit of a VRP far outweighs that of a single security researcher because each of these VRPs finds many more vulnerabilities than any one researcher is likely to be able to find.’”)); see also Mingyi Zhao et al., \textit{An Empirical Study of Web Vulnerability Discovery Ecosystems}, Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security (2015) (“Based on our results, we suggest that organizations should continuously collaborate with white hats, actively seek to enlarge the contributor base, and design their recognition and reward structure based on multiple factors.”).
vendor without being subjected to civil or criminal penalties. This does not entail an *unrestricted* right to hack. The law will still have to restrict hacking that causes serious harm to third parties (such as privacy violations), which should be treated under a criminal liability regime\(^\text{237}\) or tort law.\(^\text{238}\) Rather, there should be an intellectual freedom to use methods of hacking to fix and improve software and hardware, with a robust distinction between constructive and destructive (i.e., exploitative) hacking.\(^\text{239}\)

Many tech companies, and even governmental authorities, actively encourage ethical hacking of their systems and provide what are referred to as “bug bounties,” through which they invite hackers to test their systems for vulnerabilities and to report any possible flaws in exchange for monetary compensation.\(^\text{240}\) However, there are still certain boundaries imposed by bug bounty programs in terms of what activities are allowed and prohibited.\(^\text{241}\) Even when no compensation is guaranteed, or no official bug bounty program is in place,\(^\text{242}\) many individual security researchers still engage in bug hunting for a variety of reasons.\(^\text{243}\) This leads to some serious tensions. Not all tech companies encourage an active hunt for bugs in their software, and some would

\(^{237}\) See Samuelson, *supra* note 13, at 567.

\(^{238}\) See *Restatement (Second) of Torts* § 652B (1977) (“One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.”); *Id.* § 652D (“One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public.”); Tran, *supra* note 157, at 265 (where author argues common law privacy torts, particularly “disclosure of private facts” and “intrusion upon seclusion,” could provide some remedy to the privacy harms enabled by the IoT ecosystem).

\(^{239}\) See Samuelson, *supra* note 13, at 567–68. “[A] right to repair that which is broken and make other uses of artifacts as long as one is not harming the interests of others.” *Id.* at 566.


\(^{241}\) See Kirsch, *supra* note 179, at 397–98 (“[T]esting must not violate any law, or disrupt or compromise any data that is not your own.”) (quoting *Google Vulnerability Reward Program (VRP) Rules*, *supra* note 215).

\(^{242}\) Many companies do not have a vulnerability disclosure program. *Id.* at 398.

\(^{243}\) Bambauer & Day, *supra* note 20, at 1066 (listing reasons for security researchers engaging in vulnerability hunting: “possible future remuneration, intellectual satisfaction, peer recognition, ideological commitment, animus toward a particular vendor, and expectations in a larger community of testers”).
even be quite unwelcoming of any vulnerabilities reported, whether due to reputational or cost-associated reasons, and might claim such vulnerability collection to be in breach of contract or in violation of the law.

With regard to possible circumvention liability, DMCA prohibits circumvention of TPMs in copyrighted software, thus possibly exposing security researchers to liability. At the same time, with regard to criminal liability, the CFAA contains a fair number of ambiguous concepts in relation to hacking — or unauthorized access—that, if interpreted in a certain light, could expose legitimate security researchers to legal jeopardy. The DMCA, CFAA, and contractual hurdles will be further discussed in the following two subparts.

A. The Digital Millennium Copyright Act (DMCA)

Computer software, just like any other creative work, is protected under copyright law. In 1998, Congress enacted the DMCA, creating a legal barrier for tinkerers. The DMCA implemented the World Intellectual Property Organization (WIPO) treaties by creating a legal regime against circumvention of TPMs, protecting copyrighted works through the criminalization of circumvention of these measures.

Subsection 1201(a)(1)(A) of the U.S.C. reads, “No person shall circumvent a technological measure that effectively controls access to a work protected under this title.” In this way, Section 1201 restricts legitimate users from controlling their devices, since the IoT environment is ultimately a collection of devices running on copyrighted software often protected by TPMs. This would mean that smart vehicles, pacemakers, insulin pumps, thermostats, and any

---

244 Id. at 1064–65.
245 Jack Detsch, Influencers: Antihacking Law Obstructs Security Research, CHRISTIAN SCI. MONITOR (July 14, 2016), https://www.csmonitor.com/World/Passcode/Passcode-Influencers/2016/0714/Influencers-Antihacking-law-obstructs-security-research [https://perma.cc/A8ZG-QM4W] (comparing companies with established bug bounty programs to those who opted to use the CFAA as a weapon against security researchers, providing the example of Justin Shafer, who was arrested by the FBI for allegedly discovering a vulnerability in dental office management software, allowing access to the information of 22,000 patients, with the vendor arguing that Shafer’s actions violated the CFAA).
251 See Samuelson, supra note 13, at 590.
other IoT devices are covered by the Section on anti-circumvention, unless an explicit exemption is provided by the DMCA, as discussed below.

Realizing that an absolute exclusion of the right to tinker is unreasonable with respect to digital works, the DMCA also provides certain exemptions from infringement liability, which will be discussed in the following sections. Initially, however, the DMCA provided a very narrow exemption from copyright infringement for reverse-engineering of software for the purposes of interoperability, encryption research, and security testing.

In addition to the DMCA, users often agree to certain “terms of service,” which create a contractual obligation vis-à-vis the software or hardware vendor, creating another hurdle for users and, therefore, security researchers. This private ordering restricts security researchers because it grants vendors legal tools to stifle security research, or any sort of tinkering with their products, purely for business reasons, trumping any security concerns.

In 2002, for example, HP was allegedly the first company to use the DMCA as a weapon against security researchers. HP threatened to file a lawsuit against software security company SnoSoft, which had identified a security flaw in HP’s Tru64 operating system. HP threatened the researchers by noting that they “could be fined up to $500,000 and imprisoned for up to five years” under the DMCA. Eventually, HP had to back down from this threat, due to public...

---

253 *Id.* § 1201(f)(1) (“Notwithstanding the provisions of subsection (a)(1)(A), a person who has lawfully obtained the right to use a copy of a computer program may circumvent a technological measure that effectively controls access to a particular portion of that program for the sole purpose of identifying and analyzing those elements of the program that are necessary to achieve interoperability of an independently created computer program with other programs, and that have not previously been readily available to the person engaging in the circumvention, to the extent any such acts of identification and analysis do not constitute infringement under this title.”).

254 *Id.* § 1201(g)(2) (“[I]t is not a violation of that subsection for a person to circumvent a technological measure as applied to a copy, phonorecord, performance, or display of a published work in the course of an act of good faith encryption research.”).

255 *See id.* § 1201(j) (“[I]t is not a violation of that subsection for a person to engage in an act of security testing.” However, this exemption differs from the newly adopted security research exemption, since it required “authorization from the owner or operator” of the computer that was accessed.).

256 The government has previously argued that violating Terms of Service ought to be considered a violation of the CFAA, since it is construed as “unauthorized access.” *See United States v. Drew*, 259 F.R.D. 449, 452 (C.D. Cal. 2009).


258 *See id.*


260 *Id.*

261 *Id.*
Since then, the DMCA has been used against academic researchers, such as when the Recording Industry Association of America (RIAA) threatened Professor Edward Felten. Felten’s paper dealt with breaking the Secure Digital Music Initiative (SDMI)’s systems and incited the RIAA to demand that Felten withdraw his paper from a conference. Felten ultimately did so. Felten is just one example of many researchers who, after disclosing vulnerabilities, receive cease-and-desist letters from companies with threats of legal action and explicit demands to discontinue any further security research due to the alleged illegality of the act.

1. The DMCA Exemption for Security Research

A lot has been said about the unclear relationship between intellectual property and security research, primarily how the DMCA is an ill-suited framework for authorizing security research. Copyright (or the right to exclude tinkerers) is not an absolute legal concept, and certain interests, such as security and privacy, should prevail when balanced against the need to protect the rights of copyright owners. Therefore, the Library of Congress (LoC) has a routine procedure—the triennial review—to assess whether certain exemptions from copyright (and criminal) liability are required in order to ensure that other important interests are fulfilled. Before discussing the

---

264 Id.
265 Freeman, supra note 36, at 129.
267 Letter from John T. Lynch, Jr., Chief of the Computer Crime & Intellectual Prop. Section at the Dep’t of Justice, to Regan Smith, Gen. Counsel & Associate Register of Copyrights 2–4 (June 28, 2018) [hereinafter Letter from John T. Lynch], https://www.justice.gov/criminal-ccips/page/file/1075496/download [https://perma.cc/6X3T] (“The purpose of the DMCA is to provide legal protection for technological protection measures, ultimately to protect the exclusive rights protected by copyright. As critically important as the integrity of voting machines or the safety of motorized land vehicles are the American public, the DMCA was not created to protect either interest, and is ill-suited to do so.”).
268 See Helen Nissenbaum, Where Computer Security Meets National Security, 7 ETHICS INFO. TECH. 61, 62 (2005) (“Security deserves a place alongside privacy, intellectual property, equity, and other values that have been vigorously debated in light of developments in and application of digital electronic information technologies.”).
269 See Arielle Singh, Note, Agency Regulation in Copyright Law: Rulemaking Under the DMCA and Its Broader Implications, 26 BERKELEY TECH. L.J. 527, 529 (2011) (citing
specific exemption within the DMCA relevant to IoT, it is essential to understand the triennial process, as well as how the world of copyright slowly creeps into other territories, such as information security.

The DMCA created a procedure of triennial review so that potential exemptions to the DMCA could be proposed by the broader public. Parties can claim that they are adversely affected by the DMCA’s anti-circumvention rule, and, after public hearing and comment, the Registrar of Copyrights submits recommendations to the Librarian of Congress, who then determines whether to approve the proposed exemptions to the rule. For example, the Librarian has to assess, among other things, “the impact that the prohibition on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research” and “such other factors as the Librarian considers appropriate.” In other words, the DMCA does not directly prescribe security as part of what the Librarian has to consider when recognizing new exemptions, but it gives the Librarian broad discretion.

In 2016, the LoC authorized an exemption that was no less than a breakthrough for the computer security community. In 2018, the LoC renewed and expanded the security exemption, and the current version of the exemption reads as follows:

H.R. REP. No. 105-551, pt. 2, at 36 (1998) (“When Congress drafted the DMCA, it recognized that it could not predict the future technology landscape, and therefore, included the rulemaking process in the statutory scheme to create flexibility.”).

270 See 17 U.S.C. § 1201(a)(1)(C) (2012) (“[T]he Librarian of Congress, upon the recommendation of the Register of Copyrights, who shall consult with the Assistant Secretary for Communications and Information of the Department of Commerce and report and comment on his or her views in making such recommendation, shall make the determination in a rulemaking proceeding for purposes of subparagraph (B) of whether persons who are users of a copyrighted work are, or are likely to be in the succeeding 3-year period, adversely affected by the prohibition under subparagraph (A) in their ability to make noninfringing uses under this title of a particular class of copyrighted works. In conducting such rulemaking, the Librarian shall examine: (i) the availability for use of copyrighted works; (ii) the availability for use of works for nonprofit archival, preservation, and educational purposes; (iii) the impact that the prohibition on the circumvention of technological measures applied to copyrighted works has on criticism, comment, news reporting, teaching, scholarship, or research; (iv) the effect of circumvention of technological measures on the market for or value of copyrighted works; and (v) such other factors as the Librarian considers appropriate.”).

271 Id. § 1201(a)(1)(C).
272 Id. § 1201(a)(1)(C)(iii).
273 Id. § 1201(a)(1)(C)(v).

The prohibition against circumvention of technological measures that effectively control access to copyrighted works set forth in 17 U.S.C. 1201(a)(1)(A) shall not apply to persons who engage in noninfringing uses of the following classes of copyrighted works: ... (10) Computer programs that are contained in and control the functioning of a lawfully acquired smartphone or home appliance or home system, such as a refrigerator, thermostat, HVAC, or electrical system, when circumvention is a necessary step to allow the diagnosis, maintenance, or repair of such a device or system, and is not accomplished for the purpose of gaining access to other copyrighted works. ... (11)(i) Computer programs, where the circumvention is undertaken on a lawfully acquired device or machine on which the computer program operates, or is undertaken on a computer, computer system, or computer network on which the computer program operates with the authorization of the owner or operator of such computer, computer system, or computer network, solely for the purpose of good-faith security research and does not violate any applicable law, including without limitation the Computer Fraud and Abuse Act of 1986. (ii) For purposes of this paragraph (b)(11), “good-faith security research” means accessing a computer program solely for purposes of good-faith testing, investigation, and/or correction of a security flaw or vulnerability, where such activity is carried out in an environment designed to avoid any harm to individuals or the public, and where the information derived from the activity is used primarily to promote the security or safety of the class of devices or machines on which the computer program operates, or those who use such devices or machines, and is not used or maintained in a manner that facilitates copyright infringement.\(^\text{275}\)

In the 2015 exemption, which was renewed in 2018, the LoC had explicitly recognized two sub-categories of devices covered by the exemption: motorized land vehicles and medical devices.\(^\text{276}\) These two sub-categories were there for a reason. Any flaws and vulnerabilities in these two types of devices could potentially be deadly or at least pose a serious danger to the safety of their users.\(^\text{277}\) Medical devices, including insulin pumps, pacemakers, implantable

\(^{\text{275}}\) 37 C.F.R. § 201.40(b)(10)–(11) (2018). Maintenance is defined as “the servicing of the device or system in order to make it work in accordance with its original specifications and any changes to those specifications authorized for that device or system,” and repair is defined as “the restoring of the device or system to the state of working in accordance with its original specifications and any changes to those specifications authorized for that device or system.” Id. § 201.40(b)(10)(i)–(ii).

\(^{\text{276}}\) Id. § 201.40(b)(7) & (9).

\(^{\text{277}}\) The FDA in its premarket cybersecurity guidelines for medical devices categorizes five types of risks: negligible (inconvenience or temporary discomfort); minor (results in temporary injury or impairment not requiring professional medical intervention); serious (results in injury or impairment requiring professional medical intervention); critical (results in permanent impairment or life-threatening injury); and catastrophic (results in patient death). FOOD & DRUG ADMIN., CONTENT OF PREMARKET SUBMISSIONS FOR MANAGEMENT OF CYBERSECURITY IN MEDICAL DEVICES: GUIDANCE FOR INDUSTRY AND FOOD AND DRUG ADMINISTRATION STAFF 17 (Oct. 2, 2014), https://www.fda.gov/downloads/MedicalDevices/DeviceRegulationandGuidance/GuidanceDocuments/ucm482022.pdf [https://perma.cc/J
494

OHIO STATE LAW JOURNAL

[Vol. 80:3

cardioverter defibrillators, and glucose monitors, are prone to software flaws,
posing an actual and immediate danger to the patients using them.278 Only
recently the FDA reported that certain implantable cardiac devices are
vulnerable to attacks, which could allow an unauthorized user to control the
device and exfiltrate data from it.279 Surprisingly, medical devices are ridden
with vulnerabilities; as already reported, certain insulin pumps280 and
pacemakers281 are vulnerable to hacking.
Motorized land vehicles are increasingly computerized and connected to the
Internet, creating a whole host of vulnerabilities that may be fatal. The
automobile industry has yet to realize the many risks associated with such
development in the architecture of cars.282 In fact, Wired reported that security
researchers were able to hack into the entertainment-system computer of a Jeep,
letting hackers command the vehicle — including steering and braking.283 This
led to Chrysler recalling its 1.4 million vulnerable vehicles in order to patch the
bug.284 The fact that smart vehicles often have more than a hundred million lines
of code strengthens the notion that security research is essential for vehicles.285
There are a few shortcomings to the 2018 DMCA security exemption that
could further stifle certain types of security research. While the exemption does
give significant leeway to security researchers who circumvent the software of
a “smartphone or home appliance or home system” for “diagnosis, maintenance,
2FB-7YEG] [hereinafter FDA CONTENT OF PREMARKET SUBMISSIONS].
278 Jay G. Ronquillo & Diana M. Zuckerman, Software-Related Recalls of Health
Information Technology and Other Medical Devices: Implications for FDA Regulation of
Digital Health, 95 MILBANK Q. 535, 550 (2017); see also U.S. COPYRIGHT OFFICE, THE
REGISTER OF COPYRIGHTS, RECOMMENDATIONS ON SECTION 1201 RULEMAKING: SIXTH
TRIENNIAL PROCEEDING TO DETERMINE EXEMPTIONS TO THE PROHIBITION ON
OF COPYRIGHTS RECOMMENDATIONS].
279 Cybersecurity Vulnerabilities Identified in St. Jude Medical’s Implantable Cardiac
Devices and Merlin@home Transmitter: FDA Safety Communication, FOOD & DRUG
ADMIN. (Jan. 9, 2017), https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm5
35843.htm [https://perma.cc/34EZ-WN8P].
280 Jim Finkle, J&J Warns Diabetic Patients: Insulin Pumps Vulnerable to Hacking,
281 Khandelwal, supra note 164.
282 UC BERKELEY SCH. OF INFO., supra note 44, at 3.
283 Andy Greenberg, Hackers Remotely Kill a Jeep on the Highway—With Me in It,
284 Andy Greenberg, After Jeep Hack, Chrysler Recalls 1.4M Vehicles for Bug Fix,
285 David Zax, Many Cars Have a Hundred Million Lines of Code, M.I.T. TECH. REV.


or repair” of such devices, it excludes a considerable subgroup of IoT devices—those that are not used by individual consumers, such as those used by the government or by other organizations.

Notwithstanding, the comments submitted in connection with the next triennial rulemaking process suggest that some conceptual shift could take place with regard to the DMCA security research exemption. For example, the Computer Crime and Intellectual Property Section at the Department of Justice recently filed comments with the Library of Congress, in which it expressed its willingness to eliminate the ambiguousness of the language contained within the exemption. This includes broadening the scope and classes of devices that may be researched (beyond devices for individual use), elimination of controlled environment as a prerequisite for legitimate research, and clarification of what it means to “lawfully acquire” a device on which security research takes place. Indeed, in 2018, the exemption removed the requirement of lawfully acquiring a device as a prerequisite for good-faith security research, and changed that to “authorization of the owner or operator” which does not require ownership, but is rather based on the owner’s consent.

a. Good Faith

The DMCA exemption is conditioned upon “good faith,” which is tricky to define in the context of security research, particularly on behalf of unaffiliated hackers. The exemption provides that “good-faith security research” means:

[A]ccessing a computer program solely for purposes of good-faith testing, investigation, and/or correction of a security flaw or vulnerability, where such activity is carried out in an environment designed to avoid any harm to individuals or the public, and where the information derived from the activity is used primarily to promote the security or safety of the class of devices or machines on which the computer program operates, or those who use such

---


288 See Letter from John T. Lynch, supra note 267.

289 Id.


291 See id. § 201.40(b)(11)(i).

devices or machines, and is not used or maintained in a manner that facilitates copyright infringement.293

This requirement limits the security research exemption to circumvention efforts intended for testing, investigation, and correction of vulnerabilities and flaws.294 It also requires an environment that is appropriate to the potential harms that could arise from such activity, with the purpose of avoiding them.295 The information obtained through the security research should be used primarily to promote security.296

These requirements implicate security research in several ways. First, they exclude security researchers who happen to stumble upon a vulnerability or who identify a possible fix to a flaw without intending to do so (i.e., not in an appropriate environment). Recently, an “accidental hero” offered a kill-switch to the global ransomware “WannaCry,” but according to him finding a solution to WannaCry had not been his intention initially.297 This could stifle vulnerability reporting by researchers whose intentions at the outset are not to promote security.

Second, the DMCA does not define “environment,” therefore potentially excluding security researchers whose environments would not be considered “designed to avoid any harm” and possibly allowing vendors to abuse this requirement against unaffiliated security researchers.298 The introduction of cloud computing as a central part of the IoT ecosystem is another exacerbating factor to the notion of “environment.”299 In fact, some opposition to the “environment” standard has been raised by the DOJ itself, noting that “[a]lthough such a tightly-controlled environment might be necessary for certain types of research that present especially serious risks of harm, isolated lab-like settings are not required in every instance of security research.”300

295 Id. § 1201(j)(1).
296 Id. § 1201(j)(3)(A).
299 See Bambauer & Day, supra note 20, at 1091–92 (explaining how cloud computing complicates researchers’ ability to test their own security).
300 Letter from John T. Lynch, supra note 289, at 4.
Third, the exemption provides that information gathered from exempted security research should be used “primarily” to enhance security and safety.\(^\text{301}\) However, this potentially opens the door to security research that crosses from a white- or gray-hat world into black-hat territory, where motivations are usually malicious.\(^\text{302}\)

Lastly, these requirements provide a glimpse into the phenomenon of copyright bleeding over into cybersecurity,\(^\text{303}\) meaning that the requirement is not necessarily in line with the way ethical hackers actually operate in the vulnerability detection space.\(^\text{304}\) This is more of an institutional problem, in which the question is whether the organs involved in the DMCA triennial review process are actually well-equipped to address the security issues within their purview.

b. Opposition by U.S. Regulatory Agencies

Agencies that commented on the proposed exemption during the triennial review process had several reservations. While the National Telecommunication and Information Administration (NTIA) supported the aforementioned exemption to the prohibition on circumvention,\(^\text{305}\) other agencies, such as the FDA, DOT, and EPA, strongly opposed and had significant reservations to exempting computer programs for good-faith security research.\(^\text{306}\) The main thrust of these agencies’ argument is that security research into computer programs could actually compromise security and privacy.\(^\text{307}\) As certain opponents noted, “‘fixing’ of medical devices without FDA or manufacturer permission would risk patient safety because it would ‘enable others to bypass proper regulatory controls.’”\(^\text{308}\)


\(^{302}\) See Zetter, Hacker, supra note 206 (describing black hat hackers as “criminals”).

\(^{303}\) See Paul Ohm & Black Reid, Regulating Software When Everything Has Software, 84 Geo. Wash. L. Rev. 1672, 1686 (2016) (“Suddenly, the Copyright Office found itself at the center of a full-fledged, multiagency debate over the extent to which code regulation might be necessary not just for copyright policy reasons, but for environmental, traffic, health, and various other noncopyright policy reasons as well.”).

\(^{304}\) See HARPER ET AL., supra note 205, at 16.

\(^{305}\) See U.S. Dep’t of Commerce, Nat’l Telecomm. & Info. Admin., Sixth Triennial Section 1201 Rulemaking, Recommendations to the Register of Copyrights on Proposed Exemptions from the Digital Millennium Copyright Act’s Prohibition Against Circumvention 73 (Sept. 18, 2015), https://www.copyright.gov/1201/2015/2015_NTIA_Letter.pdf [https://perma.cc/RR6W-QJRK] (“[T]o the extent that there is a copyright interest, NTIA believes that security research is noninfringing and constitutes fair use.”).

\(^{306}\) See, e.g., Section 1201 Register of Copyrights Recommendations, supra note 278, at 313 (detailing the FDA’s position on the exemption).

\(^{307}\) See id., at 313–15.

\(^{308}\) Id. at 293.
The FDA, for example, opposed the exemption because every medical device has to undergo FDA premarket approval, and unrestricted meddling with or changes to software in medical devices would put patients “at increased risk from bad faith attempts to modify devices during the period required to develop and obtain [FDA] approval for the change.” As a result, the FDA, the agency responsible for the safety and privacy of medical devices, would not be able to support any exemption that would compromise that responsibility.

FDA guidance in *Premarket Submissions for Management of Cybersecurity in Medical Devices* contains certain suggestions for vendors of medical devices, such as limiting access to trusted users, ensuring trusted content, and planning for detection, response, and recovery from security compromises. However, this guidance is only a recommendation for effective cybersecurity management. Though vendors submitting medical devices for FDA premarket review will want to implement these recommendations to ensure FDA approval, they are by no means legally binding. This demonstrates that even the seemingly strictest agency in terms of IoT security provides only recommended guidelines to vendors, highlighting the need for external security research due to the increasing volume of vulnerabilities.

**B. The Computer Fraud and Abuse Act (CFAA)**

Federal and state statutes have outlawed unauthorized access to computers. While each state statute is slightly different, they all share some basic concepts. The CFAA of 1984 criminalizes certain potentially harmful computer-related activities. Since its enactment, the CFAA has been amended ten times, and each time its scope has been expanded. The CFAA is often said to be “one of the most far-reaching criminal laws in the United

---

309 See generally FDA CONTENT OF PREMARKET SUBMISSIONS, supra note 277 (describing recommended premarket steps related to cybersecurity).
310 SECTION 1201 REGISTER OF COPYRIGHTS RECOMMENDATIONS, supra note 278, at 293.
311 See id., at 314–15.
312 See FDA CONTENT OF PREMARKET SUBMISSIONS, supra note 277, at 13–16 (outlining FDA suggestions for vendors).
313 See id. at 2.
314 See Medical Devices, Digital Health: Cybersecurity, FOOD & DRUG ADMIN. (Feb. 19, 2019), https://www.fda.gov/medicaldevices/digitalhealth/ucm373213.htm [https://perma.cc/E65Q-RQVU] (This vulnerability increases as “medical devices are increasingly connected to the Internet, hospital networks, and to other medical devices.”).
315 ORIN KERR, COMPUTER CRIME LAW 29–30 (3d ed., 2012) [hereinafter KERR COMPUTER] (overviewing the different state and federal statutes outlawing unauthorized access).
316 See id. at 30 (stating that different state statutes have common characteristics).
318 See Thompson, supra note 16, at 560 (describing the amendments to the CFAA).
States Code” due to its broad language and enforcement.\footnote{Orin S. Kerr, \textit{Vagueness Challenges to the Computer Fraud and Abuse Act}, 94 MINN. L. REV. 1561, 1561 (2010) [hereinafter Kerr, \textit{Vagueness}].} This vagueness raises constitutionality questions, particularly in the context of the void-for-vagueness doctrine,\footnote{See United States v. Williams, 128 S. Ct. 1830, 1845 (2008) ("Vagueness doctrine is an outgrowth not of the First Amendment, but of the Due Process Clause of the Fifth Amendment. A conviction fails to comport with due process if the statute under which it is obtained fails to provide a person of ordinary intelligence fair notice of what is prohibited, or is so standardless that it authorizes or encourages seriously discriminatory enforcement.").} exerting “pressure on courts to adopt narrow interpretations of access and authorization.”\footnote{See Kerr, \textit{Vagueness}, supra note 319, at 1572.} The statute was inspired by the common-law trespass doctrine, which does not always fit perfectly with the realities of the Internet.\footnote{See Kirsch, \textit{supra} note 179, at 393 (explaining that the now-outdated CFAA was based in common law tort doctrines).} The central provision applicable to security research is located in 18 U.S.C. § 1030(a)(2), which deals with unauthorized access to protected computers and criminalizes the obtaining of “information from any protected computer”\footnote{18 U.S.C. § 1030(a)(2)(C). The CFAA also prohibits obtaining “information contained in a financial record of a financial institution, or of a card issuer as defined in section 1602(n) of title 15, or contained in a file of a consumer reporting agency on a consumer, as such terms are defined in the Fair Credit Reporting Act (15 U.S.C. 1681 et seq.),” or “information from any department or agency of the United States.” 18 U.S. Code § 1030(a)(2)(A)-(B).} through intentional access to “a computer without authorization” or exceeding “authorized access.”\footnote{18 U.S.C. § 1030(a)(2).} The concepts of “access” and “authorization” have been the subject of substantial debate.\footnote{See generally Orin S. Kerr, \textit{Cybercrime’s Scope: Interpreting “Access” and “Authorization” in Computer Misuse Statutes}, 78 N.Y.U. L. REV. 1596 (2003) (discussing the competing interpretations of “access” and “authorization” in computer misuse statutes).} This has led to confusion among computer users, security researchers, and even law enforcement.\footnote{See Kirsch, \textit{supra} note 179, at 392–93 (discussing the resulting confusion due to uncertain interpretations of “access” and “unauthorized”).} Experts admit that this provision has the lowest thresholds and is therefore applicable to a broad subset of online activities.\footnote{See Kerr, \textit{Vagueness}, supra note 319, at 1567 (“The 1996 amendments expanded the prohibition dramatically to prohibit unauthorized access that obtained \textit{any} information of \textit{any} kind so long as the conduct involved an interstate or foreign communication.”).} It would be outside the scope of this Article to reiterate the debate over the precise contours of authorization and access. The focus would be on how security research is stifled by the prohibition on unauthorized access.

The scope of unauthorized access largely criminalizes any instance of interstate hacking\footnote{See Kerr, \textit{Vagueness}, supra note 319, at 1571.} and encompasses every Internet-connected device within the scope of “protected computer,”\footnote{See id. at 1571.} including anything that has a “microchip
or that permits digital storage.”330 The CFAA defines “computer” in a broad manner and excludes only a few devices, such as “an automated typewriter or typesetter, a portable hand held calculator, or other similar device.”331 Since some security research requires the use of hacking methods, this overbroad approach stifles research into vulnerabilities in such critical systems as voting machines,332 resulting in adversaries learning about these vulnerabilities before the vendor can identify them.333 Even at present, security researchers at the renowned DefCon hacking conference managed to hack into several voting machines in less than ninety minutes.334 This reveals the need to rebalance the goals of criminal law and cybersecurity.

Notwithstanding the overbroad scope of the CFAA, another structural problem it presents is the absence of a “legal feedback loop of the exemption request process Congress provided in the DMCA.”335 This is a significant structural difference, because while the DMCA is amenable to reconsideration of its scope through the triennial review procedure, the CFAA is generally not as flexible and does not allow for exceptions or defenses that are not explicitly provided in the law.336 This structural difference limits the power of the DMCA

---

330 See id.
331 18 U.S.C. § 1030(e)(1). A “computer” is defined as “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical, arithmetic, or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device, but such term does not include an automated typewriter or typesetter, a portable hand held calculator, or other similar device.” Id.
332 See Brian Barrett, America’s Electronic Voting Machines Are Scarily Easy Targets, WIRED (Feb. 8, 2016), https://www.wired.com/2016/08/americas-voting-machines-aren-ready-election [https://perma.cc/ZMR6-LF3S] (explaining that vulnerable voting machines are very much a reality, giving the example of WinVote, Virginia’s voting machines that were vulnerable to remote hacking—“anyone within a half mile could have modified every vote undetected”).
336 See U.S. COPYRIGHT OFFICE, RECOMMENDATIONS ON SECTION 1201 RULEMAKING: SEVENTH TRIENNIAL PROCEEDING TO DETERMINE EXEMPTIONS TO THE PROHIBITION ON CIRCUMVENTION I (Oct. 5, 2018), https://www.copyright.gov/1201/2018/2018_Section_1201_Acting_Registers_Recommendation.pdf [https://perma.cc/WEP5-Y96U] (describing the triennial review process); see also Kerr, Vagueness, supra, note 296, at 1578, n.128 (citing
in creating security research exemptions, since these are still subject to the far-reaching CFAA provisions.\textsuperscript{337}

The overbreadth of computer crime statutes is not a problem in only U.S. law; it has also been a matter of concern in security research communities overseas.\textsuperscript{338} For instance, in the United Kingdom, the Computer Misuse Act of 1990 was recently amended to criminalize the “creation, supply or application of ‘hacker tools’ for use in computer misuse offences.”\textsuperscript{339} This has significantly broadened the scope of application of the Act, making ethical hackers concerned about potential legal jeopardy.\textsuperscript{340}

The threat posed to security researchers by the CFAA is far from theoretical. In 2002, Bret McDanel, an employee of Tornado Development, Inc., was convicted and sentenced to sixteen months in federal prison for disclosing a serious vulnerability in the online-messaging product offered by his employer.\textsuperscript{341} At first, McDanel reported the vulnerability to his employer, but the employer never patched it.\textsuperscript{342} As a last resort, McDanel e-mailed as many as 5,600 Tornado customers to inform them of the unpatched vulnerability.\textsuperscript{343} As a result, the Department of Justice indicted McDanel, arguing that his actions knowingly caused “the transmission of a program, information, code, or command, and[,] as a result of such conduct, intentionally cause[d] damage without authorization[] to a protected computer.”\textsuperscript{344}

The DOJ has since admitted that prosecuting McDanel was a mistake; it filed a motion to reverse the conviction in the Ninth Circuit Court of Appeals, noting that his actions had not indicated an intent to harm his employer and could have potentially pressured his employer to fix the vulnerability, thus protecting the privacy of customers using the messaging product.\textsuperscript{345} The

\textsuperscript{337} See Daniel Etcovitch & Thyla van der Merwe, Coming in from the Cold: A Safe Harbor from the CFAA and DMCA §1201 for Security Researchers, BERKMAN KLEIN CTR. RES. PUBLICATION NO. 2018-4 (June 2018), https://dx.doi.org/10.2139/ssrn.3055814 [https://perma.cc/3FUQ-V8QU] (explaining that the CFAA limits the DMCA).


\textsuperscript{339} STEFAN FAFINISKI, COMPUTER MISUSE: RESPONSES, REGULATION AND THE LAW 76 (2009).

\textsuperscript{340} A testimony by UK-based technician read, “That’s the end of penetration testing. Why would I risk ending up in jail for doing my job? It’s madness. It takes away the incentive for making systems secure and plays right into the hands of criminals.” Id.

\textsuperscript{341} See Freeman, supra note 36, at 129 (outlining McDanel’s discovery and subsequent prosecution).

\textsuperscript{342} See id.

\textsuperscript{343} See id.

\textsuperscript{344} 18 U.S.C. §1030(a)(5)(A).

\textsuperscript{345} See Government’s Motion for Reversal of Conviction at 6, United States v. Bret McDanel, C.A. No. 03-50135 (9th Cir. Oct. 14, 2003) (“[T]he government believes it was an error to argue that defendant intended an “impairment” to the integrity of Tornado’s computer system . . . [i]instead, the evidence established that defendant informed Tornado’s
relationship between intent and harm is a critical one, since it could exclude
security researchers from the scope of the CFAA if unauthorized access can be
shown to lack intent to cause harm. Since the CFAA does not require a
showing of scienter in relation to the harm, it “overcriminalizes hacking activity
that involves mere access and inadvertent minor damage” and “effectively
establishes strict liability beyond the intentional access . . . regardless of moral
culpability.”

However, it is not only hacking that is criminalized; access to portions of
the Web that the owner did not design for public access is also generally deemed
illegal. These were the facts in United States v. Auernheimer, where the
defendant, Andrew Auernheimer, was charged under the CFAA for
“unauthorized access” because he revealed an AT&T-owned URL that
contained private account data belonging to as many as 100,000 iPad users. Such an approach to the concept of unauthorized access puts security
researchers at risk not only for using hacking techniques but also for pursuing
benign activities online that the vendor or owner deems unfriendly. This leads
to “authorization,” a legal term of art within the CFAA, being de facto defined
by tech companies rather than by Congress, courts, or law enforcement
authorities. This problematic breadth is paired with outdated notions of
sentencing, discussed in the following subpart.

customers -- the people whose data may have been vulnerable to unauthorized access -- about
the vulnerability, an action that could have brought about repair of the problem.

Similarly, in United States v. Morris, Morris argued that he had no intent to cause damage when he
created the Morris worm, although he did have intent to access a protected computer in an
unauthorized manner (the double scienter question) which caused a considerable amount of
damage to many computers affected by the Morris worm. United States v. Morris, 928 F.2d 504, 507 (2d Cir. 1991).

See Thompson, supra note 16, at 562–63 (analyzing the intent component of §1030).

See id. at 562.

See id. at 568.

For example, see the story of Aaron Swartz who was prosecuted on multiple charges
under the CFAA. Swartz accessed AT&T and JSTOR data in what some termed “data
liberation.” See The Prosecution of Aaron: A Response to Orin Kerr, PUB. DOMAIN (Jan. 18,


See Kirsch, supra note 179, at 397–98.

See id. at 399 (pointing out that private entities often define criminal activity under
the CFAA).
1. U.S. Sentencing Guidelines

The U.S. Federal Sentencing Guidelines can provide insight into how courts currently approach punishment for computer crimes. The Guidelines provide for harsher punishments for property crimes where the criminal act causes great economic loss. In the context of computer crimes, such a loss includes, among other things, “the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost . . . .” This punishment model does not take into account beneficial security research, and it ignores the far costlier alternative of malicious exploitation of vulnerabilities. Losses also include the cost of patching a vulnerability, which would have taken place even in absence of the crime.

The Guidelines impose still greater punishment if the target computer belonged to critical infrastructure. The exploitation of vulnerabilities in critical infrastructure computers, such as those intended to manage power and gas, transportation, national security, and public health, could result in devastating disruption effects. At the same time, if critical infrastructure and other non-critical computers operate on that same vulnerable software, it would be preferable to target the latter from a risk standpoint; however, that is not always possible when critical infrastructure computers operate on their own software and systems. Therefore, the Guidelines should also consider the degree of benefit of the act in question, by comparing it to the full potential of exploiting the vulnerability, which could be far more devastating than the prosecuted crime.

---

353 See generally U.S. SENTENCING COMM’N, GUIDELINES MANUAL (2016) [hereinafter U.S. SENTENCING GUIDELINES] (describing recommended sentences for various federal crimes, including computer misuse).
354 Id. § 2B1.1(b)(1).
355 Id. § 2B1.1(3)(A)(v)(III) (“[R]easonable cost to any victim, including the cost of responding to an offense, conducting a damage assessment, and restoring the data, program, system, or information to its condition prior to the offense, and any revenue lost, cost incurred, or other damages incurred because of interruption of service.”).
356 On the lack of instrumentality in the U.S. Sentencing Guidelines, see Immunizing the Internet, supra note 17, at 2453 (“[C]urrent U.S. Sentencing Guidelines do not sufficiently take instrumental concerns into account.”).
357 See id. at 2454 (citing Creative Computing v. Getloaded.com LLC, 386 F.3d 930, 935–36 (9th Cir. 2004) (where the court ruled that routine maintenance and updating would be assessed as part of the damages)).
359 See Immunizing the Internet, supra note 17, at 2455.
360 See id. at 2455–56 (illustrating the difficulties in addressing the flaw in only the less-critical system).
361 See id. at 2455 (“[P]unishments should encourage attacks that fall shortest of their full destructive potential, at the very least by taking into account the gap between potential and actual damage during sentencing.”).
C. Contractual Prohibitions

While statutory prohibitions provide for some serious hurdles for security researchers, contractual obligations may also contribute to the restrictive information security research environment. The contractual perspective of security research, coming into play in many bug bounty programs, has only recently received serious academic attention. Bug bounty programs typically represent a contractual relationship between the sponsoring company and the security researcher, meaning that both sides are bound by the terms of the contract. At the same time, due to differences in bargaining power, as well as stakes, the contractual language does not always provide for a “safe harbor” for security researchers.

Many bug bounty contracts surveyed by Elazari Bar On suggest that the language contained within these agreements does not mention “authorization,” which is required in order to establish the legality of security research. For example, the language usually requires that security researchers “comply with ‘all applicable laws’” which could defeat the purpose of security research and expose these individuals to legal jeopardy. Some contractual language also prohibits reverse engineering, which is a commonly used tool to identify security vulnerabilities. In general, there is a growing awareness to ambiguous contractual language that shifts the risk to security researchers, with researchers recommending that safe harbors are incorporated in bug bounty guidelines across the board.

V. CREATING A SECURE HYPERCONNECTED WORLD THROUGH LAW

If law, and the institutions creating, enforcing, and interpreting it, were to recognize the benefits of ethical hacking, this could help resolve many systematic shortcomings in what experts call the “security theater.”

First, incentivizing ethical hackers to report vulnerabilities to the vendor would decrease the overall number of unpatched vulnerabilities, narrowing

---

362 See Elazari Bar On, supra note 233 (manuscript at 3) (describing the increased use of “bug bounty” programs).
363 See id. at 7 (explaining contractual nature of “bug bounty” programs).
364 See id. at 12 (noting lack of safe-harbor provisions in many contracts).
365 See id. at 26–27 (pointing out that many contracts do not explicitly exempt hackers from liability).
366 See id. at 26.
367 See id. at 27 (discussing prohibitions on reverse engineering).
368 See Elazari Bar On, supra note 233 (manuscript at 13) (overviewing the current difficulties with common “bug bounty” contractual language).
369 Similarly, Bruce Schneier refers to a related phenomenon as “security theater,” which is “security measures that make people feel more secure without doing anything to actually improve their security.” Bruce Schneier, Beyond Security Theater, SCHNEIER ON SECURITY (Nov. 2009), https://www.schneier.com/essays/archives/2009/11/beyond_security_thea.html [https://perma.cc/MA42-LQNM].
down the opportunities for adversaries to attack the IoT ecosystem. This could also pressure the IoT industry to create secure devices, as companies will attempt to avoid public shaming based on flaws in their software detected by ethical hackers. This will by no means prevent malicious hacking entirely; it may, however, decrease its likelihood, by increasing the costs associated with mounting a cyber-attack and enabling more targeted and efficient law enforcement efforts to deal with the most serious offenses. This could be achieved through clear distinctions between malicious and benevolent actors and through certain legislative and administrative adjustments, such as clarification of the boundaries of the CFAA and DMCA in relation to security research.

Second, there should be consensus on how to disclose vulnerabilities in an acceptable manner. At present, the philosophy on disclosure is highly fragmented and context-dependent. In *The Hacker’s Aegis*, Derek Bambauer and Oliver Day recommend that security researchers adhere to five rules of thumb, in exchange for immunity from civil liability: report the vulnerability to the vendor first; do not sell it; test on the researcher’s own system; do not weaponized it; and create a trail. While these rules are certainly helpful, there is still a need to revisit the fundamental disagreement over disclosure practices.

Finally, allowing security researchers to snoop around for vulnerabilities is insufficient on its own; important modifications should support efforts to patch flaws in software. Such modifications might include requiring that vendors embed built-in *patchability* into IoT devices, using privacy tort law to address

---


371 See *Immunizing the Internet*, supra note 17, at 2450 (“[M]edia coverage, and user complaints can prompt vendors to take action” otherwise, “vendors would be more complacent.”).


373 See Bambauer & Day, supra note 20, at 1088 (laying out five suggested rules for hackers).
potential externalities associated with security research, tackling vendors who employ the “security by obscurity” practice, and empowering the FTC to enforce cybersecurity and vulnerability management practices against rogue vendors. These modifications are required in order to achieve a truly secure IoT ecosystem, one that encourages vendor accountability and cooperation.

A. Distinguishing Malicious from Benign Hackers

The main difficulty with the proposition that security research should not be impeded by legal hurdles is that it is somewhat burdensome to draw a clear line between benign and malicious activities in cyberspace. This difficulty mainly arises because hackers use the same tools regardless of their motives.

There are factors, however, that distinguish between malicious and benign hackers, though they are highly dependent on the specific case and facts in question. It is one thing to discover a vulnerability, and it is quite a different thing to exploit that vulnerability to its full disruptive and destructive potential. The red line here should be focused on weaponization and exploitation—whether the hacker simply identified a flaw and reported it responsibly to the vendor (ethical hacking), or whether she or he exploited it to cause damage (malicious hacking). This is a case-by-case assessment that should focus on whether the hacker used tools and techniques that caused minimal harm given the specific circumstances.

The central part of this assessment is the nature of the vulnerability. Some vulnerabilities allow access to certain protected information; others grant full administrator privileges; and some could even result in malfunction or destruction of the hacked device. The dividing line is between reasonable tools and effects of vulnerability research versus unreasonable techniques that cause damage beyond what is required to identify the flaw.

Weaponization of a vulnerability can indicate that a hacker is motivated not by a desire to fix flaws but rather by a wish to monetize or exploit the vulnerability in a manner that causes damage to the unsecure computer systems and networks and thus violates the law. However, weaponizing a

---

374 See generally Larisa April Long, Profiling Hackers, SANS INST. INFOSEC READING ROOM 6 (Jan. 26, 2012), https://www.sans.org/reading-room/whitepapers/hackers/profiling-hackers-33864 [https://perma.cc/348P-9QSX] (“While the law is clear concerning hacking, the definition gets a bit fuzzy among the general population and even computer professionals. Added into this mix are the Gray Hats, or Ethical Hackers, who blur the line between White and Black.”).

375 See Paul N. Stockton & Michele Golabek-Goldman, Curbing the Market for Cyber Weapons, 32 YALE L. & POL’Y REV. 239, 244 (2013) (“As an alternative to engaging in ‘responsible disclosure,’ a researcher could instead ‘exploit’ or weaponize the 0-day vulnerability.”).

vulnerability (creating a mechanism to exploit the vulnerability) requires a tremendous amount of time and resources, and such a substantial activity would make it easier for law enforcement to determine whether the act in question is malicious or benign, since the effort of weaponizing is not trivial.\footnote{See Stockton & Golabek-Goldman, supra note 375, at 245 ("Transforming a vulnerability into a weaponized exploit may require significant investments of time, money, and resources.").}

Supplementing factors include whether hackers cooperate with law enforcement (if it comes to that), whether they disclose their actions and findings to the vendor, and whether they provide as much information as possible to relevant agencies, if needed—for example, reporting a pacemaker vulnerability to the FDA, or using US-CERT as an intermediary in the process.\footnote{See Battery Performance Alert and Cybersecurity Firmware Updates for Certain Abbott (Formerly St. Jude Medical) Implantable Cardiac Devices: FDA Safety Communication, FOOD & DRUG ADMIN. (Apr. 17, 2018), https://www.fda.gov/MedicalDevices/Safety/AlertsandNotices/ucm604706.htm [https://perma.cc/ZY65-UDPH] (explaining that “[t]he FDA takes reports of vulnerabilities in medical devices very seriously").}

At least one commentator argues that if a security researcher notifies the vendor within 24-48 hours of his or her activities, it should provide a “safe-harbor” in terms of CFAA liability.\footnote{See Kirsch, supra note 179, at 400 (offering a model for a safe harbor provision).}

\section*{B. Legislative and Administrative Efforts to Date}

Congress has realized the importance of ethical hacking on many occasions, primarily in proposed legislation initiatives. Recently, the Senate introduced a bipartisan “Internet of Things (IoT) Cybersecurity Improvement Act of 2017” bill, proposing, among other things, to amend the CFAA and DMCA to allow good-faith security research of “Internet-connected device(s)” used by a “department or agency of the United States.”\footnote{See Internet of Things Cybersecurity Improvement Act of 2017, S. 1691, 115th Cong. § 3(k)(1) (2017) [hereinafter IoT Bill].}

The bill expands the notion of security research, which is already part of the DMCA exemption, to IoT devices used by the U.S. government and its agencies, removing the legal barriers if researchers follow a clear set of guidelines.\footnote{See id. § 3(k)(2).}

This addresses part of the critique this Article makes of the current DMCA exemption for security research, which excludes a whole subset of Internet-connected devices.\footnote{See, e.g., supra notes 288–290 and accompanying text.}

The bill also requests that IoT contractors certify that their devices do not have any known vulnerabilities and that they are patchable and follow industry-standard protocols.\footnote{See IoT Bill, § 3(a)(1)(A)(i).}

\begin{footnotesize}
\footcites{377}{See Kirsch, supra note 179, at 400 (offering a model for a safe harbor provision).}
\footcites{378}{See Stockton & Golabek-Goldman, supra note 375, at 245 ("Transforming a vulnerability into a weaponized exploit may require significant investments of time, money, and resources.").}
\footcites{379}{See Kirsch, supra note 179, at 400 (offering a model for a safe harbor provision).}
\footcites{380}{See IoT Bill, § 3(k)(1) (2017) [hereinafter IoT Bill].}
\footcites{381}{See id. § 3(k)(2).}
\footcites{382}{See, e.g., supra notes 288–290 and accompanying text.}
\footcites{383}{See IoT Bill, § 3(a)(1)(A)(i).}
\end{footnotesize}
Protection and Programs Directorate (NPPD) to create guidelines, in consultation with security researchers, for vulnerability disclosure. At present, and as discussed below, there is no uniform federally mandated vulnerability disclosure procedure, and creating authoritative rules in this area is of the utmost importance. However, this bill creates only minimal standards of cybersecurity and includes exceptions that still leave many potential gaps.

Additionally, in response to the Jeep hack, the Senate introduced a bill that deals specifically with vehicle security by requiring isolation of critical software systems from other internal networks as well as penetration testing by security analysts and onboard systems to detect malicious activity. Considering that vehicle software may have as many as a hundred million lines of code, substantially more than other software, this vehicle-specific bill makes a lot of sense. This demonstrates the magnitude of potential individuals (and vehicles) affected by unpatched bugs, the fact that it was not the vehicle manufacturer that identified the vulnerability, and that Congress realizes the looming threat of Internet-connected vehicles running flawed software. This has also led the vehicle industry to invest more in cybersecurity efforts. Volkswagen, for example, has established its very own cybersecurity firm with the goal of preventing hacking.

Recently, Congress, realizing how integral ethical hacking is to overall cybersecurity, has attempted to come up with a resolution that proactively promotes ethical hacking, including a bill creating a bug bounty program for vulnerabilities disclosed in a “Hack the Department of Homeland Security” program. Other departments announced similar challenges for private

384 See id. § 3(b)(1).
385 See id.
390 See Maggie Hassan & Rob Portman, Why We’re Encouraging Ethical Hackers to Try and Hack the Department of Homeland Security, TIME (June 30, 2017), http://time.com/4837557/hackers-homeland-security-cyber-attacks [https://perma.cc/SHB6-RTMG] (arguing that “one of the best ways to protect places like DHS is actually to recruit
citizens, including the Department of Defense ("Hack the Pentagon"), which also contacted the well-known vulnerability coordination platform HackerOne in order to facilitate a vulnerability disclosure program for private security researchers.

C. Clarifying CFAA and DMCA Boundaries

Clarifying the boundaries of the CFAA, DMCA, and bug bounty contracts as pertaining to security researchers is immensely important. The CFAA’s strict liability for access “without authorization” is certainly a major threat to security researchers. At the same time, it discourages talented researchers from engaging responsibly with vendors. Although there have been many calls to reform the CFAA in recent years, this Article advances a proposal focused on the DOJ, the prosecuting authority of the CFAA. The DOJ already acknowledged in the McDanel case that it had erred when it prosecuted an employee exposing a vulnerability in his employer’s product. This, however, is only one individual case and does not necessarily provide guidance for potential future prosecutions of security researchers engaged in vulnerability snooping.


393 See Hack the Pentagon, HACKERONE, https://www.hackerone.com/resources/hack-the-pentagon (noting that the first vulnerability was reported 13 minutes after the launch of the program).

394 See McBoyle v. United States, 283 U.S. 25, 27 (1931) (noting that creation of new crimes requires giving “fair warning...in a language that the common world will understand”).


396 See Kerr, Vagueness, supra note 319, at 1561.

397 See also Jennifer Granick, Thoughts on Orin Kerr’s CFAA Reform Proposals: A Great Second Step, STAN. CTR. FOR INTERNET & SOC’Y BLOG (Jan. 23, 2013), http://cyberlaw.stanford.edu/blog/2013/01/thoughts-orin-kerrs-cfaa-reform-proposals-great-second-step (suggesting possible amendments that could be made to the CFAA).

398 See, e.g., Freeman, supra note 36, at 129.

The recommendation, therefore, is to facilitate publicly available CFAA enforcement guidelines in the context of security research. This would ensure that white- and gray-hat-hackers engaging in vulnerability research are aware of the boundaries and limitations and of their rights and duties. For example, a simple port scan, a basic operation used to learn about services running on a computer and entryways into the system, could lead to prosecution under the CFAA.\textsuperscript{400} While this is clearly absurd in the eyes of security researchers, law enforcement authorities may not have the same perspective. This is just one example of the many basic activities of security researchers on which the CFAA should elaborate, particularly in light of the Senate Judiciary Committee’s statement during the passage of Section 1030(a)(2) clarifying that “mere observation of the data” is enough to qualify as “obtaining information,”\textsuperscript{401} a constitutive element of the crime of unauthorized access.\textsuperscript{402} This would place security researchers who do not copy, exfiltrate, or steal protected information under potential criminal liability.

Recently, the DOJ released to the public a Memorandum by the Attorney General setting guidelines for consistent law enforcement of “Computer Crime Matters.”\textsuperscript{403} While the Memorandum does acknowledge that federal criminal statutes “have not kept pace uniformly with developments in technology,” it does not acknowledge the emerging unsecure IoT ecosystem and the role of ethical hackers.\textsuperscript{404} The Memorandum offers certain factors for consideration in CFAA prosecutions, such as the sensitivity of the computer system affected, national security concerns, and any nexus to a larger criminal endeavor.\textsuperscript{405}

The DMCA exemption for security research also raises questions in relation to scope and the meanings of key terms. Since exemptions expire after three years, requiring renewed submission of petitions for exemptions, that could be an opportunity to further clarify what a security research exemption means,

\textsuperscript{400} Though, a U.S. district court in \textit{Moulton v. VC3} ruled that a port scan is not in violation of the CFAA, its decision does not have binding authority. \textit{See Moulton v. VC3, No. 1:00CV434-TWT, 2000 WL 33310901, at *6 (N.D. Ga. Nov. 7, 2000).}

\textsuperscript{401} S. COMM. ON THE JUDICIARY REP. NO. 99 432, at 6–7 (1986).

\textsuperscript{402} \textit{Id.} (“Because the premise of this subsection is privacy protection, the Committee wishes to make clear that ‘obtaining information’ in this context includes mere observation of the data. Actual asportation, in the sense of physically removing the data from its original location or transcribing the data, need not be proved in order to establish a violation of this subsection.”).


\textsuperscript{404} \textit{Id.}

\textsuperscript{405} \textit{See id.} at 1–2.
especially when it comes to devices not for individual consumer use, and the meaning of “controlled environment” in the age of cloud computing.406

So far, it appears that the Department of Justice is expected to take a liberal approach to the next iteration of the DMCA security research exemption.407 In its comments for the next triennial rulemaking process, the DOJ emphasizes it’s “support for legitimate security research and its appreciation of how such research benefits the public by identifying errors and vulnerabilities in software, digital devices and networks, developing solutions to fix them, and preventing them from being exploited by criminals.”408

In the same letter, the DOJ addresses many of the challenges addressed by this Article in relation with the DMCA.409 First, it notes that the rationale behind the scope of devices covered by the exemption is unclear, recommending an expansion of that scope to include devices not primarily designed for individual use.410 Second, it objects to the “Controlled Environment Limitation,” suggesting that some security research needs to take place in real world circumstances.411 Third, it asks whether “lawfully acquired” is a necessary condition for the legitimacy of security research.412 Overall, it illustrates a conceptual shift which recognizes that security research should not be restricted by arbitrary and unnecessary requirements, as provided by the sixth triennial review security research exemption.413

D. Requiring Built-In Patchability in IoT Devices

The important work of security researchers in the field of IoT security will not bear any fruit if IoT devices cannot be patched in the first place. While computer users generally have control over what they install, this is not necessarily the case in the IoT context, where users have limited control over security features and have to trust the vendor to ensure up-to-date and secure software.414 This means that regulators would have to require vendors to


408 Id. at 2.

409 Id.

410 Id. at 4.

411 Id.

412 Id. at 5.

413 See U.S. Dep’t of Justice, supra note 407, at 6.

414 See FTC STAFF REPORT, supra note 8, at v.
manufacture IoT devices that can be patched if security flaws are discovered. The reality is that the market does not incentivize vendors to do so; we must therefore consider a regulatory approach.415

Patchability has been an important topic of discussion in the IoT regulation context. Many agencies, including the FTC and NTIA, have been strong proponents of patchability as a requirement for responsible IoT manufacturing.416 Patching is a substantial part of overall security, but it is by no means a magic solution. Many users do not patch their software (if given a choice),417 certain organizations, such as hospitals and power plants, cannot patch immediately due to concerns that the patch may create functionality problems;418 and patches often have flaws themselves.419

E. Privacy Tort Law Solutions

Allowing individual hackers to perform security research may put privacy at risk should researchers encounter sensitive private information.420 Users

415 See Paez & La Marca, supra note 111, at 53 (“[M]anufacturers often lack an economic incentive to provide software updates and support: manufacturers of specialized computer chips, which are cheap and operate on a thin profit margin, are typically working on or shipping the next version of the chip, while the original device manufacturers—who often do not get their brand name on the finished product—are working to upgrade their product to support the new chip. In this mindset, where getting the product to the market is the overwhelming priority, security may not be a priority.”).


417 Immunizing the Internet, supra note 17, at 2449.


419 See Kesan & Hayes, supra note 27, at 787.

420 Some guidance could be provided by laws dealing with the protection of certain types of information. See, e.g., 45 C.F.R. § 164.306 (2010) (Health Insurance Portability and Accessibility Act—HIPAA) (providing the security standards for electronic protected health information).
whose private information is compromised or disseminated to the public should have legal recourse. In this context, privacy tort law may provide a partial remedy for informational harms caused by security research, even in cases where the private information is not otherwise protected by data protection laws.\textsuperscript{421} Recent literature focuses on two torts—intrusion upon seclusion and publicity given to private life.\textsuperscript{422}

So far, courts have largely dismissed data breach lawsuits by consumers against vendors, ruling that if consumers do not suffer quantifiable harm, there is no legal cause of action.\textsuperscript{423} These, however, are lawsuits against vendors; courts may reach a different conclusion if the defendant is a security researcher who overstepped the boundaries of his or her specific research, though proving harm will still be a necessary component.\textsuperscript{424}

F. Vulnerability Disclosure Procedure

The process by which vulnerabilities are disclosed has been a contentious topic in recent years.\textsuperscript{425} Vulnerability disclosure\textsuperscript{426} is essentially a double-edged sword; the benefits extracted from it are largely dependent on the methods of disclosure, including the parties who learn about it and what they decide to do with that information.\textsuperscript{427} Intuition suggests that once security researchers

\textsuperscript{421} See Tran, supra note 157, at 266.
\textsuperscript{422} See id. at 280.
\textsuperscript{423} See The Liability of Technology Companies for Data Breaches, ZURICH (ADVISEN) 5 (2010), https://www.advisen.com/downloads/Emerging_Cyber_Tech.pdf [https://perma.cc/2ENA-WAKT] (“Legal experts note that the majority of courts have rejected data breach claims brought by affected persons that did not suffer any appreciable injury. Simply having one’s personal information lost or stolen may not be sufficient, as the plaintiff must actually have suffered a loss in order to claim damages.”).
\textsuperscript{424} See U.S. DEP’T. OF HOMELAND SEC., STRATEGIC PRINCIPLES FOR SECURING THE INTERNET OF THINGS (IoT), at 5 (Nov. 15, 2016), https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL.pdf [https://perma.cc/T9V6-YF7R] (suggesting that “[w]hile there is not yet an established body of case law addressing IoT context, traditional tort principles of product liability can be expected to apply”).
\textsuperscript{425} Brenner, supra note 14, at 405 (arguing that the controversy about vulnerability disclosure is over how the information is disseminated); see, e.g., BugTraq: Frequently Asked Questions, SECURITY FOCUS ONLINE, https://www.securityfocus.com/archive/1/description [https://perma.cc/2LYY-QE88]; Scott Culp, It’s Time to End Information Anarchy, MICROSOFT SECURITY ESSAYS (Oct. 2001), http://www.angelfire.com/ky/microsfot/timeToEnd.html [https://perma.cc/CK54-SBNB].
\textsuperscript{426} See AMRIT T. WILLIAMS ET AL., RESPONSIBLE VULNERABILITY DISCLOSURE: GUIDANCE FOR RESEARCHERS, VENDORS AND END USERS, GARTNER 3 (Oct. 17, 2006), http://attrition.org/misc/ce/gartner-responsible_disclosure-144061.pdf [https://perma.cc/TVSS-SB6R] (“Publicity over vulnerabilities in software products is a double-edged sword. Making vulnerabilities public has, unfortunately, proved necessary to spur some software vendors to invest in better software development, patch production and patch distribution processes. However, it has also enabled attackers to more quickly produce exploits.”).
\textsuperscript{427} See id.
identify a vulnerability, they should disclose it to the relevant party, who would in turn fix or patch the flaw, thereby enhancing the overall security of the software.\footnote{See Bruce Schneier, Schneier: Full Disclosure of Security Vulnerabilities a ‘Damned Good Idea,’ SCHNEIER ON SECURITY (Jan. 9, 2007), https://www.schneier.com/essays/archives/2007/01/schneier_full_disclo.html [https://perma.cc/V4DE-NLL4].} In the words of then-Secretary of Defense Ash Carter this would be the equivalent of a “‘see something, say something’ policy for the digital domain.”\footnote{See U.S. DEP’T. OF DEF., supra note 46.} Reality, however, has been slightly more complicated than that.

While disclosing vulnerabilities to the vendor was the norm for many years, security researchers became increasingly frustrated because they were often ignored by vendors, who were reluctant investigate reported vulnerabilities.\footnote{See Schneier, supra note 428.} At that point, researchers published only very limited information about the existence of a vulnerability to the public, which resulted in some vendors claiming these vulnerabilities were “theoretical.”\footnote{See id.} Only when security researchers finally published the information they had to the public in full did vendors start taking these matters seriously.\footnote{See id.} This has led to a fragmentation of the philosophy on vulnerability disclosure.\footnote{See Marc Laliberte, A Look Inside Responsible Vulnerability Disclosure, DARK READING (Jan. 5, 2017), http://www.darkreading.com/threat-intelligence/a-look-inside-responsible-vulnerability-disclosure/a/d-id/1327800 [https://perma.cc/T54M-PVZ8].} While certain experts advocate for “responsible disclosure,” which primarily focuses on disclosing vulnerabilities to the vendor, there is a strong group of experts who oppose that approach and argue for “full disclosure,” encouraging security researchers to publish the flaws they have identified to the broader public and assuming the vendor will then be pressured to fix the flaw more promptly.\footnote{Freeman, supra note 36, at 128.} There is a substantial group of individuals and organizations who adopt the “nondisclosure” approach to vulnerabilities, mainly black hats and intelligence agencies such as the National Security Agency (NSA).\footnote{See generally Bruce Schneier, The NSA Is Hoarding Vulnerabilities, SCHNEIER ON SECURITY (Aug. 26, 2016), https://www.schneier.com/blog/archives/2016/08/the_nsa_is_hoar.html [https://perma.cc/SK5R-7769] (explaining how the NSA is hoarding vulnerabilities of software used both by private and governmental entities, including companies like Cisco, Fortinet, TOPSEC, and more. A portion of these vulnerabilities were patched since, but some vulnerabilities were still unknown until a group named Shadow Brokers leaked 300 megabytes worth of NSA-hoarded vulnerabilities).}

1. Responsible Disclosure

Responsible disclosure typically refers to reporting a vulnerability to the relevant vendor and allowing the vendor a certain amount of time to fix the
vulnerability, depending on its complexity and other circumstances. This type of disclosure is the most commonly used approach by vendors, who naturally prefer to learn about the vulnerability before other parties or the public. Initially, the DMCA exemption for security research was expected to include a requirement of responsible disclosure as part of its good-faith term. However, the Librarian of Congress noted that the community was divided on what constituted responsible disclosure and that therefore the DMCA rulemaking did not require responsible disclosure, or any other type of disclosure, other than requiring that information gathered be used primarily “to promote the security or safety” of the device in question.

This is not to say that the public will not learn about the vulnerability; rather, such information will be released to the public only once a patch is released and the risk of exploitation by third parties decreases. Another variation of

---

436 See Laliberte, supra note 433 (“First, the researcher identifies a security vulnerability and its potential impact . . . . Next, the researcher creates a vulnerability advisory report including a detailed description of the vulnerability, supporting evidence, and a full disclosure timeline . . . . After submitting the advisory to the vendor, the researcher typically allows the vendor a reasonable amount of time to investigate and fix the exploit . . . . Finally, once a patch is available or the disclosure timeline (including any extensions) has elapsed, the researcher publishes a full disclosure analysis of the vulnerability.”).

437 See, e.g., Art Manion, Vulnerability Disclosure Policy, CERT COORDINATION CTR. (Feb. 19, 2018), http://www.cert.org/vulnerability-analysis/vul-disclosure.cfm? [https://perma.cc/6XH8-6ZG7] (providing that “[v]ulnerabilities reported . . . will be disclosed to the public 45 days after the initial report, regardless of the existence or availability of patches”); see also Chris Evans & Drew Hintz, Disclosure Timeline for Vulnerabilities Under Active Attack, GOOGLE SEC. BLOG (May 29, 2013), https://security.googleblog.com/2013/05/disclosure-timeline-for-vulnerabilities.html [https://perma.cc/9MSM-LEDV] (“Our standing recommendation is that companies should fix critical vulnerabilities within 60 days—or, if a fix is not possible, they should notify the public about the risk and offer workarounds.”).


439 See id. (“As explained above, a significant issue with respect to the security exemptions involves the proper disclosure of security research findings, as the interests of the manufacturer and the public may both be affected by the nature and timing of disclosure of software flaws. Indeed, Congress included disclosure to the system developer as one of the factors to be considered in determining a person’s eligibility for the security testing exemption in section 1201(j). Although the Register expressed support for responsible disclosure of security flaws, she acknowledged the difficulty of attempting to define disclosure standards in the context of this rulemaking, as opinions seem sharply divided on this point. Accordingly, rather than incorporating an express disclosure rule, the recommended exemption draws upon what the Register perceives to be the basic intent of section 1201(j) by specifying that the information derived from the research activity be used primarily to promote the security or safety of the devices containing the computer programs on which the research is conducted, or of those who use those devices.”).

responsible disclosure is reporting all information regarding the vulnerability to the vendor while disclosing only limited information, excluding the proof of concept, to the public.\footnote{See Coders’ Rights Project Vulnerability Reporting FAQ, ELECTRONIC FRONTIER FOUND., https://www.eff.org/issues/coders/vulnerability-reporting-faq [https://perma.cc/LB97-Y5C9].} However, even that approach does not necessarily prevent malicious hackers from reverse-engineering the general vulnerability information that is provided to the public.\footnote{See Bambauer & Day, supra note 20, at 1064 (explaining that “if they describe flaws with too much precision, hackers can probe the weaknesses, but if they are too general, customers will encounter difficulty taking precautions”).} The general idea is to ensure that the public will not be able to directly use the information to exploit the vulnerability.

2. Full Disclosure

Full disclosure, unlike responsible disclosure, is the practice of reporting a vulnerability to the public to the fullest extent possible and without informing the vendor of it beforehand.\footnote{See Taiwo A. Oriola, Bugs for Sale: Legal and Ethical Properties of the Market in Software Vulnerabilities, 28 J. MARSHALL COMPUTER & INFO. L. 451, 483 (2011) (“[A] full disclosure occurs where independent security analysts promptly post vulnerabilities to a public listing.”).} The practice of full disclosure is evidence of some of the frustration of the security research community resulting from vendors sometimes ignoring vulnerabilities reported to them.\footnote{See Lynch, supra note 440 (arguing that full disclosure is controversial because it creates a race between vendors and potential exploiters, who both have equal access to the information pertaining to the vulnerability).} It is immensely controversial because it allows equal access to information about a vulnerability to vendors and to potential exploiters.\footnote{See Schneier, supra note 444.} The idea behind full disclosure is to pressure the vendor to patch the vulnerability since public scrutiny is a strong motivation for vendors to take security seriously.\footnote{Schneier, supra.} Bruce Schneier, a supporter of the full disclosure practice, called it a “damned good idea,”\footnote{See Schneier, supra note 447 and many others agree.} and many others agree.\footnote{See, e.g., Kevin Johnson, Exposing the Fallacies of Security by Obscurity: Full Disclosure, ISACA (2017), https://www.isaca.org/Journal/archives/2017/Volume-5/Pages/exposing-the-fallacies-of-security-by-obscurity.aspx [https://perma.cc/E4CW-QAJC].}

However, full disclosure is not always a provocative step against vendors. It is often used to publish information about a vulnerability so that customers can protect themselves from exploitation, given that the vendor will either ignore or take too long to fix the flaw.\footnote{See Schneier, supra note 449.} Many assume that full disclosure
allows malicious actors to exploit vulnerabilities published by security researchers, but there is an assumption that black-hat hackers are aware of certain vulnerabilities, if not sold to them in the zero-day vulnerability market.\(^{450}\)

3. The Road Forward on Vulnerability Disclosure

This subpart has demonstrated that the debate over vulnerability disclosure stems from distrust between security researchers and vendors.\(^{451}\) But security researchers could regain their trust in vendors, and vice versa, if a robust form of oversight is implemented. This can be achieved by relying on intermediaries and enforcers of norms in that context—for example, US-CERT and the FTC. Primarily, this will require official guidelines from an authoritative body (the FTC, for example) regarding how to responsibly disclose vulnerabilities in a way that properly balances vendors’ interests and the need for cybersecurity.

G. Transnational Law Enforcement and Reducing National Security Threats

The DOJ recently indicted a group of Russian FSB officers who were involved in hacking Yahoo!, gaining access to as many as 500 million e-mail accounts.\(^{452}\) Transnational law enforcement is expensive and resource-intensive. In an environment friendlier to ethical hacking, where tech companies do not threaten security researchers, such a massive data breach could have been prevented. In addition, the FBI has already admitted that it is losing the “war on hackers,”\(^{453}\) which indicates that law enforcement may be increasingly inclined to consider “alternative architectures that are more secure” in the first place.\(^{454}\)

\(^{450}\) See Schneier, supra note 430.


Patching vulnerabilities before foreign governments learn about them could enhance overall national security. If we assume that national security includes dams, transportation, healthcare, and other sectors operating on information technology, we might also conclude that patching vulnerabilities in advance would keep foreign malicious actors largely at bay, since their options to attack the cyber infrastructure would be limited to only zero-day vulnerabilities, which would be far more limited than the number of vulnerabilities that could be identified by ethical hackers and patched by the manufacturer.

H. Tackling Security by Obscurity

The concept of security by obscurity provides that keeping the code for a particular piece of software, and therefore vulnerabilities in that code, hidden and unknown to hackers can make the software seemingly more secure. In software engineering, this is sometimes called “obfuscation.” Vendors may make their code overly complex or ridden with gibberish code lines in order to confuse a potential attacker. But this has not worked in the past, and it will not work in the future. In today’s cybersecurity world, it is almost impossible to hide vulnerabilities; the only way to prevent their exploitation is to patch them and get rid of them. Security by obscurity also violates Kerckhoff’s principle, which posits that the public release of a system should not be to its

458 See, e.g., Johnson, supra note 448.
459 Michael Gegick & Sean Barnum, Never Assuming That Your Secrets Are Safe, US-CERT (Sept. 14, 2005), https://www.us-cert.gov/bsi/articles/knowledge/principles/never-assuming-that-your-secrets-are-safe [https://perma.cc/UBB2-JF9H] (“Always assume that an attacker knows everything that you know -- assume the attacker has access to all source code and all designs. Even if this is not true, it is trivially easy for an attacker to determine obscured information.”) (citing Michael Howard & David LeBlanc, Chapter 3: Security Principles to Live By, in NEVER DEPEND ON SECURITY THROUGH OBSCURITY ALONE 66–67 (2d ed. 2003)).
460 See Johansson & Grimes, supra note 457 (“Security by obscurity is, in a nutshell, a violation of Kerckhoffs’ Principle, which holds that a system should be secure because of its design, not because the design is unknown to an adversary. The basic premise of Kerckhoffs’ Principle is that secrets don’t remain secret for very long.”). But see Corey Nachreiner, How a Little Obscurity Can Bolster Security, DARK READING (Apr. 17, 2014), http://www.darkreading.com/risk/how-a-little-obscurity-can-bolster-security/d/d-id/1204452 [https://perma.cc/NN23-Y98E].
detriment, since systems should be secure by design, not due to their confusing nature.461

This shows that the emphasis on securing IoT devices should be on revealing vulnerabilities, possibly providing an incentive for individuals to do so, as well as on patching those vulnerabilities, which is the responsibility of the vendor.

In this regard, the FTC can play an important role. The FTC has been recently actively enforcing consumer privacy based on Section 5 of the Federal Trade Commission Act, which prohibits “unfair or deceptive acts or practices in or affecting commerce.”462 The FTC has become a de facto data protection authority.463 Given that the degree of privacy could be affected by the strength of security, the FTC ought to ensure that companies do not engage in practices that could compromise private information belonging to consumers, with security by obscurity being one of those practices.464 Furthermore, the Third Circuit in FTC v. Wyndham held that the FTC has authority to sue for inadequate security practices.465

This common law of FTC privacy enforcement could lead to stronger enforcement against companies who do not act according to industry best practices of privacy and security.466 Security by obscurity, a practice that certain vendors adopt in order to avoid vulnerability detection,467 should be treated as a deceptive or unfair practice in the same way the FTC deals with other security-violating practices.468 The FTC has already pursued action against an IoT vendor, TRENDnet, in a claim that its smart webcams did not provide consumers with “reasonable security to prevent unauthorized access to sensitive information, namely the live feeds from the IP cameras.”469 It is anticipated that

---

461 See Bruce Schneier, Secrecy, Security, and Obscurity, SCHNEIER ON SECURITY (May 15, 2002), https://www.schneier.com/crypto-gram/archives/2002/0515.html [https://perma.cc/9W47-499M] (“Today, there is considerable benefit in publication, and there is even more benefit from using already published, already analyzed, designs of others. Keeping these designs secret is needless obscurity. Kerckhoffs’ Principle says that there should be no security deterrent from publication.”).
466 See Solove & Hartzog, supra note 464, at 653 (providing examples of FTC common law of privacy enforcement against companies for “[f]ailure to implement cheap, easy-to-use, or common industry security practices”).
467 See Johansson & Grimes, supra note 457.
468 See Solove & Hartzog, supra note 464, at 637 (“In the early 2000s, the FTC initiated a flurry of activity around security—nearly overshadowing its privacy cases.”).
469 See Trendnet, Inc., No. 122-3090, 2013 WL 4858250, at *2–3 (F.T.C. Sept. 3, 2013) (“[A]s a result, hackers exploited the security vulnerabilities leading to ‘compromised live feeds display[ing] private areas of users’ homes and allow[ing] the unauthorized surveillance...”)
the FTC will pursue further enforcement against IoT vendors who engage in unfair or deceptive security or privacy practices, which should encompass practices like security by obscurity and, perhaps, unwillingness to respond to vulnerability disclosures.470

VI. CONCLUSION

This Article argues that the DMCA, CFAA, and certain contractual prohibitions impede security research into software vulnerabilities, which are on the rise in the emerging IoT ecosystem due to an industry-specific market failure. Contractual language could also put security researchers in legal jeopardy should it not contain safe harbor and authorization provisions. These legal barriers discourage security researchers from discovering flaws and reporting them to the relevant vendors, which would enhance overall privacy and security. This could be partially resolved by mitigating the threat of legal jeopardy through a further development of the DMCA exemption and reconsideration of the CFAA boundaries as well as by enacting legal and regulatory adaptations such as requiring patchability in IoT, tackling security by obscurity, and enforcing the law against noncomplying vendors. This will create a friendly and fruitful environment for security research, leading to a more secure IoT ecosystem and, ultimately, a more secure Internet system.

The IoT ecosystem creates a host of opportunities but also a variety of risks and dangers, which should be addressed through legitimizing the activities of the community of dedicated vulnerability hunters. Security research is important where market forces fail and where vendors are unlikely to discover vulnerabilities on their own, which they currently lack the incentive to do. Broad interpretation of these “anti-hacking” laws is resulting in a less secure Internet, and the stakes are constantly increasing given the ubiquity of sensors and physicality of the IoT ecosystem.

The law should clearly distinguish between white- and gray-hat hackers, whose purpose is to fix flaws (to varying degrees), and black-hat hackers, who use vulnerabilities for criminal ends. This distinction has been overlooked for too long, and IoT ought to be a turning point in that regard, creating a space for benevolent actors to fully utilize their talent.

---

470 See Hetcher, supra note 463, at 131.
Offshore Tax Enforcement and Divorce

KHRISTA MCCARDEN*

High-net-worth taxpayers continue to hide assets offshore, and offshore tax enforcement remains an immense problem for the United States. In 2016, the Panama Papers revealed another previously unnoticed reason that high-net-worth tax cheats place assets offshore: to hide them from their spouses during divorce proceedings. Typically, these offshore tax evaders also will refuse to disclose their offshore accounts during divorce proceedings even though required to do so. The individuals hiding offshore assets in this manner are predominantly males. Ultimately, their wives are forced to hire forensic accountants to trace an extensive maze of offshore ownership during the divorce.

This Article proposes a novel solution to the problem of offshore tax enforcement by using high-net-worth divorces. Currently, an offshore tax evader may frustrate his wife’s attempts to discover family assets held offshore during divorce proceedings and still remain eligible for tax amnesty programs. Moreover, he can later claim that he did not “willfully” hide assets from tax authorities and thereby escape criminal prosecution. This Article solves these two problems in a manner that will strengthen offshore tax enforcement while truncating prolonged divorce proceedings.

In addition, currently, a wife who learns of her husband’s offshore tax fraud during divorce will face civil and criminal liability as well, unless she can secure innocent spouse relief. Such relief is difficult to attain due to existing inequities and misperceptions about financial and other forms of domestic abuse. As a result, our current approach protects the guilty, high-net-worth tax cheat who refuses to disclose his offshore assets either to tax authorities or to his wife. At the same time, it diminishes the chances that his wife will ever whistle blow to the Internal Revenue Service by failing to protect her from civil and criminal liability. This Article argues for reforms in the areas of family law and tax law that would (1) hold high-net-worth husbands accountable for noncompliance in both contexts and (2) incentivize

---

* Hoffman F. Fuller Associate Professor of Tax Law, Tulane Law School; J.D. cum laude, Harvard Law School, 2003; A.B. Harvard College, magna cum laude. I am grateful to the Tulane Law School Faculty, the Sanford E. Sarasohn Conference on Critical Issues in Comparative and International Taxation, the Junior Tax Scholars Workshop, and the Critical Tax Theory Conference, for helpful feedback. My particular thanks to Paul Caron, Heather Field, Shuyi Oei, Henry Ordower, Robert Pushaw, and Diane Ring for helpful comments and critiques.
wives to whistle blow using information about offshore assets gathered from the divorce proceedings.

TABLE OF CONTENTS

I. INTRODUCTION ................................................................. 523
   A. Noncompliance in Divorce & Offshore Tax Reporting ....... 527
   B. Hold High-Net-Worth Husbands Accountable & Empower Their Wives as IRS Whistleblowers ......................... 528

II. NONCOMPLIANT SPOUSES IN THE DIVORCE AND OFFSHORE TAX CONTEXTS .................................................. 529
   A. Hiding Offshore Assets from Spouses and the IRS .......... 531
      1. Family Law Discovery Process and Tracing Offshore Assets ............................................................... 533
      2. Current Tax Consequences of Noncompliant Spouses .............................................................................. 534
      3. Offshore Reporting Requirements .......................................................... 536
   B. Willful Violation Equals Three Possible Penalties .......... 537
   C. Using Family Law Discovery Devices to Prove Willfulness ............................................................................. 538
      1. Imputing Knowledge Through Discovery Devices .......................................................... 539
      2. Willfulness in the FBAR Context .......................................................... 541
   D. Removing the Possibility of Voluntary Disclosure for Noncompliant Spouses ................................................. 543
      1. Current Pre-Clearance Procedure .......................................................... 543
      2. Proposed Ineligibility for Pre-Clearance .......................................................... 544

III. THE UNJUST DENIAL OF INNOCENT SPOUSE RELIEF FOR WIVES OF NONCOMPLIANT SPOUSES ............................... 545
   A. Joint Civil and Criminal Liability .................................................. 546
   B. Innocent Spouse Relief and Its Inadequacies ......................... 547
      2. Legislative History of Innocent Spouse Relief and Wives ............................................................................. 549
      3. Lingering State Liability .......................................................... 554
   C. Problems with the Current Approach ................................. 556
      1. Election Under Section 6015(c) .......................................................... 558
      2. Election Under Section 6015(f) .......................................................... 559
   D. Rethinking Domestic Abuse and Innocent Spouse Relief Relief .......................................................... 563
      1. Domestic Abuse Victims Married to Primary Wage Earners .......................................................... 564
      2. Preconceived Notions of Abuse .......................................................... 564
3. Correlation Between Abuse Claims & Innocent Spouse Relief ............................................................. 567
4. Problematic Corroboration Requirement ...................... 568
5. Financial Abuse Mitigates “Knowledge” .................. 569
E. Remaining Issues ............................................................ 571

IV. WIVES AS OFFSHORE WHISTLEBLOWERS DURING DIVORCE . 573
A. IRS Whistleblower Program ........................................... 574
B. Empowering Wives to Report Offshore Tax Evasion...... 577

V. CONCLUSION........................................................................ 581

I. INTRODUCTION

In the last two years, the American public has become keenly aware of hidden issues that will shape our nation’s legal landscape, debates, and choices for decades to come.¹ These developments have relevant implications for another issue related to secrecy: the hiding of offshore wealth.² According to a recent Tax Justice Network report, wealthy individuals are holding over $21 trillion to $32 trillion of unreported private wealth offshore.³ Offshore tax enforcement is a legal regime aimed at catching wealthy tax evaders that remains a top priority for the Internal Revenue Service (IRS) in 2018.⁴ However, the United States largely ignores a context where information regarding offshore assets is gleaned, i.e., high-net-worth divorce proceedings.⁵

It is undeniable and commonly known that one use of offshore accounts is to hide assets from tax authorities.⁶ Nevertheless, the Panama Papers revealed

¹ See infra notes 6–27 and accompanying text.
² Id.
⁵ See infra Part I.A.
another less obvious use of offshore accounts: hiding assets from a spouse during a divorce.\textsuperscript{7} The Panama Papers divulged that public officials, drug dealers, money launderers, and unexpectedly, high-net-worth divorcees all use offshore accounts to hide assets.\textsuperscript{8} The source of the leak was a Panamanian firm named Mossack Fonseca, and it confessed to at least considering aiding wealthy individuals with hiding assets from their spouses in a type of pre-divorce planning designed to prevent a claim to those assets.\textsuperscript{9}

In October 2017, the #MeToo movement\textsuperscript{10} and the indictment of President Trump’s former campaign manager, Paul Manafort, showed the world that powerful men also must face consequences for their misdeeds, including their offshore ones.\textsuperscript{11} Last year, the momentum of the anti-sexual harassment #MeToo movement thrust the hidden marginalization and objectification of both famous and unknown women alike into unwavering light for all to see.\textsuperscript{12} No longer would the latent sins of prominent American men remain out of focus due to the courage of women.

Later in October 2017, the indictment of Manafort for failure to report foreign bank and financial accounts, inter alia, brought the secret world of offshore companies and assets to sharp focus yet again.\textsuperscript{13} Recently, the IRS has

---


\textsuperscript{9} See Swanson, \textit{supra} note 7.


\textsuperscript{12} See Bennett, \textit{supra} note 10.

noted that individuals who maintain foreign financial accounts and fail to comply with U.S. reporting requirements “are breaking the law and risk significant fines, as well as the possibility of criminal prosecution.”14 The indictment alleges, “Manafort used his hidden overseas wealth to enjoy a lavish lifestyle in the United States, without paying taxes on that income.”15 It also contends that Manafort and Rick Gates “funneled millions of dollars in payments into foreign nominee companies and bank accounts, opened by them and their accomplices in . . . Cyprus, Saint Vincent & the Grenadines . . . and the Seychelles.”16 FBI agents entered Mr. and Mrs. Manafort’s condominium before dawn after the indictment,17 and ultimately, on August 21, 2018, Manafort was convicted of eight counts of tax and bank fraud, including one count of not reporting a foreign bank account.18 Mrs. Manafort, an attorney, has been involved with her husband’s multi-million-dollar real estate acquisitions.19 It is unclear whether she was aware of her husband’s failure to report offshore accounts.20

Meanwhile, in early 2018, former White House staff secretary Rob Porter’s two ex-wives exposed just how incorrectly the United States perceives domestic violence and abuse in alleging their former husband engaged in verbal and

---

16 Indictment, supra note 13, at 2.
17 See Scarborough, supra note 15.
19 See Áine Cain, Paul Manafort’s Wife Kathleen Has Been a Quietly Pivotal Part of the Investigation Against Him—Here’s Everything We Know, BUS. INSIDER (Oct. 31, 2017), https://www.businessinsider.in/law-order/paul-manaforts-wife-kathleen-has-been-a-quietly-pivotal-part-of-the-investigation-against-him-heres-everything-we-know/articleshow/61350660.cms [https://perma.cc/U4E3-RHLS] (explaining that Kathleen Manafort’s role in tax fraud is not lucid but noting funds from offshore accounts were used to purchase U.S. real estate, including properties in New York and Virginia); Scarborough, supra note 15. An IRS agent testified that approximately $9 million was transferred from Manafort’s offshore accounts to the United States and about $6.7 million of this amount was used to purchase personal real estate in New York and Virginia. Del Quentin Wilber & Aruna Viswanatha, IRS Agent Testifies Manafort Failed to Declare More than $16 Million on Taxes, WALL ST. J. (Aug. 8, 2018), https://www.wsj.com/articles/forensic-accountant-next-up-in-manafort-trial-as-gates-ends-testimony-1533748826 [https://perma.cc/Q3X4-MQGM].
20 Cain, supra note 19.
physical abuse.\textsuperscript{21} Porter’s second wife, Jennie Willoughby, poignantly stated: “Society as a whole doesn’t acknowledge the reality of abuse.”\textsuperscript{22} Ms. Willoughby has pointed out the cultural norm that often pervades our legal system, as well as the questioning of the victim of the abuse instead of embarrassing an abuser.\textsuperscript{23} Colbie Holderness, Porter’s first wife, noted that often women are with their abusers for an extended period of time.\textsuperscript{24} Ms. Holderness explained, “[t]hey marry them, become financially intertwined with them, have children with them.”\textsuperscript{25} Suddenly, U.S. politicians and the general public were asked to acknowledge that abuse happens to “the poor and the rich, the least educated and the most” and is committed by those with “a stellar résumé and background.”\textsuperscript{26} Ultimately, Porter stepped down from his role after these allegations surfaced.\textsuperscript{27}

Examining these three stories, several questions arise that are relevant to how we view offshore tax enforcement. What if, similar to women prior to the #MeToo movement, wives of wealthy tax evaders fear the implications of disclosing their husbands’ bad tax behavior and thus have remained silent, even during divorce? An article in the U.K. \textit{Guardian} disclosed that several members of President Trump’s Administration, including his chief economic adviser who spearheaded the latest tax reform effort, have offshore dealings, providing further evidence of an offshore network comprised of wealthy U.S. men.\textsuperscript{28}

\begin{thebibliography}{99}
\bibitem{23} See Willoughby, supra note 22. (“The tendency to avoid, deny, or cover up abuse is never really about power, or money, or an old boys’ club. It is deeper than that. Rather than embarrass an abuser, society is subconsciously trained to question a victim of abuse.”).
\bibitem{24} Holderness, supra note 21.
\bibitem{25} Id.
\bibitem{27} See Willoughby, supra note 22; Levenson, supra note 26.
Surely, some of the men in this offshore circle have gone through one or more divorces. Why did their wives choose not to inform the IRS of their husbands’ offshore holdings through the IRS Whistleblower Program?

Imagine if Mr. and Mrs. Manafort were in the process of divorce at the time of the FBI raid, and she had learned during the divorce that her husband had engaged in tax fraud and evasion. Would she provide information to the IRS and under what circumstances? What if Colbie Holderness or Jennie Willoughby had discovered during their divorces from Rob Porter that he also was engaging in offshore tax fraud and evasion? Should they have a shield from possible joint civil and criminal liability given their allegations of abuse? To summarize, the main question is the following: Are both the Department of Justice and the IRS missing out on an opportunity to impose civil and criminal liability on offshore tax evaders by failing to speak with wives during the divorce process? Relatedly, what can the United States do to empower wives who learn of offshore tax fraud and evasion during divorce proceedings to report the behavior to the IRS?

A. Noncompliance in Divorce & Offshore Tax Reporting

High-net-worth husbands who refuse to comply with the divorce discovery process and thus fail to disclose hidden offshore assets (“noncompliant spouses”) are by nature also tax frauds and evaders.29 If they were not, their wives would not have to hire forensic accountants and file motions to compel to discover an accurate financial picture.30 They could simply look at prior and current year tax returns. The ability of noncompliant spouses to escape civil and criminal liability in the tax arena, despite their bad behavior in the family law context, is perplexing.

Under current law, a noncompliant spouse is able to frustrate his wife’s attempts to discover family assets and accounts by failing to comply with discovery.31 However, at the end of the proceedings, there is no mechanism for reporting his attendant tax fraud, and he remains eligible for tax amnesty programs.32 Moreover, even if he decides to take a gamble and not divulge his tax wrongdoing under a tax amnesty program, he will likely escape criminal liability by alleging he did not know he had a legal duty to report or to pay tax on offshore income and assets, or in other words, that he did not act...
“willfully.” The government will bear a heavy burden of proving willfulness.44

Even worse, his wife likely will face civil and criminal liability as well because of the joint and several liability that attaches with the filing of joint tax returns during marriage.35 Her only chance of avoiding this result is to pursue innocent spouse relief under section 6015(c) or section 6015(f) of the Internal Revenue Code (I.R.C.).36 However, she will face an almost insurmountable obstacle because knowledge of the receipt of money not reported to the IRS is enough to disqualify her in most cases, regardless if she knew nothing about the source of such money or the failure to report it.37

The current mismatch in “knowledge” standards leads to a perverse result. A noncompliant spouse may claim that he lacked “knowledge” of tax reporting to escape liability.38 Nevertheless, his wife’s mere “knowledge” that money was received is enough to disqualify her from innocent spouse relief, i.e., her one shield against joint civil and/or criminal liability.39 Ultimately, our current law deters wives of noncompliant spouses from sharing information with the IRS about hidden offshore assets uncovered during divorce proceedings.40

B. Hold High-Net-Worth Husbands Accountable & Empower Their Wives as IRS Whistleblowers

Offshore tax enforcement may be strengthened through high-net-worth divorce proceedings by utilizing a two-fold approach. First, we must curtail the ability of noncompliant spouses to use tax amnesty programs and assist the government and/or the IRS with establishing “willfulness” on the part of such offshore tax cheats. Second, we must shield unknowing wives from shared civil and criminal liability and thereby empower them to report offshore assets discovered during divorce through the IRS Whistleblower Program. Unfortunately, innocent spouse relief is difficult to achieve even in this instance because of existing inequities and the way judges, including those in Tax Court, view financial and other forms of domestic abuse. These misperceptions must change.

Part I argues that family law discovery devices should be modified in order to impute knowledge of reporting requirements to noncompliant spouses and that noncompliant spouses should be ineligible for voluntary disclosure programs and delinquent Report of Foreign Bank and Financial Accounts (FBAR) procedures and delinquent international information return

33 See infra Part I.B.
34 See id.
35 See infra Part II.A.
36 I.R.C. §§ 6015(c)(3)(C), (f) (2012); See infra Part II.B.
37 See infra Part II.B–C.
38 Id.
39 See infra Part II.A.
40 See infra Part II.
procedures that allow taxpayers to avoid criminal prosecution and cap civil penalties. Part II examines current challenges facing wives of noncompliant spouses in obtaining relief from the joint and several liability that attaches with the filing of joint returns during the marriage, or in other words, innocent spouse relief. Relatedly, the link between financial abuse and offshore tax evasion is explored to argue for extending innocent spouse relief to this group of wives in particular. Finally, Part III proposes that innocent spouse relief would enable these wives to serve as effective whistleblowers under the IRS Whistleblower Program.

This Article’s proposed reform comes at a particularly relevant time. The IRS indicated in 2018 that stemming offshore tax evasion remains one of its main goals. Recent news stories show how widespread offshore dealings are, including among the politically prominent. They also have revealed that when women are empowered to speak out about the misdeeds of men, even those of the highest socioeconomic rankings are held accountable for violating the law. In addition, recent headlines show that wives of powerful men are not strangers to abuse. While Tax Court may not seem like the obvious place for legal reform to our notions of domestic abuse, this Article challenges that idea. It sets forth a new framework for indemnifying financially abused wives from the offshore tax sins of their high-net-worth husbands and thus encouraging them to serve as whistleblowers.

II. NONCOMPLIANT SPOUSES IN THE DIVORCE AND OFFSHORE TAX CONTEXTS*

Given the ease associated with electronically transferring funds to countries today, it has become increasingly difficult to uncover assets that have been hidden offshore. While in recent years there have been numerous efforts to combat offshore tax haven abuses—such as heavy penalties and new reporting


41 For purposes of this Article, voluntary disclosure encompasses both the Offshore Voluntary Disclosure Program (OVDP) and the delinquent FBAR submission procedures and the delinquent international information return submission procedures, which will remain open after the 2014 OVDP closure on September 28, 2018. See Closing the 2014 Offshore Voluntary Disclosure Program Frequently Asked Questions and Answers, INTERNAL REVENUE SERV., https://www.irs.gov/individuals/international-taxpayers/closing-the-2014-offshore-voluntary-disclosure-program-frequently-asked-questions-and-answers [https://perma.cc/L9T4-WX4] (last updated Nov. 30, 2018) [hereinafter Closing the 2014 OVDP] (addressing the OVDP closing at FAQs 1, 9, and 10); see also infra note 52.


43 See, e.g., Swaine & Pilkington, supra note 28; Swanson, supra note 7.

44 See HENRY, supra note 3, at 10.
requirements—a fundamental problem persists: the IRS does not have the time or resources to untangle the intricate maze of corporate structures used by wealthy individuals to hide their assets offshore. The spouses of wealthy tax evaders do. In fact, the scope of divorce cases can far exceed that of federal tax investigations because they seek to “map the wealth of the some of the world’s richest people.”

The discovery process that is an integral part of divorce proceedings is conducive to the unraveling of multiple chains of corporate ownership inherent in such “offshore planning.” Under I.R.C. § 7201, tax evasion is a felony that carries either a fine of up to $250,000, or five years’ imprisonment, or both. The three elements of the crime of tax evasion are (1) willfulness, (2) an attempt to evade tax, and (3) additional tax due.

Part I of this Article argues that discovery devices should be modified in order to impute knowledge of reporting requirements to a spouse refusing to comply with the discovery process—or what is termed a “noncompliant spouse”—given the willfulness standard applies to all three categories of


46 IRS ADVISORY COUNCIL, GEN. REP. 11 (2011) (explaining there are still perhaps millions of noncompliant taxpayers who refuse to voluntarily come into compliance and recommending adequate funding for enforcement and compliance efforts by the Internal Revenue Service); Craig M. Boise, Breaking Open Offshore Piggybanks: Deferral and the Utility of Amnesty, 14 GEO. MASON L. REV. 667, 701 (2007) (addressing the use of voluntary disclosure programs to promote compliance of offshore tax evaders). See generally Itai Grinberg, The Battle Over Taxing Offshore Accounts, 60 UCLA L. REV. 304 (2012) (detailing the current initiatives used to uncover and tax offshore accounts).

47 Swanson, supra note 7.


50 There are two offenses under I.R.C. § 7201: (a) the willful attempt to evade the assessment of tax and (b) the willful attempt to evade the payment of tax.

51 A refusal to comply with discovery requests generally results in the filing of one or more motions to compel. See FED. R. CIV. P. 37(a). For purposes of this Article, it is assumed
possible consequences for violating tax requirements. It also contends that noncompliant spouses in the divorce context should be ineligible for voluntary disclosure programs that allow taxpayers to avoid criminal prosecution and cap civil penalties.52 Strengthening the tax implications of failing to disclose assets in the divorce context would incentivize noncompliant spouses to comply with discovery from an early stage in the proceedings. This would lead to two benefits: (1) more expeditious family court proceedings and (2) more timely and accurate reporting of hidden offshore assets of the noncompliant spouse and other associated tax evaders.53

A. Hiding Offshore Assets from Spouses and the IRS

There is a predictable pattern in high-net-worth divorce proceedings that involves hiding assets from both a spouse and the IRS.54 In fact, it is not unusual for a spouse who is hiding money offshore in anticipation of a divorce also to hide their assets from the IRS.55 Typically, a wealthy spouse opens an account under the name of a shell company in a tax haven country, such as Panama, and transfers assets into the company to hide them from their spouse.56 During the divorce proceedings, the wealthy spouse can claim that investments are tied up that such noncompliant spouses have also refused to comply with the reporting requirements outlined herein.

52 The OVDP from prior years was replaced with the 2014 OVDP. There was no deadline for participating in the OVDP; however, the IRS retained the ability to revise or end the program at any point. See Closing the 2014 OVDP, supra note 41. Accordingly, the IRS announced the closing of the 2014 OVDP effective September 28, 2018, but the IRS indicated there may be future voluntary disclosure programs and began soliciting suggestions regarding such future programs. Id. (FAQ 1, 10, and 12). The IRS “streamlined” procedure is not discussed here since that program requires a certification that previous failures to comply were due to non-willful conduct. I.R.S. News Release IR-2014-73 (June 18, 2014), https://www.irs.gov/newsroom/irs-makes-changes-to-offshore-programs-revisions-ease-burden-and-help-more-taxpayers-come-into-compliance [https://perma.cc/8RJZ-NESF]. In addition, “quiet disclosure” is not discussed since it subjects participants to civil or criminal penalties. See Closing the 2014 OVDP, supra note 41 (describing quiet disclosures at FAQ 8).

53 Oei, supra note 6, at 689–90 (explaining that the United States has been able to gather information about additional offenders by using information collected by virtue of its offshore voluntary disclosure programs or through what is termed “cascading compliance”).

54 See Swanson, supra note 7.


56 Swanson, supra note 7. See generally Zarroli, supra note 55 (“The ease with which [shell companies] can be established is one reason more and more money is pouring into them each year.”).
in the sham corporation and then later lost. At the same time, the wealthy spouse does not report the offshore account to the IRS, as required under the FBAR and Foreign Account Tax Compliance Act of 2010 (FATCA) filing requirements and engages in tax evasion. For purposes of this Article, such spouses are included in the term “noncompliant” spouses.

57 Id.
60 I.R.S. News Release IR-2015-86 (June 10, 2015), https://www.irs.gov/newsroom/taxpayers-with-foreign-assets-may-have-fbar-and-fatca-filing-requirements-in-june [https://perma.cc/DBF8-VBRF] [hereinafter IRS, “Taxpayers with Foreign Assets” News Release]; Steven Toscher & Michel R. Stein, FBAR Enforcement Is Coming!, 5 J. TAX PRAC. & PROC. 27, 29 (2003); Joanna Heiberg, Note, FATCA: Toward a Multilateral Automatic Information Reporting Regime, 69 WASH. & LEE L. REV. 1685, 1698–99 (2012). For purposes of this Article, voluntary disclosure also encompasses the delinquent FBAR submission procedures and the delinquent international information return submission procedures, which will remain open after the 2014 OVDP temporarily closes on September 28, 2018. Closing the 2014 OVDP, supra note 41. Taxpayers who do not need “to file delinquent or amended tax returns to report and pay additional tax,” contrary to those using the OVDP or the Streamlined Filing Compliance Procedures, may use the submission procedures noted provided they meet certain requirements. Delinquent FBAR Submission Procedures, INTERNAL REVENUE SERV., https://www.irs.gov/individuals/international-taxpayers/delinquent-fbar-submission-procedures [https://perma.cc/8PCY-MZVJ] (last updated July 18, 2018) (explaining that taxpayers are eligible if they “have not filed a required . . . [FBAR], are not under a civil examination or criminal investigation by the IRS, and have not already been contacted by the IRS about the delinquent FBARs”); Delinquent International Information Return Submission Procedures, INTERNAL REVENUE SERV., https://www.irs.gov/individuals/international-taxpayers/delinquent-international-information-return-submission-procedures [https://perma.cc/DMH9-5YS3] (last updated June 18, 2018) (explaining that taxpayers are eligible if they “have not filed one or more required international information returns, have reasonable cause for not timely filing the information returns, are not under a civil examination or a criminal investigation by the IRS, and have not already been contacted by the IRS about the delinquent information returns”). Notably, the IRS criminal investigation voluntary disclosure program will remain open after September 28, 2018 as well. I.R.S. News Release IR-2018-52 (Mar. 13, 2018), https://www.irs.gov/newsroom/irs-to-end-offshore-voluntary-disclosure-program-taxpayers-with-undisclosed-foreign-assets-urged-to-come-forward-now [https://perma.cc/2W24-UJYM].
1. Family Law Discovery Process and Tracing Offshore Assets

Generally, family lawyers attempt to use the discovery process, where documents must be exchanged by court order, to gather financial and other information. A family lawyer often must resort to filing motions to compel. Even in responding to these motions to compel, a truly recalcitrant spouse will continue to fail to disclose assets and provide incomplete or inaccurate information. Ultimately, the family lawyer must subpoena financial documents of any known bank or other financial accounts.

After obtaining documents through a subpoena, or less likely cooperation from the noncompliant spouse, a family lawyer conducts a review to determine whether any assets have mysteriously disappeared. Generally, the other spouse must resort to hiring one or more forensic accountants that will trace assets and liabilities in order to uncover hidden offshore assets. Forensic accountants also rely on document review to conduct such tracing. In fact, it is not uncommon to learn there are 100 people in twenty countries delving into a secret world of offshore intricacies accessible only to the wealthiest

---

61 See 2 VALUATION AND DISTRIBUTION OF MARITAL PROPERTY § 29.04 (2005) (first quoting Ronnkvist v. Ronnkvist, 331 N.W.2d 764, 765–66 (Minn. 1983) (“[P]arties to a marital dissolution proceeding have a duty to make a full and accurate disclosure of all assets and liabilities to facilitate the trial court’s property distribution.”) and then quoting Rothman v. Rothman, 320 A.2d 496, 503–04 (N.J. 1974) (stating that the trial judge must insist upon “full cooperation of the litigants” in a divorce proceeding to effectuate equitable distribution of marital property) (explaining that almost every equitable distribution and community property state recognizes the need for financial discovery)).

62 See id. § 29.04[2] (noting that the initial step is document disclosure and that a single demand may not be adequate).

63 See RICE & RICE, supra note 48, at 306.


65 Id.


67 See generally Brigitte W. Muehlmann et al., The Use of Forensic Accounting Experts in Tax Cases as Identified in Court Opinions, 4 J. FORENSIC & INVESTIGATIVE ACCT., no. 2, 2012, at 1 (analyzing the use of forensic accounting experts in federal and state courts).

individuals. Their main objective is to unravel a web of company ownership that leads back to the wealthy instigator of it all, i.e., the beneficial owner. Their work is frustrated by noncompliant spouses who refuse to turn over documents or financial information. The requests for these documents are often ignored or completed only partially.

After the noncompliant spouse’s hidden assets are uncovered in the family law setting, the assets become subject to tax related penalties, which include criminal liability or civil penalties. Although the other spouse may qualify for innocent spouse relief in theory, there are substantial roadblocks under the current provisions, which are discussed in Part II.

2. Current Tax Consequences of Noncompliant Spouses

Once hidden assets are disclosed during divorce proceedings, the most important issue in the tax context becomes whether a noncompliant spouse “willfully” failed to report their foreign assets. This is because a willful failure could result in criminal prosecution or enormous civil penalties as discussed more fully in this section. Moreover, new reporting laws, such as FATCA, require foreign financial institutions (FFIs) around the globe to report bank accounts held by U.S. customers to the IRS. While these new reporting laws make it easier for the IRS, creditors, and spouses to find hidden foreign accounts, strengthening the consequences of failing to comply with these tax reporting laws and requirements in the context of divorce proceedings would result in more timely and accurate disclosure as well as locating additional offenders.

Currently, even after hidden foreign assets have come to light during divorce proceedings, there are too many ways for a noncompliant spouse to mitigate the tax consequences of their bad behavior. Most importantly, the IRS will rely on voluntary disclosure in determining whether to criminally

---

69 Swanson, supra note 7.
70 Id.
72 See infra notes 98–101 and accompanying text.
73 Skarlatos & Sardar, supra note 45, at 108; see infra Part II.
75 See infra notes 98–101 and accompanying text.
76 FATCA, enacted in 2010 as part of the HIRE Act requires U.S. persons to report specified foreign assets to the IRS on Form 8938 pursuant to I.R.C. § 6038D and FFIs to report U.S. customers to the IRS. See I.R.C. §§ 1471–1474.
77 See Oei, supra note 6, at 731–32.
prosecute.78 Voluntary disclosure takes place when in a manner that is truthful, timely, and complete, the taxpayer (a) evinces a willingness to cooperate followed by such cooperation with the IRS to determine accurate tax liability and (b) engages in a good faith effort to satisfy in full applicable tax, interest, and penalties.79 Often, as stated above, the noncompliant spouse never chooses to reveal these assets. They are only uncovered through a family lawyer’s use of motions to compel and subpoenas and through the hiring of forensic accountants.80 Once tax fraud is apparent in divorce proceedings, the judge may report the fraud to the IRS.81 In a 2004 New York case, for example, a judge reported a husband to the IRS after an admission that he had not paid taxes.82

However, a spouse who has remained noncompliant over the course of several years of divorce proceedings will only be subject to criminal prosecution or to civil penalties if willfulness is shown.83 Currently, the discovery process enables noncompliant spouses to claim their failure to report hidden foreign assets was not willful.84 This Article proposes that discovery documents should include statements of reporting requirements to prevent a noncompliant spouse from getting away with tax fraud with little or no ramifications. In addition, such noncompliant spouses are still eligible to participate in voluntary disclosure programs85 or delinquent FBAR procedures and delinquent international information return procedures.86 This Article contends that family lawyers should be able to report noncompliant spouses who meet certain thresholds to the IRS so that they will become ineligible for pre-clearance for voluntary disclosure.

78 See IRM 9.5.11.9(1) (Dec. 2, 2009).
79 See IRM 9.5.11.9(3). For the requirements applicable for the delinquent FBAR and international information return submission procedures, see supra note 60.
80 See supra notes 54–73 and accompanying text.
81 Abrams, supra note 59.
83 See Spies v. United States, 317 U.S. 492, 499–500 (1943) (holding that willfulness requires a specific intent or active desire to engage in tax evasion); see also United States v. Ragen, 314 U.S. 513, 513 (1942) (holding that tax evasion conviction requires proof that defendant acted willfully); Eliwrt v. United States, 231 F.2d 928, 932–33 (9th Cir. 1956) (stating taxpayer’s acting with specific intent to defraud must be shown).
84 See Skarlato & Sardar, supra note 45.
86 See supra note 60 (stating that voluntary disclosure is deemed to include delinquent FBAR and international information return submission procedures for purposes of this Article).
disclosure programs. The following section briefly outlines the reporting requirements for foreign assets that a noncompliant spouse would have failed to fulfill during the divorce proceedings and likely in prior years.

3. Offshore Reporting Requirements

Since the United States has a worldwide system of taxation for individuals, all U.S. citizens and residents are required to report worldwide income, regardless of whether such income is earned abroad. U.S. taxpayers may use a foreign tax credit or a foreign income exclusion to prevent double taxation largely. Moreover, U.S. taxpayers have a legal duty to report their ownership interest in foreign assets, e.g., foreign accounts and foreign entities, such as corporations, partnerships, and trusts. Finally, under a separate reporting obligation, U.S. taxpayers are required to file a FBAR with the Treasury Department for each foreign financial account that has a balance over $10,000 at any time during the taxable year. An unreported foreign account may result in the imposition of huge penalties that may far exceed the value of the unreported account. Foreign asset reporting obligations are complex and require reporting the same foreign asset in multiple ways at times. To summarize, all foreign income and the majority of foreign assets must be reported in the United States even if earned or kept abroad.

---

87 A taxpayer can become ineligible for the OVDP if the IRS receives information pertinent to their undisclosed OVDP assets while a hypothetical question (e.g., from his/her attorney) is pending. See Offshore Voluntary Disclosure Program Frequently Asked Questions and Answers 2012, supra note 85 (FAQ 22).
89 I.R.C. §§ 901, 911.
91 See 31 U.S.C. § 5314 (2012); 31 C.F.R. § 1010.350 (2012). The FBAR is filed on Form 114 with the Financial Crimes Enforcement Network (FinCEN), a division of the Treasury Department. IRS, “Taxpayers with Foreign Assets” News Release, supra note 60.
92 Skarlatos & Sardar, supra note 45, at 103.
93 Id. at 85.
94 Id. For a complete discussion of the tax return reporting requirements and related penalties, see id. at 85–93.
possible categories of consequence for failure to comply: (1) criminal conviction;\(^95\) (2) a 50% FBAR penalty;\(^96\) and (3) a 75% civil tax fraud penalty.\(^97\)

**B. Willful Violation Equals Three Possible Penalties**

Once an IRS agent, a prosecutor, or a court determines that a noncompliant spouse has acted willfully in failing to meet reporting requirements, the spouse is subject to criminal prosecution or enormous tax and FBAR penalties.\(^98\) In fact, willfulness is the standard for all three categories of penalties to which a noncompliant spouse may be subject: (1) criminal conviction;\(^99\) (2) a 50% FBAR penalty;\(^100\) and (3) a 75% civil tax fraud penalty.\(^101\) As a result, proving willfulness is the key to strengthening the implications of failure to comply with reporting requirements.\(^102\) Although the Department of Justice’s Offshore Compliance Initiative (OCI) has been advertised as a top litigation priority of the Tax Division, as of July 2016, it has only resulted in indictments of 117 taxpayers with offshore accounts and nineteen guilty verdicts overall according to one tax blog.\(^103\)

---

\(^95\) I.R.C. § 7201 (2012).

\(^96\) If a taxpayer can prove reasonable cause for failing to file an FBAR, e.g., the taxpayer told a tax preparer who neglected to file the FBAR about the foreign account(s), no penalty will be imposed. See IRM § 4.26.16.4.11 (Nov. 6, 2015). However, if the taxpayer cannot prove reasonable cause for failing to file an FBAR, a non-willful violation of the FBAR reporting requirement may result in a civil penalty up to $10,000 if it occurred after October 22, 2004. 31 U.S.C. § 5321(a)(5)(B) (2012); see also Matthew A. Melone, *Penalties for the Failure to Report Foreign Financial Accounts and the Excessive Fines Clause of the Eighth Amendment*, 22 GEO. MASON L. REV. 337, 346, 358 (2015).


\(^99\) Regarding criminal conviction, the government must show the taxpayer willfully failed to report a foreign asset. Skarlatos & Sardar, *supra* note 45, at 93; see also Spies v. United States, 317 U.S. 492, 497 (1942).

\(^100\) See 31 U.S.C. § 5321(a)(5)(B); IRM § 4.26.16.4.11.

\(^101\) Regarding the 75% penalty, the government must show the taxpayer willfully under-reported his/her income tax. See *supra* note 82; see also Skarlatos & Sardar, *supra* note 45, at 93.

\(^102\) See, e.g., Sansone v. United States, 380 U.S. 343, 353 (1965) (“Given petitioner’s material misstatement which resulted in a tax deficiency, if, as the jury obviously found, petitioner’s act was willful in the sense that he knew that he should have reported more income than he did for the year 1957, he was guilty of violating both §§ 7201 and 7207. If his action was not willful, he was guilty of violating neither.”).

The only difference in terms of the willfulness standard that applies to each penalty category is the level of proof required. For a criminal conviction, the level of proof is “beyond a reasonable doubt” whereas for the civil FBAR or civil fraud penalty cases, the level of proof is “clear and convincing.” If the government has large amounts of evidence that the taxpayer acted willfully in failing to report a foreign asset, it will have an easier time meeting the higher burden of showing willfulness “beyond a reasonable doubt.” However, if the government does not have much evidence of willfulness or the taxpayer is able to offer cogent excuses, then the government may only be able to meet the “clear and convincing” standard of proof and will not be able to seek a criminal charge.

C. Using Family Law Discovery Devices to Prove Willfulness

There are a number of factors that establish willfulness, and the devices used in the divorce discovery process should be modified to make proving willfulness easier. The definition of willfulness is “an intentional violation of a known legal duty.” A taxpayer who knows they should report a foreign asset, but intentionally refuses to do so, has acted willfully. The problem is that ignorance of the law may be used as a defense in this context. In other words, a taxpayer may claim that he or she did not know there was a legal requirement to disclose a foreign asset, and as a result, willfulness cannot be proven.

In light of the definition for willfulness, the discovery process should embody informing a noncompliant spouse of the legal duty to disclose foreign assets through complying with offshore reporting requirements. Once a noncompliant spouse has provable knowledge of offshore reporting requirements, if the other spouse still refuses to comply, willfulness would be easily established by the government. At that point, the noncompliant spouse

---

104 Steven Toscher & Lacey Strachan, Proving Willfulness in an FBAR Case, 14 J. TAX PRAC. & PROC. 29, 29 (2012).
105 See Skarlatos & Sardar, supra note 45, at 94.
106 See id.
107 The concept of “willful blindness” also applies to “willfulness.” However, this standard is more difficult to prove since it involves conjecture about a person’s thoughts when the tax return was filed. Id. at 94–95. Accordingly, this Article will focus upon imputing knowledge to the noncompliant spouse so that the government’s burden of proof required for establishing willfulness may be met more easily.
109 A willful failure to file requires a failure that is voluntary, purposeful, deliberate, and intentional, as distinct from merely accidental, inadvertent, or negligent. Sawyer v. United States, 607 F.2d 1190, 1192 (7th Cir. 1979), cert. denied, 445 U.S. 943 (1980).
111 See id.
112 See id. at 202.
would have intentionally violated a known legal duty, which is the very definition of willfulness.113

1. Imputing Knowledge Through Discovery Devices

There are several discovery devices that could be used to impute knowledge to a noncompliant spouse and thus help the government meet its burden of proof in showing a willful violation. As stated earlier, noncompliant spouses are able to claim a lack of knowledge of reporting requirements after having been served with numerous requests for financial documents during the divorce discovery process.114 As discussed earlier, family lawyers often must rely on subpoenas, motions to compel, and the work of forensic accountants to gain a full picture of assets, especially those that have been hidden offshore in anticipation of divorce.115 Only through the expenditure of much time and money are the hidden assets brought to light.116 The noncompliant spouse who has refused to disclose assets at every turn can escape both criminal liability and civil penalties, which require a showing of willfulness, simply by claiming they had no knowledge of reporting requirements.

This stark reality begs an important question: Why not include in discovery requests statements that will impute knowledge of reporting requirements to such noncompliant spouses? Following is a discussion of how certain discovery devices, namely (1) interrogatories, (2) requests for production of documents, and (3) depositions could be used in this manner and thus alleviate the government’s burden in proving willfulness in a criminal prosecution or in assessing civil penalties.117 The threat of successful criminal prosecution or the imposition of huge civil penalties should encourage noncompliant spouses to comply with discovery and reveal hidden assets to the tax authorities.118

First, interrogatories may be used to impute knowledge of the legal duty to report hidden foreign assets to the IRS. Interrogatories are written questions sent to a party (the “answering party”) that are responded to in writing under oath and then remitted to the sender.119 Interrogatories may require the answering party to provide “papers, documents or photographs” that are relevant in responding.120 Interrogatories should include a straightforward statement of the

113 See id. at 201.
114 See supra Part I.A.2.
115 See supra Part I.A.1.
116 Harmon-Vaught, supra note 64 (discussing methods for uncovering hidden assets that can “present a seemingly insurmountable wall” of difficulty for those trying to foil them).
117 See VALUATION AND DISTRIBUTION OF MARITAL PROPERTY, supra note 61, § 29.04[6] (listing, in addition to an initial document demand, other appraisal devices, including oral depositions and interrogatories).
118 See Abrams, supra note 55.
119 Hatch, supra note 68, § 36.
120 Id. § 34.
legal duty to report hidden foreign assets to the IRS by reference to specific forms and schedules. Once the answering party is served with the interrogatories, the party has knowledge of such legal duty. If the answering party is a noncompliant spouse, the government can easily meet its burden of proving willfulness and subsequently seek criminal prosecution. A warning to that effect could also be included with the interrogatories. This would incentivize potential noncompliant spouses to disclose hidden foreign assets both to the IRS and to their spouse.

Second, requests for production of documents may be used in a similar manner to provide inescapable knowledge of the legal duty to disclose hidden foreign assets. After a family law action commences, a party may request documents or other items in the possession, custody, or control of the other party or a person served with a notice or subpoena. This is referred to as a request for production of documents. Noncompliant spouses refuse to comply with these requests, which leads to unnecessary prolonging of the divorce proceedings. At the same time, noncompliant spouses also fail to disclose information ascertainable from the documents they are hiding to the IRS in violation of reporting requirements. The noncompliant spouse “willfully” abuses the discovery process and should also be deemed to “willfully” violate IRS reporting obligations. To achieve a more fair result, requests for production of documents, as with interrogatories, should include a statement of reporting requirements that references specific forms and schedules.

Third, depositions, which involve oral examination of a party, also serve as a keen opportunity to impute knowledge that in turn will make willfulness easier to prove. A deposition notice may also include the requirement of producing documents or other items at the oral examination. Documents turned over during the deposition may be marked as exhibits and used during the examination. However, typically, financial documents are requested before the taking of the deposition. The family lawyer taking the deposition of a noncompliant spouse (who has refused to provide documents) could begin the

122 Hatch, supra note 68, § 34.
123 Id.
125 See, e.g., CAL. CIV. PROC. CODE 2023.010(g), 2023.030(d) (West 2007); see also In re Marriage of Eustice, 195 Cal. Rptr. 3d 876, 889 (Cal. Ct. App. 2015) (noting that ex-husband engaged in “willful discovery abuse” by refusing to produce discovery documents for over two and a half years which resulted in the unavailability of material evidence).
126 See supra text accompanying notes 58–60.
127 Hatch, supra note 68, § 38.
128 Id.
129 Id.
130 See RICE & RICE, supra note 48, at 389.
deposition by reading a short uniform statement of reporting requirements.\(^{131}\) Since depositions are transcribed by a stenographer,\(^ {132}\) a deposition transcript could be given to the government to enable it to meet its burden of proof in a criminal prosecution once the compliant spouse is able to determine some of the hidden assets through other means, i.e., has impeached statements made during the deposition.\(^ {133}\)

### 2. Willfulness in the FBAR Context

An examination of how courts have recently analyzed willfulness in the FBAR context bolsters the argument presented. In *United States v. Williams*,\(^ {134}\) the Fourth Circuit reversed the lower court’s ruling and held that the taxpayer did in fact willfully fail to file FBARs, which resulted in the imposition of FBAR civil penalties.\(^ {135}\) In making its decision, the Circuit Court relied on three principles, the first of which is particularly relevant for these purposes: conduct designed to conceal income or additional financial information can establish willfulness.\(^ {136}\) Regarding this principle, the Court noted that the taxpayer stated on a tax return worksheet from his accountant that he did not have a foreign bank account.\(^ {137}\) The Court determined this was evidence of conduct designed to conceal income and used it to impose FBAR penalties against him.\(^ {138}\)

More than likely, obtaining a tax return worksheet from a noncompliant spouse would be a difficult task and probably require a subpoena of the tax accountant. Also, the Court had to rely heavily upon Williams’ guilty plea, i.e., admission that he failed to report foreign accounts to the IRS or the Treasury Department as part of an intricate tax scheme.\(^ {139}\) Requiring a guilty plea to establish willfulness restricts the ability of courts to impose civil FBAR penalties and is more than likely not a common occurrence.\(^ {140}\) A noncompliant spouse’s refusal to turn over information regarding foreign assets should already

\(^{131}\) Cf. id. at 303 (explaining that reading the perjury statute at the beginning of the deposition and the penalty for perjury is an effective technique for obtaining more truthful depositions).

\(^{132}\) See id. at 393.

\(^{133}\) See TAX CRIMES HANDBOOK, supra note 98, at 9.

\(^{134}\) United States v. Williams, 489 F. App’x 655 (4th Cir. 2012).

\(^{135}\) Id. at 659–60.

\(^{136}\) See id.


\(^{138}\) Williams, 489 F. App’x at 659–60.

\(^{139}\) Id.

be deemed evidence of conduct designed to conceal income. A more direct way of establishing a noncompliant spouse’s willfulness in the FBAR context would be to include statements of foreign asset/income reporting requirements on the discovery devices mentioned.

In cases involving a noncompliant spouse, the government should be able to point to the noncompliant spouse’s behavior during discovery to establish willfulness instead of having to rely on finding a tax worksheet given to an accountant and a guilty plea. A noncompliant spouse’s behavior by its nature is conduct designed to conceal income. That is why motions to compel and subpoenas must be used to obtain any documents; even in the face of motions to compel and subpoenas, noncompliant spouses persist on concealing their income, which should satisfy the standard set forth in Williams. However, to make the willfulness even clearer, the discovery devices should include statements of reporting requirements. Including such statements of reporting requirements would make it even easier for the government to prove that a noncompliant spouse has acted willfully in failing to report hidden foreign assets. The government need only point to the statements of reporting requirements contained in the interrogatories, requests for documents, etc. The noncompliant spouse’s decision to ignore written statements of reporting requirements contained in discovery requests would enable the government to show willfulness and thus impose civil FBAR penalties under Williams.

In another case that resulted in the imposition of FBAR penalties, United States v. McBride, the taxpayer was held to have willfully failed to file FBARs due to certain egregious actions, including describing his offshore structuring as tax evasion himself. Because McBride had signed his income tax returns, knowledge of the FBAR reporting requirement was imputed to him. However, his failure to comply with the legal duty to file the FBAR was deemed either “reckless or due to willful blindness.” The court then had to find that recklessness is adequate to show willfulness in terms of imposing a civil FBAR penalty. If a court is not willing to make the same determination regarding “willfulness,” a noncompliant spouse could escape civil FBAR penalties and escape any meaningful financial consequences despite his/her deliberate concealing of assets over the course of a multi-year divorce

141 See Spies v. United States, 317 U.S. 492, 499 (1942) (noting that conduct likely to conceal or mislead constitutes an affirmative act of evasion, and in contrast to a passive failure to file, may serve as the basis a tax evasion conviction); see also United States v. Williams, 489 F. App’x 655, 659 (4th Cir. 2012) (finding that false answers regarding tax documents are “meant to conceal or mislead sources of income” and constitute willful blindness to FBAR requirements).

142 See supra Part I.C.


144 Id. at 1206.

145 See id. at 1212–13, 1214.

146 See id. at 1212–13.

147 Id. at 1204–05.
proceeding. A better course of action is to include statements of reporting requirements in discovery devices and impute to the noncompliant spouse knowledge of such requirements. Although Williams and McBride deal with willfulness in the FBAR civil penalty context, there is no reason why willfulness could not be proven beyond a reasonable doubt, the standard required for criminal prosecution. The potential exposure to criminal liability should serve as a deterrent to a continued failure to cooperate with the discovery process and to continue to violate reporting requirements throughout divorce proceedings.  

D. Removing the Possibility of Voluntary Disclosure for Noncompliant Spouses

A taxpayer who has failed to disclose foreign assets may participate in what is known as a voluntary disclosure program in order to escape criminal liability and to prevent at least some civil penalties. There are four requirements for participation in the offshore voluntary disclosure program: (1) a “timely” disclosure; (2) undisclosed income or assets that were legally derived; (3) truthful cooperation with requests for information; and (4) payment or a good faith arrangement to pay taxes, penalties, and interest owing. The first two requirements are threshold requirements. This Article assumes that the offshore assets have been legally derived.

1. Current Pre-Clearance Procedure

“Timely” means that the noncompliant spouse is not already subject to an IRS investigation or audit. If the IRS has already started an investigation or audit, the noncompliant spouse is ineligible for the voluntary disclosure program. A “pre-clearance” procedure enables taxpayers to determine whether there is an IRS investigation or audit underway before disclosing the unreported assets. The taxpayer is required to send the IRS Criminal Investigation Division a letter identifying, inter alia, himself/herself and any financial institution that holds unreported assets. The IRS then runs a check

---

148 See, e.g., Gary S. Becker, Crime and Punishment: An Economic Approach, 76 J. Pol. Econ. 169, 176 (1968) (“Practically all the diverse theories agree . . . an increase in a person’s probability of conviction or punishment if convicted would generally decrease, perhaps substantially, perhaps negligibly, the number of offenses he commits.”).  
149 Skarlatos & Sardar, supra note 45, at 103–06.  
150 See Offshore Voluntary Disclosure Program Frequently Asked Questions and Answers 2012, supra note 85 (describing the program’s requirements at FAQ 7); Skarlatos & Sardar, supra note 45, at 103.  
151 Skarlatos & Sardar, supra note 45, at 103–04.  
152 IRM 9.5.11.9(4) (Dec. 2, 2009).  
153 See id.  
155 Id. (stating the required disclosures at FAQ 25).
against a list of taxpayers whom the IRS or the Department of Justice has previously identified and will then inform the taxpayer whether they are “pre-cleared” and therefore may make a disclosure.\(^{156}\) In most cases, a noncompliant spouse would need to request pre-clearance before making a disclosure.\(^{157}\)

2. Proposed Ineligibility for Pre-Clearance

Instead of allowing noncompliant spouses an opportunity to enter a voluntary disclosure program after evading the discovery process for prolonged periods of time,\(^{158}\) there should be a shortened window for these taxpayers. Once a motion to compel has been filed against a noncompliant spouse and has either remained pending for a given period, e.g., six months or longer or has been granted, and the other spouse can prove an offshore connection in the form of (1) at least one known foreign account (whether disclosed or not); (2) prior offshore business activity; or (3) frequent trips abroad, the noncompliant spouse’s name should be added to a separate list that makes them ineligible for the disclosure program if the noncompliant spouse does not make a disclosure within a prescribed time frame, e.g., ninety days. By giving the noncompliant spouse a deadline for starting the disclosure process that works in tandem with the discovery process timeline, the IRS can assist with the uncovering of hidden assets and promote compliance with reporting requirements, which ultimately will generate more revenue in the form of taxes, penalties, and interest from the noncompliant spouse and additional offenders.

Allowing a noncompliant spouse the opportunity to mitigate criminal liability and civil penalties easily through entering a voluntary disclosure program leads to an unjust result. The discovery process is unnecessarily prolonged, and accurate reporting is unnecessarily delayed by enabling noncompliant spouses to face only minor consequences for failing to comply. Such flagrant disregard of the family law discovery process and reporting requirements should not go unreprimanded. The solution is to add statements of reporting requirements to discovery devices to enable the government to prove willfulness and to allow family lawyers dealing with noncompliant spouses to have their names added to the list the IRS uses to determine ineligibility for voluntary disclosure pre-clearance. These two changes will serve as a powerful disincentive for continued noncompliance and will result in more expedient divorce proceedings and greater compliance with reporting requirements.

\(^{156}\) See id.; Skarlatos & Sardar, supra note 45, at 103.

\(^{157}\) See Offshore Voluntary Disclosure Program Frequently Asked Questions and Answers 2012, supra note 45 (discussing the preclearance procedure for both spouses at FAQ 24.1).

\(^{158}\) See Harmon-Vaught, supra note 64.
III. THE UNJUST DENIAL OF INNOCENT SPOUSE RELIEF FOR WIVES OF NONCOMPLIANT SPOUSES

The next step that must be confronted is what happens to the compliant spouse who has uncovered the hidden assets during the divorce process. Since joint and several liability attaches with the filing of joint tax returns, such spouse, typically the wife, will also face the possibility of civil and criminal liability unless she obtains innocent spouse relief under section 6015. The mismatch of requiring willfulness to criminally convict the noncompliant spouse while allowing mere “knowledge” of the receipt of income (not even the source) to eviscerate the ability of his wife to obtain federal innocent spouse relief leads to a perverse result. Our current law disincentivizes wives of noncompliant spouses from disclosing the offshore assets and accounts unearthed in dissolution proceedings through forensic accountants and investigative accounting.

Granted, there are two additional avenues that a wife in this circumstance could use, but neither is as complete and thus neither would incentivize whistleblowing. First, the wife could avail herself of other statutory relief provisions. However, these forms of relief generally involve an assessment of liability against the wife and a later acknowledgment of her inability to pay in full at the time. A wife would be unlikely to run the risk that the IRS would assess total tax liability to her and thus dissuaded from whistleblowing. Second, a wife who is unable to receive federal mitigation could request that the other spouse contribute toward the tax liability and seek relief under state law. Nevertheless, this is not a viable solution if the noncompliant husband is judgment proof, and a ruling on the state level could require her to pay.

Part II argues that the United States must provide wives of noncompliant spouses with at least federal innocent spouse relief to encourage them to whistle blow about offshore tax evasion uncovered during dissolution proceedings. It also concludes that this is in most cases an equitable result because such wives typically would not have participated in or known about the wrongdoing of their spouses.

159 See infra Part II.B.1.
163 See id. at 151 n.53 (“Wives sought relief in 85.4% of cases brought . . . and won 37.4% of their trials and 21.6% of subsequent appeals.”).
164 See infra Part II.B.3 (discussing state law implications).
165 See McMahon, supra note at 162, at 157.
spouses. Had they known of the unreported income, they would not have needed to hire forensic accountants to engage in investigative accounting.

First, it explains the problem of civil and criminal liability that attaches with the filing of a joint tax return. Second, it provides a summary of innocent spouse relief, with a particular focus on relief under section 6015(c), which is available for spouses no longer married, and under section 6015(f), the equitable relief provision. Third, it then addresses the current challenges facing wives of noncompliant spouses in obtaining such relief and examines relevant omitted income cases. Fourth, it argues that the legislative history of innocent spouse relief supports extending innocent spouse relief to wives of noncompliant spouses. Fifth, a reform of innocent spouse relief is proposed based upon new understandings of financial and other forms of domestic abuse relevant in this context. Finally, it addresses remaining issues associated with expanding relief.

A. Joint Civil and Criminal Liability

Couples often decide how to delegate the preparation of tax returns or what has been termed the duty to disclose.166 As a result, even if a spouse deliberately conceals a failure to report income on a tax return, the other spouse may become liable for the resulting tax liability in full, including any penalties and interest, which could eclipse in size the original tax liability.167

Even more distressingly, the other spouse, who was really a mere signatory, may be held criminally liable for tax and nontax offenses if a court finds the individual was “willfully blind” to omissions of income and fraudulent representations.168 Pursuant to innocent spouse relief under I.R.C. § 6015, each spouse’s tax liability is allocated as though fictional separately filed individual returns had been filed.169 However, the IRS may deny this relief if the spouse had actual knowledge of unreported income.170

The threats of civil liability and criminal indictment for a wife of a noncompliant spouse are very real ones.171 In the case of civil liability, this threat never disappears due to an exception to the usual three-year statute of limitations period.172 However, there is no statute of limitations for assessing taxes in the case of false or fraudulent returns relating to tax evasion. That means

---
167 See id. at 107–09.
169 Id. § 6015(d)(3)(A).
170 See Cheshire v. Commissioner, 282 F.3d 326, 336 (5th Cir. 2002) (stating in the case of deductions, actual knowledge of the facts that caused the deduction not to be available bars relief).
171 Gold-Kessler, supra note 166, at 103 (observing “a spouse must tread very carefully” to avoid criminal liability).
172 See I.R.C. § 6501(c)(1). Typically, the IRS only has three years from the date a return was filed to assess additional taxes. Id.
a wife could be hit with an enormous tax liability at any time after the divorce, which leads to great uncertainty for her, particularly as the typical primary caregiver.

In the case of criminal indictment, such wives are subject to possible liability for six years after the filing of the false and/or fraudulent returns.\textsuperscript{173} Each year that taxes were not paid constitutes a separate offense.\textsuperscript{174} Moreover, a court may use the repeated omission of income to infer knowing, willful falsification of returns.\textsuperscript{175} A taxpayer’s good faith reliance upon the advice of a qualified accountant may serve as a defense but only if the accountant was informed of all relevant facts.\textsuperscript{176} Accordingly, the passage of time may result in freedom from criminal prosecution; however, in the civil context it will lead to the compounding of interest on unpaid tax liability.\textsuperscript{177}

This is a reason for the noncompliant husband to use the offshore voluntary disclosure program. At least under regular voluntary disclosure, the reporting of previously unreported income and the satisfaction of any resulting tax liability will limit exposure to only civil penalties.\textsuperscript{178} Although voluntary disclosure cannot guarantee a taxpayer will not face criminal prosecution,\textsuperscript{179} it may help to avoid criminal sanctions provided certain conditions are satisfied.\textsuperscript{180}

B. Innocent Spouse Relief and Its Inadequacies

Simply stated, innocent spouse relief serves as an exception to the general rule that a husband and wife filing a joint return are jointly and severally liable for the taxes owed on such return.\textsuperscript{181} Once a compliant spouse finds hidden offshore assets, he or she will be confronted with the need for innocent spouse relief to escape the joint and several liability that attaches to all jointly filed tax returns.\textsuperscript{182} There are three types of innocent spouse relief under I.R.C. § 6015: (1) an election under section 6015(b) for taxpayers still married; (2) an election under section 6015(c) for taxpayers separated or divorced whereby the innocent

\textsuperscript{173} I.R.C. § 6531 (2012). In terms of criminal liability, the government has six years from the date of the offense to issue a criminal indictment for tax evasion, failure to pay taxes, or filing a false return. \textit{Id.}

\textsuperscript{174} United States v. Smith, 335 F.2d 898, 901 (7th Cir. 1964).

\textsuperscript{175} United States v. Allen, 551 F.2d 208, 210 (8th Cir. 1977).

\textsuperscript{176} United States v. Whyte, 699 F.2d 375, 379–80 (7th Cir. 1983).

\textsuperscript{177} I.R.C. § 6622(a) (2006).

\textsuperscript{178} See Gold-Kessler, \textit{supra} note 166, at 108–09 (concluding that taxpayers who voluntarily disclose unreported income before an investigation begins or information is received regarding their noncompliance may escape criminal liability).

\textsuperscript{179} United States v. Hebel, 668 F.2d 995, 998–99 (8th Cir. 1982).

\textsuperscript{180} See IRM 9.5.11.9 (Dec. 2, 2012) (explaining that the disclosure must be “truthful, timely, complete” and made before the IRS starts an investigation, notifies the taxpayer of an intention to do so, or has received information relating to failure to comply).


\textsuperscript{182} See generally I.R.C. § 6015 (containing the provision for “relief from joint and several liability on joint return”).
spouse will have her liability limited to only those items allocable to her; or (3) equitable relief under section 6015(f) for those innocent spouses who can prove full liability would be unfair due to factors such as economic hardship and abuse. In section 6015(b) cases, the taxpayer has the burden of proving that he or she did not know there was “an understatement of tax attributable to [one or more] erroneous items [of the other spouse].” In section 6015(c) (taxpayers no longer married) cases, the Service has the burden of proof.

This Article primarily addresses an election made under section 6015(c) or section 6015(f). In terms of both elections, a consideration of “significant benefit”—defined as any benefit beyond normal support due to the failure to report or pay tax—is a factor and is discussed infra in Part II.C. The main problem with section 6015(c) is that a compliant spouse is ineligible for relief if the IRS demonstrates “actual knowledge” of a tax understatement at the time of the signing of the tax return. However, even though section 6015(c) refers to knowledge of a tax understatement, courts have held that knowledge of the underlying facts giving rise to a deduction or omission of income is enough for ineligibility. The primary problem with section 6015(f) is that the balancing test associated with it fails to correctly conceive of financial abuse and other forms of domestic abuse likely present in the discussed context.


In order to obtain innocent spouse relief under section 6015(b) or section 6015(c), the taxpayer must petition the IRS no later than two years after collection activities have started. In the event he or she does not, or otherwise cannot obtain relief under these two provisions, the spouse may obtain relief under section 6015(f): an equitable relief provision. In determining section 6015(f) equitable relief, one of the factors considered is whether the spouse substantially benefited from the failure to pay taxes owed. This inquiry involves examining whether the spouse could make otherwise unaffordable expenditures by having larger amounts of disposable income. Additionally, a court may decide to grant section 6015(f) equitable relief if after the payment of the tax liability, the spouse would not have income left to cover

---

183 See id. §§ 6015(b), (c), (f).
184 See id. § 6015(b)(1)(B).
185 Id. § 6015(c)(2).
186 See infra Part II.C.
188 See McMahon, supra note 162, at 149.
190 Id. § 6015(f).
There are a number of factors examined to make this determination, including geographic area, the wife’s age, employment status and history, and number of dependents.

Section 6015(f) equitable relief is also relevant when knowledge—either reason to know, as identified in section 6015(b) relief, or actual knowledge, as identified in section 6015(c) relief—are at play. Relevantly, a spouse who has knowledge may still be granted relief under section 6015(f) provided she (1) did not exercise control over her husband’s business income and (2) did not have direct access to business receipts. This would seem the case in the omission of income instances addressed in this section because if the wife had control over income or access to business receipts, she would not have to hire forensic accountants or expend funds for investigative accounting. The importance of this distinction is discussed later in this section.

Nevertheless, because the IRS and Tax Court judges, like society and the family law system, misperceive financial abuse and other forms of domestic abuse, wives are routinely denied innocent spouse relief. Generally, innocent wives of high-net worth tax evaders would be deemed to have knowledge that income was received and thus ineligible for relief under section 6015(c), even though they did not know about offshore assets and accounts until they hired a forensic accountant in the divorce proceedings. Alternatively, their allegations of domestic abuse are not believed, and they are deemed ineligible for relief under section 6015(f). This section argues that wives of noncompliant spouses fit the criteria set forth in section 6015(f) once misperceptions about financial and other forms of domestic abuse are corrected, and they should be granted innocent spouse relief.

2. Legislative History of Innocent Spouse Relief and Wives

An examination of the legislative history of innocent spouse relief shows that the provision was enacted to help wives specifically; they were seen as being unfairly burdened by the joint and several liability that attaches with the

---

193 See, e.g., Wiener v. Comm’r, 96 T.C.M. (CCH) 227, 236, 238 (2008) (granting equitable relief to petitioner who had reason to know of items giving rise to tax deficiencies and/or failed to satisfy her duty of inquiry regarding these items, but who would suffer economic hardship if relief were not granted).

194 Treas. Reg. § 301.6343-1(b)(4) (2002); see also I.R.S. Notice 2012-8, 2012-4 I.R.B. 311 (proposing “to provide minimum standards based on income, expenses, and assets, for determining whether the requesting spouse would suffer economic hardship if relief is not granted”).


196 See id.

197 See infra Part II.D.

filing of a joint return. An unnerving problem is that Congress failed to define “unfair burden” in this context. At the same time, there are other provisions in the Internal Revenue Code that may provide relief to wives who are unable to pay taxes owed, and the discussion here must acknowledge these other avenues as well.

Up until the end of the 1960’s, joint and several liability was applied without much objection from joint filers. In the early years of joint filing, the only way wives could escape liability for taxes owed in connection with joint returns was to prove that they signed a return under duress. Moreover, relief under the now repealed I.R.C. § 6013(e) required a substantial understatement of tax. In 1971, after several wives were held liable for taxes owed due to their husband’s embezzlement, complaints arose regarding the inadequacy of the duress defense, and Congress’s answer was innocent spouse relief. As initially enacted, innocent spouse relief was not intended to apply to all joint filers but rather was to relieve wives from extreme financial hardship posed because of joint and several liability. Innocent spouse relief continued to operate as a constricted form of relief until 1984 when modest expansion occurred.

However, it was not until 1998 that innocent spouse relief was liberalized to its present form since prior to this time relief was only available in a highly restricted form. In 1998, Congress enacted the IRS Restructuring and Reform Act of 1998 (RRA), which provided several exceptions to the usual rule of joint and several liability. One of the purposes of the RRA was to provide relief to

199 See McMahon, supra note 162, at 147.
200 Id.
wives who unknowingly became liable for tax deficiencies caused by their husbands.\textsuperscript{210} As stated in the 1998 Congressional Conference Report, prior to the passage of the RRA, 90\% of innocent spouse relief cases were brought by wives.\textsuperscript{211} Moreover, Professor Stephanie McMahon’s 2012 empirical study confirms that women make up an overwhelming number of innocent spouse relief requests.\textsuperscript{212} Specifically, 338 women compared to 59 men brought cases before the Tax Court, i.e., 85\% of the cases were from women.\textsuperscript{213} In fact, McMahon emphasizes that Congress termed innocent spouse relief a women’s issue.\textsuperscript{214} Jacqueline Clarke’s 2014 study builds upon the McMahon Empirical Study and evinces that the number is even more skewed in terms of the number of requesting taxpayers who alleged abuse.\textsuperscript{215} She found that 91.67\% of taxpayers requesting innocent spouse relief while alleging abuse were women.\textsuperscript{216} Notably, women have won 89.50\% of innocent spouse relief victories in general and 93\% of those where abuse was alleged.\textsuperscript{217} One must conclude, as Clarke does, that innocent spouse relief and allegations of abuse are gendered in terms of the tax world.\textsuperscript{218}

Nevertheless, it is clear that family law courts and tax courts still misconceive domestic violence and the danger it poses.\textsuperscript{219} Typically, women who raise domestic violence concerns are mischaracterized as doing so to gain

\textsuperscript{210} See McMahon, supra note 162, at 147; see also 144 CONG. REC. 14,688–689 (1998); H.R. REP. NO. 105-599, at 252–53 (1998) (Conf. Rep.) (stating that women commonly are liable for their ex-husband’s tax liabilities resulting from their filing of illegal tax returns).

\textsuperscript{211} 144 CONG. REC. 14737 (1998); see also Stephen Zorn, Innocent Spouses, Reasonable Women and Divorce: The Gap Between Reality and the Internal Revenue Code, 3 MICH. J. GENDER & L. 421, 425 n.13 (1996).


\textsuperscript{213} Id.

\textsuperscript{214} Id. at 631.

\textsuperscript{215} Clarke Study, supra note 198, at 836. Both studies are described in detail and are discussed infra Part II.C.

\textsuperscript{216} Id.

\textsuperscript{217} Id.

\textsuperscript{218} Id. The Clarke Study points out the inconsistent gendered nature of domestic violence in other contexts. See id. For example, a study conducted by the National Coalition Against Domestic Violence found 85\% of domestic violence victims are women. Id. at 836, n.74 (citing CALLIE MARIE RENNISON, U.S. DEP’T OF JUSTICE, BUREAU OF JUSTICE STATISTICS: CRIME DATA BRIEF, INTIMATE PARTNER VIOLENCE, 1993-2001 (2003), https://www.bjs.gov/content/pub/pdf/ipv01.pdf [https://perma.cc/Z3WJ-R4DL]). However, a 2010 national survey by the U.S. Department of Justice and the Centers for Disease Control and Prevention contradicts this result. NAT’L CTR. FOR INJURY PREVENTION & CONTROL, DIV. OF VIOLENCE PREVENTION, THE NATIONAL INTIMATE PARTNER AND SEXUAL VIOLENCE SURVEY (Nov. 2011), 18–20 https://www.cdc.gov/violenceprevention/pdf/nisvs_report2010-a.pdf [https://perma.cc/M3Y7-8UMA].

\textsuperscript{219} Clarke Study, supra note 198, at 828–29.
a tactical advantage.220 In order to properly analyze the granting of innocent spouse relief to women, one must understand the other biases that operate in our justice system.221 Additionally, Clarke confronts the distressing problem that some men may feign abuse and claim innocent spouse relief when, in fact, they are the abuser in the relationship.222

It is estimated that since the RRA was passed, the IRS has received more than 1,000 applications for innocent spouse relief every week.223 As part of sweeping changes resulting from Congress’ direction to the IRS to view taxpayers more akin to customers, the innocent spouse relief provisions became more flexible and thereby opened up to a larger number.224 Instead of focusing on financial hardship, the provisions focused on whether innocent spouse relief granted “meaningful relief in all cases where such relief is appropriate.”225 Nevertheless, Congress’ failure to define when such relief is “appropriate” has led to a number of problems, which are relevant for the aforementioned discussion. For example, is it “appropriate” to provide relief to spouses who were not coerced into false tax reporting?226 Is it “appropriate” to afford relief to spouses who are already suffering financial hardship?227 When one examines the committee reports and statements made during the congressional debates, a common thread is that an innocent spouse is one who lacked knowledge of his or her spouse’s wrongdoing in filing a fraudulent return.228

220 Peter G. Jaffe et al., Child Custody and Domestic Violence: A Call for Safety and Accountability 17 (2003) (stating that judges tend not to believe women who raise concerns about domestic violence because they are perceived as doing so to strengthen their contentions for custody).

221 Clarke Study, supra note 198, at 836.

222 See id. at 837 (recognizing at the same time that some men are actually subject to abuse and are less likely to have evidence of it given their hesitancy to report abuse by their wives).


226 See McMahon, supra note 162, at 148 (interpreting “truly innocent” spouses only as those who are “coerced into filing the return”).

227 See id.

228 See, e.g., S. REP. NO. 105-174, at 56–58 (1997) (discussing that it is inequitable to hold a spouse liable if they did not know or had no reason to know); H.R. REP. NO. 105-599, at 252–55 (1998) (discussing that the conferees intended an innocent spouse to have no knowledge); 144 Cong. Rec. 8509 (1998) (statement of Sen. Barbara Boxer) (“An ‘innocent spouse’ is one—usually a wife—who signs a joint tax return not knowing that the information contained therein . . . ”); 144 Cong. Rec. 8517–8518 (1998) (statement of Sen. Dianne Feinstein) (“The bill would expand the protections provided to ‘innocent spouses’ who find themselves liable for taxes, interest, or penalties because of a spouse’s action taken without their knowledge.”); 144 Cong. Rec. 14689 (1998) (statement of Sen. William Roth) (discussing relief will not be available if a spouse did not have any knowledge); 144 Cong.
It is patently clear that Congress’ expanded relief was meant primarily for wives.\(^2\) The unrelenting pursuit of wives in terms of abusive collection was deemed unacceptable.\(^3\) Moreover, Congress intended to provide relief to divorced or separated wives who were left with debilitating tax liabilities due to calculating and deceiving husbands.\(^4\) Some scholars have posited that Congress left the definition of “appropriate” ambiguous due to the costs associated with drafting a more specific rule.\(^5\) Nevertheless, the IRS and the courts have been left to use, in most cases, a facts and circumstances test to determine whether relief is warranted.\(^6\) While the two other forms of relief explicitly call for an examination of equity, the section 6015(c) form does not expressly.\(^7\) As explained earlier, section 6015(c) relief is intended to assist the spouses that are divorced or separated.\(^8\) These wives are able to obtain relief

\(^2\) All Congressional Record references regarding innocent spouse relief were to wives, usually divorced wives. See, e.g., 144 CONG. REC. 2045 (1998) (statement of Sen. Bob Graham) (discussing how a wife may have little income and sign a return she knows little about); 144 CONG. REC. 2043 (1998) (statement of Sen. Al D’Amato) (discussing how this will mostly help women and that many divorced/separated women came forward at the hearing); 144 CONG. REC. 8510 (1998) (statement of Sen. Spencer Abraham) (discussing the story of a divorced immigrant who faced joint and several liability); 144 CONG. REC. 7694 (1998) (statement of Sen. Mike DeWine) (discussing testimony, including from a divorced woman from Toledo); 144 CONG. REC. 13968 (1998) (statement of Rep. William Archer) (discussing how the act gives new protections, including spousal relief to women). Husbands as victims were infrequently mentioned; see also 144 CONG. REC. 8521 (1998) (statement of Sen. Olympia Snowe) (examining the potential benefits from spousal relief and only giving examples with women in them).


\(^6\) McMahon, supra note 162, at 150 (“A third subsection provides relief that is meant to function as a clear allocation of liability for divorced, widowed, or separated spouses unless the spouse is proven to have actual knowledge of the tax evasion. However, this third test is not applied mechanically. Not only do courts consider equitable factors before applying this last form of relief, in 15.4% of reported cases in which a spouse won under this third test the requesting spouse was found to have actual knowledge of the tax evasion contrary to the test’s statutory requirement.”). Widowed spouses are also included. Id.
provided they did not have “actual knowledge,” which is a problematic requirement as this Article explains.\textsuperscript{237}

3. Lingering State Liability

Even if a wife secures federal innocent spouse relief, a state hurdle of liability may also be present. Both marriage and dissolution are governed by state law.\textsuperscript{238} State courts tasked with dividing marital assets have mainly affirmed their right to do so—separate and without influence from any IRS or federal tax court proceedings.\textsuperscript{239}

For example, in the 1984 \textit{In re Marriage of Dunseth}, the Appellate Court of Illinois scolded a trial court for trying to protect a wife in a dissolution proceeding from liability owed to creditors, including the IRS.\textsuperscript{240} The appellate court maintained that the creditors were not parties to the proceeding, and therefore, the trial court’s order that the husband pay debts owed to them was not binding upon the creditors.\textsuperscript{241} Importantly, the \textit{Dunseth} court was skeptical of the innocent spouse relief the wife had obtained because she enjoyed a lavish lifestyle during the marriage due to her husband’s failure pay taxes, inter alia.\textsuperscript{242}

Several months later, the Ninth Circuit held that an innocent spouse determination is not controlling in terms of contribution rights under state law under either the Supremacy Clause or the doctrine of res judicata.\textsuperscript{243} Contribution rights could stem from either a divorce decree or a general contribution statute.\textsuperscript{244} In this case, a former husband sought to challenge the Tax Court’s acceptance of his ex-wife’s and the IRS’s stipulation that the ex-wife was an innocent spouse “on the ground that she relied on her husband and their accountant to assure that the returns were properly prepared, and she did not benefit from the understatement of tax because the unpaid tax money was spent on his new wife or previous affairs.”\textsuperscript{245}

In other words, state decisions confirm a wife may receive innocent spouse relief from the IRS but still remain liable for an allocation of tax liability under state law.\textsuperscript{246} The California Court of Appeals case \textit{In re Marriage of Hargrave}

\begin{itemize}
\item \textsuperscript{237} I.R.C. § 6015(c)(3)(C).
\item \textsuperscript{238} See Gold-Kessler, supra note 166, at 109.
\item \textsuperscript{239} Id.
\item \textsuperscript{240} \textit{In re Marriage of Dunseth}, 633 N.E.2d 82, 94–95 (Ill. App. Ct. 1994).
\item \textsuperscript{241} Id. at 94 (noting that even if the wife convinced the IRS she was an innocent party she would also have to make the same showing in a proceeding where the IRS was a party).
\item \textsuperscript{242} Id. at 95.
\item \textsuperscript{243} Estate of Ravetti v. United States, 37 F.3d 1393, 1395 (9th Cir. 1994).
\item \textsuperscript{244} Id.
\item \textsuperscript{245} Id. at 1394 (internal quotations omitted).
\item \textsuperscript{246} Id. at 1395-96. In addition, consent judgements and marital settlement agreements have been deemed controlling even in the face of subsequent federal innocent spouse relief. \textit{See, e.g.,} PM v. MW, Nos. 1095-83, 06-28642, 2007 WL 1518621, at *2 (Del. Fam. Ct. Feb. 23, 2007) (“[B]oth parties will share the penalties to the IRS as was the terms of their agreement.”); Kozak v. Kozak, No. 198799, 1998 WL 1990458, at *3 (Mich. Ct. App. Aug.
\end{itemize}
admonishes spouses that it is not a foregone conclusion that they will escape tax liability through a grant of innocent spouse relief where a state court previously has apportioned liability in a dissolution proceeding.\textsuperscript{247} The Kentucky Court of Appeals has taken a similar approach, reasoning that IRS innocent spouse relief is an “administrative process” and not an adjudication that directs the party from whom the IRS will pursue payment.\textsuperscript{248} It further noted that a Federal Tax Court decision is not controlling in terms of state division of marital debt that encompasses tax liability.\textsuperscript{249}

The Court of Appeals of Washington has taken a slightly softer stance.\textsuperscript{250} It has acknowledged that the deliberate and unnecessary shoring up of tax liability by one spouse may be considered in apportioning marital debts in a dissolution proceeding.\textsuperscript{251} At the same time, the Court prohibited a trial court from basing its order on a federal innocent spouse relief finding.\textsuperscript{252} Some appellate courts have concluded that federal tax liability must be litigated solely in federal courts relying on precedent from other jurisdictions.\textsuperscript{253} Similarly, the Court of Appeals of Wisconsin recognized in \textit{In re Marriage of Jahimiak} that although the trial court may not make a determination as to federal innocent spouse relief, it could properly allocate marital debt to the spouse who was in charge of family finances and prepared the tax returns as well as was the only beneficiary of the false returns.\textsuperscript{254}

The Court of Appeals of Arkansas has taken a slightly more nuanced approach, and Nebraska has largely agreed with it. In \textit{Killough v. Killough}, the appellate court upheld a trial court’s divorce decree allocating to the husband responsibility for paying penalties and interest resulting from his failure to report income and allocating to the wife one half of the tax liability that she

\textsuperscript{4} 1998 (holding that it is unreasonable to change the tax liabilities when they specifically intended to share them); Bryant v. Flint, 894 S.W.2d 397, 400 (Tex. App. 1994) (“Although the IRS ‘innocent spouse’ exemption may have extinguished her liability to the IRS, it did not diminish her liability to the estate under the settlement agreement.”).

\textsuperscript{247} \textit{In re Marriage of Hargrave}, 43 Cal. Rptr. 2d 474, 478 (Cal. App. 1995).


\textsuperscript{249} \textit{Id.}


\textsuperscript{251} \textit{Id.}

\textsuperscript{252} \textit{Id.} at 61. \textit{But cf. In re Marriage of Behar}, No. D045377, 2005 WL 2386325, at *7 (Cal. App. Ct. Oct. 21, 2005) (concluding that where it was unlikely that the husband would receive innocent spouse relief, it was appropriate to assign tax liabilities stemming from the wife’s separate property as marital debt).

\textsuperscript{253} \textit{See Lakewood Plantation, Inc. v. United States}, 272 F. Supp. 290, 294 (D.S.C. 1967); \textit{see also Craig v. United States}, 69 F. Supp. 229, 239 (W.D. Pa. 1946) (“[I]n order to achieve absolute uniformity in all of the states of the Union in connection with tax liability created by Revenue Acts enacted by Congress . . . the state courts’ decisions of questions, over which they have final say, cannot and should not decide issues of federal tax law and thus hamper the effective enforcement of a valid federal tax.”).

would have been responsible for if the income had been reported.\footnote{255} The Supreme Court of Nebraska has taken a similar approach, characterizing penalties and interest as nonmarital debt and allocating liability for them to the spouse responsible for the incurrence.\footnote{256} Likewise, funds owed to the IRS spent by one spouse on nonmarital pursuits have been deemed nonmarital debt.\footnote{257}

On the one hand, the trial court setting serves as another bite at the apple beyond federal innocent spouse relief to shield a spouse from at least civil liability provided a convincing case exists that equity dictates such a result.\footnote{258} On the other hand, there is no guarantee that the trial court will uphold a grant of federal innocent spouse relief.\footnote{259} However, it is still important for a wife of a noncompliant spouse to receive at least federal innocent spouse relief and hopefully reforms in that area will lead to eventual state reform as well.

C. Problems with the Current Approach

An examination of innocent spouse relief reveals that it is quite difficult to obtain.\footnote{260} One of the reasons for the difficulty in securing relief under section 6015(c) is the mismatch in terms of intent. As explained earlier, a noncompliant spouse must intentionally violate a known legal duty to face criminal prosecution or penalties.\footnote{261} In contrast, a compliant spouse is disqualified from receiving innocent spouse relief by simply knowing that income was received.\footnote{262} In other words, a compliant spouse who does not know about the legal duty to report or pay tax on foreign income typically will be ineligible for innocent spouse relief under current law: “actual knowledge” of any item giving rise to a tax deficiency (i.e., knowledge that income was received) is enough to disqualify such a spouse even if the individual had no knowledge of the source of such income.\footnote{263} Until this inequity is corrected, we are disincentivizing compliant spouses from working with the government and punishing them for the sins of the noncompliant spouse, even if they knew nothing about them.

Another contributing factor is the pervasive misperception about financial and other forms of domestic abuse. In theory, there are two ways out of the “actual knowledge” trap. First, an “innocent” spouse may receive relief despite actual knowledge if the individual was (1) “the victim of [domestic] abuse” before the return was signed and (2) as a result, failed to challenge the treatment

\footnote{256}{Carter v. Carter, 626 N.W.2d 576, 581 (Neb. 2001).}
\footnote{257}{Id.}
\footnote{258}{See id.}
\footnote{259}{See id. (holding under the facts of that case the court granted equity).}
\footnote{260}{See McMahon, Empirical Study, supra note 212, at 646; see also Clarke Study, supra note 198, at 827.}
\footnote{261}{See supra Part I.C.}
\footnote{262}{I.R.C. § 6015(c)(3)(C)(2006).}
\footnote{263}{Treas. Reg. § 1.6015-3(c)(2) (2002).}
of any item out of fear of retaliation.264 Second, an innocent spouse who signed the return under duress remains eligible.265 Nevertheless, the stark reality is that innocent spouse relief is denied even where domestic abuse, including financial abuse, is shown.266

As Clarke has stated, the IRS and the Tax Court do not understand the “interplay between domestic violence and innocent spouse cases.”267 Moreover, National Taxpayer Advocate Nina Olson has reprimanded the IRS for “display[ing] an astonishing ignorance about what happens to people in abusive relationships” in the context of innocent spouse relief cases.268 In the 2008 case, Nihiser v. Commissioner, Judge Holmes voiced a similar concern and noted the lack of regulations and “ordinary cannons of construction” in this context.269 Finally, scholars have also commented upon the dearth of empirical research regarding innocent spouse relief and the even greater void in terms of conclusions about how Tax Court judges rule on domestic abuse claims.270

Two leading studies are discussed in the following analysis of problems with current innocent spouse relief under section 6015(c) and section 6015(f). McMahon performed an empirical analysis of 444 innocent spouse relief claims from 1998 through 2011, noting how the Tax Court examined the factors from Revenue Ruling 2003-61 (“the McMahon Empirical Study”).271 Clarke focused more on the issue of abuse and thus specifically dealt with the fifty-six cases where the “innocent spouse” alleged abuse (“the Clarke Study”).272 Her goal was to determine what had happened when the abuse claim was sustained versus denied as a means of ultimately determining what factors courts deem dispositive in this context.273 The Clarke Study,274 like the McMahon Empirical Study, focuses on Tax Court cases since the majority of innocent spouse relief appeals are heard there.275

265 I.R.C. § 6015(c)(3)(C).
266 See Clarke Study, supra note 198, at 833.
267 Id.
268 See Fred Stokeld, Taxpayer Advocate Blasts IRS’s Handling of Innocent Spouse Case, TAX NOTES (Jan. 31, 2011), http://www.woodporter.com/Publications/Articles/pdf/Taxpayer_Advocate_Blasts_IRS_Handling.pdf [https://perma.cc/YHE4-ED5M].
271 See McMahon Empirical Study, supra note 212, at 635.
272 Clarke Study, supra note 198, at 833.
273 Id.
274 For a complete description of the Clarke Study and its reliance on the McMahon Empirical Study. See id. at 834.
275 See McMahon Empirical Study, supra note 212, at 648, 649 (noting that 89.2% of appeals from IRS innocent spouse relief decisions are heard in Tax Court). Remaining cases are heard in the Court of Claims, District Courts, and Circuit Courts). Id.
1. Election Under Section 6015(c)

“Actual knowledge” under I.R.C. § 6015(c) is determined according to a facts and circumstances test detailed in Treasury Regulation § 1.6015-3(c)(2)(iv). This test involves, for example, exploring whether the spouse deliberately avoided learning about an item on the tax return or had an ownership interest in the property that resulted in an erroneous item on the return. At the same time, the IRS’s burden in proving “actual knowledge” is a mere preponderance of the evidence, which stands in sharp contrast to the beyond a reasonable doubt standard necessary for a criminal conviction of the noncompliant spouse. One bright side for the innocent spouse is that the IRS cannot meet the preponderance of the evidence standard with mere proof of what a reasonably prudent person would be expected to know.

In terms of this Article, the “omitted income” innocent spouse cases are the most relevant. A noncompliant spouse—and by virtue of joint and several liability, their compliant spouse—who fails to report offshore income would fall into this category. A major problem with innocent spouse relief in the context of omitted income cases is the key question that the IRS and courts ask: whether the “innocent spouse” had knowledge of the receipt of income, not knowledge of the source of income. For example, if a wife knows the husband owns corporate stock but does not know a dividend has been paid, she remains eligible for innocent spouse relief. However, if a wife knows that $150,000 was received but does not know the source of the money, she becomes ineligible.

Even more perplexingly, under the Treasury Regulations, lack of knowledge of how an item was reported is not relevant. In the 2002 D.C. Circuit case Mitchell v. Commissioner, a wife was held ineligible for innocent spouse relief because she knew of the receipt of a retirement plan distribution even though she did not know the tax consequences of the distribution. The Fifth Circuit case Cheshire v. Commissioner bars relief for all spouses with actual knowledge of the income producing transaction, even if such spouses lack knowledge of the incorrect tax reporting of the transaction. However, in Martin v. Commissioner of Internal Revenue, a wife who knew her husband had transferred stock and land but did not know the amount that was transferred was deemed not to have actual knowledge regarding the amount of financial gain.

277 Id.
278 Id. § 1.605-3(c)(2).
280 See Treas. Reg. § 1.6015-3(c)(2)(i), (iii).
281 Id.
282 See id.
283 Id. § 1.6015-3(c)(2)(ii).
from the transaction. One may conclude that the only “knowledge” required to disqualify a compliant spouse is knowledge of the amount of money received, not knowledge of incorrect reporting or of failure to report the income.

Under the current law, coercion and deception, both of which are likely relevant in the offshore context, are not enough to achieve innocent spouse relief. Although due to a change in 2012 coercion was to receive greater weight in terms of the balancing factors used in determining whether innocent spouse relief will be granted, it has served an unclear role. A dispositive indicator of coercion is whether abuse was present. However, coercion and abuse have been treated inconsistently in this context. In 60.7% of the cases where abuse was alleged, the court found no abuse but still granted relief in 14.7% of these cases. In 27.3% of cases where abuse was found, no relief was granted.

Currently, the innocent spouse relief form does not even ask about deception. While a lack of knowledge does not necessarily mean deception is present, it is an important factor to consider in determining whether a wife was innocent in signing a return. In 2012, it was determined that deception alone was not enough for relief. In fact, wives who have asserted they were deceived about an ineligible deduction or unreported income have had this argument backfire. In other words, they were denied relief because they were deemed to have actual knowledge of the deficiency.

Moreover, due to a change in 2012, it was supposed to become easier to achieve relief where abuse or a lack of financial control were shown. These factors were to outweigh others in the balancing test. Clearly, that has not been the case as illustrated in the next section.

2. Election Under Section 6015(f)

Unfortunately, wives who are victims of domestic abuse, including financial abuse, often are not provided with innocent spouse relief because the tax system misconceives the nature of domestic violence. Specifically, the factors the IRS

---

287 McMahon, supra note 162, at 156.
288 Id. at 151.
289 See McMahon, Empirical Study, supra note 212, at 695.
290 Id.
291
293 McMahon, supra note 162, at 152.
294 See Chesire v. Comm’r, 115 T.C. 183 (2000), aff’d, 282 F.3d 326, 335 (5th Cir. 2002); Wiskell v. Comm’r, 90 F.3d 1459, 1462–63 (9th Cir. 1996).
295 See Cheshire, 282 F.3d at 335; Wiskell, 90 F.3d at 1463.
and the Tax Court use to determine whether a victim of domestic violence should receive relief under section 6015(f) often lead to inequitable outcomes.297 There is no guidance in the Internal Revenue Code for how the Tax Court should even evaluate a claim of abuse.298 Instead, there is only Revenue Procedure Ruling 2003-61, which provides a list of factors that the Tax Court should consider in deciding an innocent spouse relief claim.299 Perhaps more distressing, Tax Court opinions reflect inconsistent and unattainable requirements in terms of how to substantiate abuse claims.300 For example, judges have denied claims for relief unless a protection order was granted.301 In other instances, judges have dismissed the alleged abuse as not serious if joint custody of a child has been granted.302 These rulings show that Tax Court judges do not understand the power and control dynamics that accompany domestic abuse.303 Clarke examined sixty Tax Court cases where the innocent spouse sought relief and made a claim of domestic violence.304 Specifically, the study examined whether the Tax Court upheld a claim of domestic violence, and if so, upon what evidence.305 The study then determined whether there was a correlation between a finding of domestic violence and the granting of equitable relief under section 6015(f).306 Clarke noted that her research was aimed at “provid[ing] equitable tax relief to victims of domestic abuse who, because of the misconceptions of domestic violence in the present tax system, might otherwise be unsuccessful in their endeavors.”307

Under section 6015(f), a spouse is granted relief from a tax deficiency provided “taking into account all of the facts and circumstances, it is inequitable” to deny relief.308 To make this determination, the IRS must use a set of revenue procedure guidelines established by the Internal Revenue Service Commissioner in 2003.309

297 See Clarke Study, supra note 198, at 828.  
298 Id.  
300 See Clarke Study, supra note 198, at 828.  
301 See Acoba v. Comm’t, No. 4002-05S, 2010 WL 1993610, at *5 (T.C. May 19, 2010) (noting that a restraining order had been issued but where it is unclear whether the order was the result of the husband’s abuse during the marriage or after the commencement of the divorce proceedings).  
302 See Sotuyo v. Comm’t, No. 25692-10S, 2012 WL 1021306, at *5 (T.C. Mar. 27, 2012) (concluding that the wife’s evidence of abuse was insufficient to show she failed to challenge the husband’s omission of income because she feared retaliation based upon a grant of joint legal and shared custody and the lack of a supervised visitation order).  
303 See Clarke Study, supra note 198, at 828.  
304 Id.  
305 Id.  
306 Id.  
307 Id. at 828–29.  
must meet seven threshold requirements before the request for equitable relief under section 6015(f) will even commence. 310 If a requesting spouse meets these seven threshold requirements, she may automatically qualify for relief under section 6015(f) provided she falls under the safe harbor. 311 To qualify under the safe harbor, she must show (1) she is legally separated or divorced at the time of requesting relief; 312 (2) she had no knowledge or reason to know at the time she signed the return that her spouse would not pay the liability; 313 and (3) she would incur economic hardship if relief were denied. 314 At the same time, if the innocent spouse does not satisfy the safe harbor requirements, the IRS can still conclude that equitable relief is warranted by using a balancing test. 315 A non-exhaustive list of balancing factors also is set forth in Revenue Ruling 2003-61. 316 These factors include whether the innocent spouse benefited significantly from the failure to pay taxes owed, was subject to abuse, or had poor mental or physical health when she signed the return. 317 The IRS will then determine whether each of the balancing factors supports relief, does not support relief, or is neutral. 318 In terms of innocent spouse relief applicants who are also victims of domestic violence, the two most important facts to prove concern (1) whether she had knowledge of the understatement of tax and (2) whether she was abused in the marriage. 319

310 Id. at 297. These seven threshold requirements are the following: (1) the filing of a joint return, (2) an inability to qualify for relief under IRC §§ 6015(b) and (c), (3) a timely application for relief, (4) an absence of fraudulent transfers of assets, (5) an absence of transfers of disqualified assets, (6) an absence of fraudulent intent, (7) the tax deficiency is due to the non-requesting spouse. Id.

311 Id. at 298.

312 Id.

313 In terms of this factor, the court considers (1) her level of education; (2) the presence of deception or evasiveness on the part of the husband, (3) her degree of involvement in the activity leading to the income tax liability, (4) her involvement in business and household financial issues, (5) her financial expertise, and (6) any lavish spending or purchases. Id.

314 Id. In order to determine economic hardship, factors detailed in Treas. Reg. § 301.6343-1(b)(4) are used. Rev. Proc. 2003-61, 2003-2 C.B. 298. These factors include (1) the wife’s age, employment, ability to earn, and number of dependents, (2) reasonably necessary expenses for basic living expenses such as food, clothing, housing, medical, and transportation; and (3) cost of living in the relevant geographic area. Treas. Reg. § 3.01.6343-1(b)(4) (2018); Rev. Proc. 2003-61, 2003-32 C.B. 298; see also Butner v. Comm’r, 93 T.C.M. (CCH) 1290, 1297 (2007) (“[E]conomic hardship exists if collection of the tax liability will cause a taxpayer to be unable to pay such taxpayer’s reasonable basic living expenses.”).

315 Butner, 93 T.C.M. (CCH) at 1296.


317 Id. at 299.

318 Id. at 298.

319 Id. at 298–99. The requesting wife must prove that she did not have knowledge or reason to know. Id. at 298. Failure to do so will count against her claim for relief. Id. Failure to prove abuse, on the other hand, will have a neutral effect. Id. at 299.
If a requesting spouse can establish duress, she will be entitled to innocent spouse relief. However, if she is unable to prove duress and does not fall within the safe harbor provision above, she will be left with trying to prove abuse during the marriage. It is important to understand the difference between duress and abuse. Duress must be present at the time of the signing of the return, i.e., it is the forcing of the wife to sign the return. In contrast, abuse (not rising to the level of duress) is different from duress in two fundamental ways: (1) it is perceived as less severe and (2) it occurs either before or after the signing of the return, not at the time the return is signed. For example, factor two of the safe harbor provision, i.e., lack of knowledge, was not satisfied in Venables v. Commissioner because the wife knew that their family was suffering financial difficulty when she signed the return. However, under the balancing test, the wife was able to show abuse. The Tax Court recognized that the husband financially controlled the wife by threatening to physically harm her whenever she asked to withdraw funds from their joint account. As a result, the wife was granted equitable relief despite her having had knowledge. Clarke provides a summary of the types of evidence the Tax Court relies upon in determining that abuse was present and the “potential biases and inconsistencies” that plague the analyses.

Wives of noncompliant spouses should be entitled to relief due to the nature of their circumstances. This Article proposes that a spouse who has knowledge of the receipt of income, but who lacks knowledge of its source, i.e., who did not know that it came from hidden offshore assets/accounts (later discovered), should be eligible for innocent spouse relief under I.R.C. § 6015(c). Such spouses should be eligible to apply for innocent spouse relief before collection activity starts and even before the IRS notifies the taxpayer of an audit or possible outstanding liability.

To summarize leading scholars in the area, innocent spouse relief is both under- and over-inclusive. The purpose of this Article is not to explore the overall shortcomings of innocent spouse relief. Rather, this Article focuses on granting wives of noncompliant spouses innocent spouse relief in order to promote their whistleblowing either during or after dissolution proceedings. A general belief among scholars in the area is that innocent spouse relief should

---

320 Id. at 297.
325 See id. at *7.
326 Id. at *1.
327 Id. at *7.
328 Clarke Study, supra note 198, at 832.
330 See, e.g., McMahon, supra note 162, at 151.
be available for taxpayers who are not culpable in filing. Clearly, the wives of noncompliant spouses satisfy that criteria. Namely, this Article argues that coercion and deception should automatically entitle relief. In the offshore context described in Part I, at least one of these factors, and likely both, are present. As a result, it is not only “appropriate” but also expedient in terms of overall collection objectives to grant such wives relief.

D. Rethinking Domestic Abuse and Innocent Spouse Relief

A common misconception about domestic violence is that victims fall within a certain stereotype. Typically, the perception is that such women are part of a lower socioeconomic class and also are either racial minorities or immigrants. Unfortunately, this latent bias leads many to fear that judges will not find domestic violence exists if the victim does not conform to these stereotypes. One may conclude that the wives of high-net-worth tax evaders will not fall within these stereotypes by virtue of their socioeconomic status alone. As a result, Clarke set out to elucidate the “diverse profiles of domestic violence victims” to disprove the veracity of traditional stereotypes. Moreover, she explored whether Tax Court judges nevertheless continue to award innocent spouse relief based upon inaccurate stereotypes. The following Part makes use of the Clarke Study to examine the obstacles that will

---

331 See, e.g., id. at 145.
332 See id. at 176–77.
333 See, e.g., Cynthia Willis Esqueda & Lisa A. Harrison, The Influence of Gender Role Stereotypes, the Woman’s Race, and Level of Provocation and Resistance on Domestic Violence Culpability Attributions, 53 SEX ROLES 821, 822 (2005); Zanita E. Fenton, Domestic Violence in Black and White: Racialized Gender Stereotypes in Gender Violence, 8 COLUM. J. GENDER & L. 1, 6, 10 (1998).
336 See Clarke Study, supra note 198, at 835.
337 Id.
confront wives of high-net-worth tax evaders in seeking innocent spouse relief under section 6015(c) or section 6015(f) through the lens of likely attendant domestic abuse and proposes a solution.

1. Domestic Abuse Victims Married to Primary Wage Earners

Importantly for these purposes, in more than 60% of the Clarke Study cases, i.e., those where the requesting wife also alleged abuse, the abuser was the primary wage earner. In the high-net-worth divorces addressed here, the husband would also likely be the primary wage earner. As a result, Tax Court judges should be more cognizant of the likelihood that abuse is occurring in the cases described in Part I and rule appropriately.

As the Clarke Study evinces, there is no one distinguishing profile of a “domestic abuse victim seeking tax relief.” A wife’s educational level, employment qualifications, etc. are varied. However, one constant theme is the “economic dependence and financial control” present. In approximately 53% of the cases, the non-requesting spouse had complete control over finances. The requesting spouses alleging abuse typically reported that they either were given a strict allowance or knew nothing about the family’s finances. Relevantly, most of the requesting spouses were not alleging financial abuse even though it was present. Instead, they were asserting physical, verbal, or emotional abuse. Unfortunately, none of the regulations deal with whether financial control is indeed circumstantial evidence of abuse. Clarke strongly urges that where a requesting spouse is unable to provide evidence to corroborate allegations of other forms of abuse, judges should weigh the presence of financial abuse as indicative of abuse.

2. Preconceived Notions of Abuse

An overarching and pervasive problem is how Tax Court judges perceive abuse. As recently apparent, media coverage perpetuates a conception of

---

338 Id. at 843. Clarke makes clear that in her study “91.67% of the requesting taxpayers who alleged abuse were women.” Id. at 836.
339 Id. at 854.
340 Id.
341 Id.
342 Clarke Study, supra note 198, at 854.
343 Id.
344 Id.
345 Id.
346 Id.
347 Id. at 855.
348 See Clarke Study, supra note 198, at 856.
domestic abuse as involving physical violence and protection orders.\footnote{See Susan R. Paisner, Five Myths About Domestic Violence, WASH. POST (Feb. 23, 2018), https://www.washingtonpost.com/outlook/five-myths/five-myths-about-domestic-violence/2018/02/23/78969748-1819-11e8-b681-2d4d462a1921_story.html?utm_term=.c351d5c11caf [https://perma.cc/4LNK-PBEM].} As a result, if a requesting spouse alleges mental, emotional, or financial abuse, Tax Court and other judges will be reluctant to find abuse occurred because this type of abuse does not fit within their preconceived notions.\footnote{See Clarke Study, supra note 198, at 844.} At the same time, a wife who alleges physical abuse and does not have photos, protective orders, or medical records may also face an insurmountable obstacle in proving abuse in Tax Court.\footnote{See id.}

In the controversial \textit{O’Neil v. Commissioner} decision,\footnote{O’Neil v. Comm’r, 104 T.C.M. (CCH) 724, 730 (2012).} the American public became somewhat aware of the narrow view of domestic abuse used by Tax Court judges.\footnote{See Clarke Study, supra note 198, at 844 (describing the holding as “narrow”); Peter J. Reilly, Tax Court Not Quick to Find Abuse in Innocent Spouse Case, FORBES (Dec. 18, 2012), https://www.forbes.com/sites/peterjreilly/2012/12/18/tax-court-not-quick-to-find-abuse-in-innocent-spouse-case/#2e0c3c33e0b6 [https://perma.cc/LJ3E-TM7U].} Judge Holmes concluded that the plaintiff, Allison, did not prove abuse because there was no “documentation” of it.\footnote{O’Neil, 104 T.C.M. (CCH) at 733.} Attorney Cathy Brennan criticized this view since it fails to take account of the true dynamics of an abusive relationship and how an abuser “dominates all aspects of his partner’s life and uses all tactics available to him to control her.”\footnote{Reilly, supra note 353.}

Indeed, there is a high likelihood that this type of abuse is present where the husband is using offshore accounts and entities to hide money from his spouse. Taking the money offshore and then refusing to provide the wife with any information about it is part of a cycle of domination and control. Even when faced with sanctions and motions to compel in the family law context, an abusive husband will not provide his victim with requested information, reflecting a pervasive need to continue to control her.\footnote{See \textit{Coercive Control}, in ENCYCLOPEDIA OF DOMESTIC VIOLENCE 166, 169 (Nicky Ali Jackson ed., 2007).}

While the marital status of the wives described in Part II would weigh in favor of relief, the inconsistent and perplexing treatment of abuse in Tax Court will make the road to relief a difficult or impossible one. The Tax Court places significant weight on the marital status of the requesting spouse.\footnote{Clarke Study, supra note 198, at 837 (citing Rev. Proc. 2003-61, 2003-2 I.R.B. 296, 298).} Under section 6015(c), relief may be obtained only if the spouse is separated or divorced.\footnote{I.R.C. § 6015(c)(3)(A) (2012).} Although a spouse who is still married may seek relief under section 6015(f), it will weigh against the grant of such relief under the balancing
test of Revenue Procedure 2003-61.\textsuperscript{359} In fact, marital status has proven determinative.\textsuperscript{360}

In terms of considering when to file, scholars have noted that abuse often continues after the marriage has ended.\textsuperscript{361} For example, joint custody provides an abuser with an opportunity to continue to exert power and control over a victim.\textsuperscript{362} In light of this phenomenon, it must be acknowledged that some wives will avoid filing for innocent spouse relief even after separation or divorce because they fear retaliation.\textsuperscript{363} As a result, some women choose to postpone filing for innocent spouse relief until after their abuser dies.\textsuperscript{364}

Another related obstacle is the question among Tax Court judges why women do not allege domestic violence in divorce proceedings or on the innocent spouse request forms, choosing instead to wait until the case is before the IRS or Tax Court.\textsuperscript{365} This causes judges to suspect that the wife is lying about or embellishing the abuse.\textsuperscript{366} However, they fail to realize that oftentimes the women do not disclose the abuse earlier out of fear or because of the “legal repercussions.”\textsuperscript{367} For example, the presence of children in the marriage may affect whether the wife will allege domestic violence in a divorce proceeding.\textsuperscript{368} Moreover, scholars have noted that many victims of domestic violence are unable to perceive how dire the situation is, and these women are often caught in denial and secrecy.\textsuperscript{369} As a result, some women who have been abused will

\begin{thebibliography}{9}
\item \textsuperscript{359} Id. § 6015(f).
\item \textsuperscript{360} See Clarke Study, supra note 198, at 838 (illustrating this with a table entitled “Marital Status of Those Seeking Relief”).
\item \textsuperscript{361} See Clarke Study, supra note 198, at 839, 839 n.84. Orly Rachmilovitz, Bringing down the Bedroom Walls: Emphasizing Substance Over Form in Personalized Abuse, 14 WM. & MARY J. WOMEN & L. 495, 501 (2008) (explaining that even after the relationship has ended, the abuser continues to assert control over the victim through available access); Lauren A. Kent, Comment, Addressing the Impact of Domestic Violence on Children: Alternatives to Laws Criminalizing the Commission of Domestic Violence in the Presence of a Child, 2001 Wis. L. REV. 1337, 1364 (2001) (contending that joint custody allows abusers repeated access to victims and a means of exerting continued control).
\item \textsuperscript{362} See id. at 839.
\item \textsuperscript{363} See id. at 839–40.
\item \textsuperscript{364} See id. (explaining that widow status serves as a type of safeguard against retaliation but also noting that only 30% of women widowed at the time of filing secured innocent spouse relief).
\item \textsuperscript{365} Id. at 855.
\item \textsuperscript{366} Id.
\item \textsuperscript{367} Clarke Study, supra note 198, at 855.
\item \textsuperscript{368} See id. at 848, 855 (listing other factors that should be considered, including “(1) the length of time between legal proceedings where abuse was not alleged and the current innocent spouse case, (2) whether the non-requesting spouse resides in close proximity to the victim or whether he has relocated, [and] (3) whether the victim and abuser are in new personal relationships”).
\item \textsuperscript{369} See id. at 856, 856 n.164.
\end{thebibliography}
need time to realize that they were subject to abuse. Such wives should not be punished for delaying in making an abuse claim.

Again, behavior in the family law context could inform the tax context. For instance, family mediators and family law judges often do not have proper insight into domestic abuse, and as a result, alleged abusers are frequently awarded sole or joint custody of children. They suffer from the same reliance on stereotypes as Tax Court judges attempting to parse through abuse allegations. Here again, unreasonable behavior on the part of the noncompliant spouse in terms of custody mediation or time share plans should signal to the Tax Court that abuse allegations should be more fully considered in determining whether to grant innocent spouse relief.

3. Correlation Between Abuse Claims & Innocent Spouse Relief

Tax practitioners are correct in determining there is a correlation between a Tax Court judge’s upholding an abuse claim and granting innocent spouse relief. In fact, the Clarke Study showed that in 90% of cases where abuse was judicially determined, equitable relief under section 6015(f) was granted. The problem is that Tax Court judges who are often unfamiliar with domestic abuse do not have a definition of abuse and have been given a non-exhaustive list of factors to consult. Regarding the first issue, the only guidance Tax Court judges have in terms of defining abuse is provided in Revenue Procedure 2003-61. It requires that the wife have been a victim of abuse prior to signing the return and that given the abuse, she was afraid that refusing to sign the return would result in retaliation. There is really no definition provided at all.

370 See id. at 856.
372 See id. at 841.
373 See Clarke Study, supra note 198, at 841.
374 See id. at 846; see also Aiding Innocent Spouses from Joint Tax Liabilities, YOURABA (Sept. 2011) (on file with the Ohio State Law Journal) (discussing the difficulties of obtaining innocent spouse relief).
375 See Clarke Study, supra note 198, at 846.
376 See id.
378 Id.
4. Problematic Corroboration Requirement

Judicial interpretation of Revenue Ruling 2003-61 has made it more difficult for victims to secure a finding of abuse. The Tax Court’s further requirement that abuse be corroborated further shows that judges do not understand the nature of the abuse. In terms of physical abuse, even the presence or absence of police reports has not proven dispositive. Compounding the problem is the perception of domestic violence as a “private matter” by both police officers and judges. Domestic violence is common and under-reported. According to a 2003 study, only 14.5% of serious assaults lead to police reporting. Many women choose not to report domestic violence because they are afraid of retaliation, endangerment to children, and public ridicule.

Tax Court judges’ additional requirement that a claim of abuse be corroborated before it can weigh in favor of a grant of relief is particularly problematic in the context of non-physical abuse. However, even when victims have provided third party testimony of verbal and mental abuse, Tax Court judges have dismissed this form of corroboration as inadequate, and their rulings have been inconsistent. For example in Collier v. Commissioner, the wife called a friend to testify about her husband’s verbal onslauts that she had

379 See id. at 848 (discussing corroboration requirements).
380 See id.
381 See, e.g., McKnight v. Comm’r, 92 T.C.M. (CCH) 76, 81 (2006) (finding that the abuse had been corroborated despite the lack of criminal charges brought or medical attention sought where the police were called to the home on two occasions due to violent attacks); cf. e.g., Sotuyo v. Comm’r, No. 25692-10S, 2012 WL 1021306, at *5 (T.C. Mar. 27, 2012) (dismissing an abuse claim corroborated by a police report and concluding the behavior did not rise to the level that would have made the wife sign a return that omitted income out of fear); Ladehoff v. Comm’r, No. 16814-10S, 2012 WL 612501, at *3 (T.C. Feb. 27, 2012) (finding the same in the context of a husband’s request for innocent spouse relief where two police reports had been filed).
383 See Clarke Study, supra note 198, at 848 (citing SHANNAN M. CATALANO, U.S. DEP’T OF JUSTICE, NATIONAL CRIME VICTIMIZATION SURVEY: CRIMINAL VICTIMIZATION, 2003 1 (2004) (finding only 48% of all violent victimizations are reported)).
384 See KELLY, supra note 382, at 3.
385 See Clarke Study, supra note 198, at 848 (citing Barbara R. Borreno, In Search of Guidance: An Examination of Past, Present, and Future Adjudications of Domestic Violence Asylum Claims, 64 VAND. L. REV. 225, 243 (2011)) (revealing the perception of domestic violence as a “hidden problem” involving “invisible” victims that tend not to tell others about the abuse due to a number of reasons, including fear and shame).
witnessed as well as a psychologist she had seen for depression. Nevertheless, the Tax Court was dismissive of her friend’s testimony, characterizing it as conclusory and similarly found that the psychologist’s testimony was insufficient to establish abuse.

In contrast, the Tax Court held in Chadwick v. Commissioner that the wife’s testimony alone was adequate to establish that she had been abused during the marriage. Similarly, in Thomassen v. Commissioner, a judge upheld an abuse claim where children and family friends testified as to the presence of abuse.

The corroboration requirement prevents wives of high-net-worth tax evaders from securing relief even if they have been abused. Most wives seeking innocent spouse relief will not have protection orders and police reports that they can introduce during a trial. In addition, many wives will not have third parties who can testify as to the abuse because one of the tactics of an abuser is to isolate the victim to engender co-dependence and to cut off the victim from available help. Finally, many wives will not check the box indicating abuse on Innocent Spouse Relief Request Form 8857 because the IRS is mandated to contact their husbands even where domestic violence is at issue. While the wife’s information is protected during the IRS review of the request, if she appeals a denial to the Tax Court, all of the information listed on the form becomes discoverable. The key to resolving this problem is affording proper weight to provable financial abuse.

5. Financial Abuse Mitigates “Knowledge”

Tax Court judges have been extremely reluctant to uphold abuse claims where non-physical abuse has been alleged. At the same time, the current

---

388 See id.
389 See id.
392 See Clarke Study, supra note 198, at 849.
393 See id.
394 See Coercive Control, supra note 356, at 169.
396 See id. at 850, 850 n.133 (explaining that if there is an appeal, protected information becomes discovery; however, Tax Court Rule 27 (d)(1) does permit the requesting spouse to request a protective order that would require redaction).
397 See, e.g., Nihiser v. Comm’r, 95 T.C.M. (CCH) 1531, 1536–37 (2008) (characterizing nonphysical abuse as “easily exaggerate[d]” where the wife alleged verbal abuse from her husband who was suffering from drug addiction). This was the first time that a Tax Court recognized “objective indications” of abuse that did not involve physical
regulations do not address whether financial control constitutes circumstantial evidence of abuse. Clarke argues that financial abuse should serve as a lens through which to view the other factors in Revenue Ruling 2003-61, such as the “knowledge or reason to know” factor.

The “knowledge or reason to know” factor means that a requesting spouse “did not know and had no reason to know of the item giving rise to the deficiency.” As discussed earlier, “actual knowledge” that money was received often disqualifies wives in the section 6015(c) context as well. Clarke emphasizes that financial abuse, along with allegations of other types of abuse, should be enough for a requesting spouse “to be successful on this knowledge factor.” Logically, if the domestic violence victim lacks information about the family’s finances and is subject to abuse whenever she asks, she should be deemed not to have knowledge or reason to know of the item and therefore granted relief. This is even more so true in the context of a wife hiring a team of forensic accountants during a divorce proceeding. Unfortunately, the newly proposed regulations of 2012 do not incorporate this line of reasoning and the rationale.

There are issues surrounding financial abuse and in particular, whether it could mitigate the “knowledge” factor in determining whether relief is merited. Many times, victims are not aware of tax and other financial affairs because the noncompliant spouse exerts control over the information. This is even more so the case in the specific types of divorces discussed. Again, if the wife had access to financial information, she would not need to hire a team of forensic accountants or attempt to use family law proceeding discovery motions to unearth information. Fortunately, at times, Tax Court judges have upheld mental and emotional abuse claims where extreme financial control is shown. For example, in Bishop v. Commissioner, the wife was prohibited from accessing the couple’s bank accounts. Notably, there was no allegation of physical abuse. Her request for innocent spouse relief was granted.

However, the Tax Court’s rulings where financial abuse is alleged have not been consistent. Prior to Bishop, the Tax Court denied a nurse’s request for

---

violence, such as isolation, threatening suicide, substance abuse, and degrading the victim, among others. See Clarke Study, supra note 198, at 852.

398 Clarke Study, supra note 198, at 854.
399 See id. at 855.
401 See, e.g., Cheshire v. Comm’r, 282 F.3d 326, 336 (5th Cir. 2002).
402 Clarke Study, supra note 198, at 855.
403 See id.
404 See id. at 854.
405 See id. at 832.
406 Id. at 852.
408 Id. at *2.
409 Id. at *4.
410 Id. at *8.
relief, finding that given her education she could not have been “oblivious” to the family’s finances. Given that wives may readily prove financial abuse and the attendant difficulties with proving physical abuse, the Tax Court’s hesitancy in recognizing the former is distressing. Greater judicial recognition of financial abuse is the key to providing more abuse victims with appropriate relief in this context.

Notably, in January 2012, the IRS issued a proposed revenue procedure that would modify IRS review of innocent spouse relief requests, particularly in regard to abuse. In other words, it would supplant Rev. Proc. 2003-61, 2003-32 I.R.B. 296. As detailed in Notice 2012-8, the proposed regulation would address how abuse could influence a spouse’s reluctance to challenge false or fraudulent statements on a tax return. Although the proposed regulation is a step forward in confronting some of the problems plaguing wives seeking innocent spouse relief, additional guidance is necessary given the current inadequacies discussed herein.

For example, as stated above, most domestic violence victims do not have the police reports and protective orders that Tax Court judges require to make a finding of abuse. Moreover, the judges do not have clear criteria for making a determination on the issue of abuse.

E. Remaining Issues

At the same time, there is a potential for abuse in modifying innocent spouse relief in the manner proposed. For example, a “not so innocent spouse” who actually knew about offshore accounts/assets and the failure to report, may be allowed to keep the luxuries afforded by a violation of the law. Undeniably, some spouses likely would collude together to use innocent spouse relief to reduce their tax liability. At the same time, former spouses may use innocent spouse relief to escape tax liability while also punishing their former spouse.

In thinking about possible expansion, one must consider the current system and the current scholarly landscape in terms of reform. The current system, most recently modified in January 2012 by the Treasury Department, already

412 See Clarke Study, supra note 198, at 853.
413 Id.
415 See id. at 854.
416 See id.
417 See id.
418 See id.
419 Id.
420 See McMahon, supra note 162, at 145.
421 See id. at 144 n.15 (noting that it is impossible to anticipate the frequency of this behavior, but explaining that the 1948 inception of the income-splitting joint return was in response to Congress’s perceived collusive income shifting).
422 See id. at 144–45.
absolves spouses who were not coerced but who chose to sign returns.\textsuperscript{423} Generally, such spouses have benefited from paying less tax due to the filing of a false return.\textsuperscript{424}

However, a particularly important general distinction may be drawn in the case of wives of noncompliant spouses. It is likely that these wives have not benefited substantially from the filing of false or fraudulent returns because the noncompliant spouses likely also committed financial abuse and reinvested the hidden assets into other offshore ventures.\textsuperscript{425} After all, if the wife of a noncompliant spouse was benefiting substantially from the offshore funds, she may have become alerted to their presence.\textsuperscript{426} The wives discussed in this Article have remained largely in the dark about their husband’s offshore finances, necessitating the hiring of teams of forensic accountants.

Some of the viewpoints on innocent spouse relief do not adequately reflect wives’ agency.\textsuperscript{427} While scholars agree that feminist theory cannot provide a clear direction for tax policy, it is a vital aspect to any discussion of innocent spouse relief.\textsuperscript{428} There is no uniform feminist position regarding most tax issues.\textsuperscript{429} The main reason for the lack of consensus is that liberal feminists contend for equality between the sexes while cultural feminists contend there are inherent differences between women and men.\textsuperscript{430} There are shifting viewpoints between protectionist and equality models that inform the debate.\textsuperscript{431} A related paradox is how women could be equal in terms of the law but still disadvantaged when compared to men.\textsuperscript{432} McMahon argues that an expansion of innocent spouse relief may have the ill effect of further “reinforcing wives’ vulnerability.”\textsuperscript{433} However, this Article takes the view that expanding innocent spouse relief, particularly in cases of financial and other domestic abuse, will

\textsuperscript{424} McMahon, supra note 162, at 145.
\textsuperscript{425} McCarden, supra note 29, at 28–29.
\textsuperscript{426} See id.
\textsuperscript{427} McMahon, supra note 162, at 145 n.17. As McMahon points out, gendered implications associated with innocent spouse relief are more complicated because same-sex couples can file joint returns. Id. at 145. This Article also does not address this additional dimension.
\textsuperscript{429} See id. (discussing the proposition that feminists disagree on policy ideas and objectives); McMahon, supra note 162, at 145 (discussing how a single feminist theory on tax policy is impossible because of conflicting ideas); see, e.g., Patricia Cain, Taxing Families Fairly, 48 SANTA CLARA L. REV. 805 (2008).
\textsuperscript{430} McMahon, supra note 162, at 145–146; see Martha Albertson Fineman, Grappling with Equality: One Feminist Journey, in TRANSCENDING THE BOUNDARIES OF LAW: GENERATIONS OF FEMINISM AND LEGAL THEORY 47, 49–50 (Martha Albertson Fineman ed., 2011).
\textsuperscript{431} See Fineman, supra note 430, at 50.
\textsuperscript{432} See McMahon, supra note 162, at 146. See generally MARTHA ALBERSTON FINEMAN, THE AUTONOMY MYTH (2004).
\textsuperscript{433} See McMahon, supra note 162, at 168–74 (discussing whether innocent spouse relief hurts wives although it was enacted to help them).
empower women to report the offshore tax and other misdeeds of their noncompliant spouses.

Domestic abuse is an area that the United States as a whole is just beginning to understand. Tax Court judges and tax practitioners do not normally deal with domestic abuse. The U.S. Department of the Treasury, the IRS, and many Tax Court judges have acknowledged that they are not familiar with the complexities of domestic violence. Reform must occur so that victims of domestic violence may obtain equitable relief under section 6015(f) or relief under section 6015(c) even if a Tax Court judge is unfamiliar with domestic violence. One way this may happen is through permitting financial abuse, coupled with other forms of abuse, to satisfy the “knowledge factor.” The underlying rationale for doing so makes sense.

IV. WIVES AS OFFSHORE WHISTLEBLOWERS DURING DIVORCE

The government has two primary ways of discovering tax noncompliance under current law. The main way is through governmental examination power, which enables the government to audit taxpayers’ returns and then reach a conclusion as to whether such returns comply with the law. The second way is through using whistleblowers who may serve as a “tool for peeking inside the otherwise private zone of voluntary compliance.” The government and the IRS lack the resources to investigate privately the immense amount of offshore tax evasion in the United States. Thus, we should encourage wives who have uncovered information regarding offshore tax cheating during divorce to whistle blow. A system for doing so must take into account necessary protections in light of the risks posed, especially where abuse has been a factor.

---

434 See Clarke Study, supra note 198, at 856.
435 See id.
436 See id.
437 See id.
438 See infra notes 439–440 and accompanying text.
442 See infra Part III.B.
443 See id.
Empowering wives to whistle blow will have exponential effects as partners and business associates of noncompliant spouses also will be identified.444

A. IRS Whistleblower Program

Since 1867, the IRS has had the authority to pay monetary awards to whistleblowers who report tax frauds and evaders.445 The initial IRS Whistleblowing Program under I.R.C. § 7623 was ineffective due to its decentralized management, inadequate oversight, and restriction to only discretionary awards.446 In 2006, these shortcomings resulted in Congress’ amending the program to incentivize potential whistleblowers to report tax fraud and evasion.447 I.R.C. § 7623 has been interpreted as providing the IRS with broad discretion in terms of determining and paying whistleblower awards.448 Prior to 2006, the IRS gave a minimum award of 1% and a maximum award of 15% of amounts recovered, which was capped at $2 million.449 Whistleblowers had no right to appeal award decisions, and there were no advertisements for the program.450 Moreover, IRS employees could not seek out potential whistleblowers.451

Congress amended section 7623 with section 406 of the Tax Relief and Health Care Act of 2006.452 A major aim of the amendments was to encourage whistleblowers to report tax fraud and evasion and thereby raise revenue for the government.453 A significant change was the increase in the amount of...

444 See id.
445 Dennis J. Ventry, Jr., Whistleblowers and Qui Tam for Tax, 61 TAX LAW. 357, 381–82 (2008) (noting a 15% to 20% increase in the tax whistleblower bar since the passage of the 2006 amendments).
446 Ashlin Aldinger, A Race to the IRS: Are Snitches and Criminals the New Business Model?, 51 H OUS.L. R EV. 913, 923 (2014) (noting some of the drawbacks to the initial whistleblower program).
447 Ventry, supra note 445, at 362–64 (discussing monetary incentives for whistleblowers).
448 Aldinger, supra note 446, at 924.
449 See id.
450 See Michelle M. Kwon, Whistling Dixie About the IRS Whistleblower Program Thanks to the IRC Confidentiality Restrictions, 29 VA. TAX REV. 447, 453 (2010) (noting that before the 2006 amendment, whistleblowers had no right to judicial appeals).
451 Id.
453 Prior section 7623 was renamed section 7623(a). The main amendment was the addition of subsection (b). Pursuant to subsection (b), whistleblower awards are now mandated at a minimum of 15% of the amount collected, including, inter alia, any attendant penalties and interest as a result of an IRS initiated action. The maximum award is now 30% of such proceeds. Section 7623(a) now longer includes the nominal cap under prior law. I.R.C. § 7623 (2012). Notably, whistleblower claims under § 7623(b) are appealable whereas those under the prior 2006 amendment, i.e., § 7623(a) are not. I.R.C. § 7623(b)(4) (2012); I.R.S. Notice 2008-4 I.R.B. 254 (Jan. 14, 2008), https://www.irs.gov/pub/irs-irbs/irb08-
whistleblower awards.\textsuperscript{454} Congress made this step in order to decrease the tax gap, i.e., “the difference between what taxpayers owe and the amount timely paid.”\textsuperscript{455} The tax gap is a result of the voluntary compliance aspect of our federal income tax system.\textsuperscript{456} It is no secret that the IRS uses the whistleblower program to raise revenue.\textsuperscript{457} In 2015, missing tax revenue totaled at least $450 billion.\textsuperscript{458} Most of this amount is due to unreported taxes.\textsuperscript{459}

The requirements for a whistleblower award are straightforward under the current law.\textsuperscript{460} There are three main requirements: (1) the whistleblower discloses information regarding tax noncompliance dealing with over $2 million;\textsuperscript{461} (2) this information “substantially contributes” to the IRS’s filing an administrative or judicial action;\textsuperscript{462} and (3) the IRS collects funds due to an action or settlement.\textsuperscript{463} The IRS may deny a claim if it already has the information the whistleblower provided, there is no finding of liability, or the

\textsuperscript{454} Aldinger, supra note 446, at 927.

\textsuperscript{455} Id. at 926.


\textsuperscript{458} See Review of the President’s Fiscal Year 2015 Funding Request for the Department of the Treasury and the Internal Revenue Service: Hearing Before the Subcomm. on Fin. Servs. & Gen. Gov’t of the S. Comm. on Appropriations, 113th Cong. 23 (2014) (statement of J. Russell George, Treasury Inspector General for Tax Administration).

\textsuperscript{459} See id. (finding that the $376 billion or approximately 84% of the total tax gap is due to unreported taxes); see also Davis-Nozemack & Webber, supra note 457, at 367.

\textsuperscript{460} See infra notes 461–462 and accompanying text.

\textsuperscript{461} I.R.C. § 7623(b)(5) (2012).

\textsuperscript{462} Id. § 7623(b).

\textsuperscript{463} See Fiscal Year 2012 Report, supra, note 453, at 3.
taxpayer is judgment proof. Additionally, a whistleblower may not receive an award if found to be part of the planning or instigation of the tax scheme. While the amendments to the IRS Whistleblower Program have resulted in more reporting, it does not appear that high quality leads have been reported. This Article addresses how the revamped IRS Whistleblower Program may be used to reduce the international tax gap through the reporting of wives in high-net-worth divorce proceedings described in Part I.

The tax whistleblower program under I.R.C. § 7623 has been criticized frequently over the last several years. In 2006, Congress revised the whistleblower program in connection with the Tax Relief and Health Care Act of 2006. However, counsel for potential whistleblowers have emphasized several continued shortcomings of the program. At least one of these shortcomings is not relevant to the wives that are subject to this Article.

The IRS Whistleblower Program is an under-utilized resource for several reasons. Some scholars have chosen to place the blame squarely at the IRS’s feet, noting its woeful underutilization of whistleblowers. While most legal scholarship on whistleblower programs takes as a premise the ability of the agency to use effectively a tip, this assumption has been challenged in at least


465 I.R.C. § 7623(b)(3).

466 Aldinger, supra note 446, at 928 (noting that although there were 377 submissions in fiscal year 2008, many of these did not result in claims).

467 See Kwon, supra note 450, at 488 (calling the 2006 amendment an “empty promise”); Stephen W. Carman, Note, More Cheese for the Rats: Tax Court and Congress Give Big Win to Whistleblowers with Broad Definition of “Proceeds,” 83 MO. L. REV. 155, 165 (2018) (“[D]espite its lofty goals, the new whistleblower program has failed to fully deliver as promised.”).


469 Aldinger, supra note 446, at 929.

470 Although Code § 6103(n) provides for an exception to the usual prohibitions against disclosing tax return information, the IRS has refused to enter into information-sharing contracts with whistleblowers. As a result, whistleblowers are denied access to financial records. Providing whistleblowers with such access raises serious privacy concerns. See I.R.C. § 6103(n) (2012); see also Aldinger, supra note 446, at 925. However, in the case of a wife in divorce proceedings, she will have access to the joint returns even if she must subpoena them from the IRS.

471 See Davis-Nozemack & Webber, supra note 457, at 322 (explaining that despite receiving over 9,000 tips from whistleblowers in 2014 and having a backlog of over 22,000, the IRS has only paid out approximately 100 awards each year in fiscal years 2009-2014 and inquiring “why has the Service capitalized on so few tips?”).

472 Id. at 323 (“Simply put, the Service does not seek all available information and assistance from whistleblowers.”); see also id. at 341 (discussing Service executive’s attempts in 2012 and 2014 to address the debriefing process for whistleblowers which also ultimately left Service employees with inadequate guidance).
the tax arena. Although there are similarities between the amended IRS Whistleblower Program and the False Claims Act qui tam actions, there are significant differences between the two. These differences have spurred some scholars to consider whether the IRS should also allow for a qui tam action. Currently, there is not a qui tam action available for tax reporters.

B. Empowering Wives to Report Offshore Tax Evasion

Whistleblowing has been perceived as disconcerting and even morally reprehensible since at first glance it may appear to rely upon “bad blood” such as that associated with “office politics or a divorce.” One scholar states there are “serious moral issues” with rewarding individuals for telling on other’s tax noncompliance. However, in the circumstance of a noncompliant spouse acting wrongfully in the family law and tax contexts, this condemnation of whistleblowing is not justified.

In arguing for a repeal of the Whistleblower Program during the Congressional debate of the 1998 Internal Revenue Service Restructuring and Reform Act, Senator Harry Reid characterized the Whistleblower program as the “Reward for Rats” program and denounced it as the “Snitch Program.” Specifically, Senator Reid noted giving money to “snitches” to report their “associates, employers, relatives, and [ex-spouses]” was “unseemly, distasteful, and just wrong.” Nevertheless, as explained above, just eight years later, Congress decided to expand the program in 2006. Regardless of the perceived moral pitfalls, the program has survived because it does result in leads regarding tax evasion and fraud, which enhances tax enforcement efforts thereby tightening the tax gap.
This Article contends that in the divorce context presented, i.e., where a husband is showing a flagrant disregard for discovery in a family law proceeding and for tax reporting, whistleblowing should be viewed as a necessary tool for shedding light onto darkness. This is especially just when one considers the likelihood that at least financial abuse may have also been present in the marriage. 484 Granted, one may take issue with Bradley Birkenfield’s award given his involvement in criminal activity. 485 However, an innocent wife who had no knowledge of her husband’s tax noncompliance and who is later confronted with his overall noncompliance in terms of revealing assets during a divorce proceeding is a different story. One observer asks, “Is it not morally reprehensible to allow a criminal to become wealthy from a tax evasion scheme in which he was personally involved?” 486 In contrast, a wife who is an innocent spouse has at least been determined not to have been personally involved. 487 There is nothing wrong in allowing her to report tax noncompliance.

Furthermore, innocent spouses who are eligible for a whistleblower award may help to alleviate some of the needless backlog that accompanies most family law proceedings where a noncompliant spouse is the party on the other side. 488 In fact, the wife may decide to stop expending funds on forensic accountants and motions to compel if she may receive a share of the marital assets through a whistleblower award. At the same time, of course, there will be wives who would prefer to keep using the family law proceedings with the hope that the marital assets would not have to be shared with the government through the rectifying of unpaid tax. However, this Article addresses the truly innocent spouse who desires to remedy the wrongs of the marriage and to move on with her life in a compliant manner.

There are of course numerous downsides to whistleblowing, 489 and it is unthinkable that a wife would do so without the guarantee of innocent spouse relief. She could end up in jail if criminal prosecution of the husband is


485 Aldinger, supra note 446, at 931 (suggesting that Bradley Birkenfield was only spared because of his more limited criminal involvement instead of having been “the mastermind of the tax violations” and noting that Bradley Birkenfield received the largest whistleblower award in history in 2012 in the amount of $104 million).

486 Aldinger, supra note 446, at 931.

487 See supra Part II.B.


489 The whistleblowing process is long, and the threat of retaliation is a real one. In the employment context, as Aldinger notes, whistleblowers sometimes become unemployable, and there is a high correlation between whistleblowers and bankruptcy. Aldinger, supra note 446, at 932.
successful or with heavy civil penalties to pay. If she has primary custody of the children, she will be unlikely to take such exorbitant risks without the assurance of innocent spouse relief. Unlike other tax whistleblowers, her identity would not be protected. Just as fear of retaliation would cause some wives not to seek innocent spouse relief, it would also deter them from tax whistleblowing. Unfortunately, there is no federal law prohibiting retaliation in the tax whistleblowing context.

Currently, there is not much literature on why whistleblowers choose to report noncompliance. As one author has stated, “[t]he primary purpose of the IRS Whistleblower Program is to encourage the reporting of major tax noncompliance issues.” Scholars have condemned whistleblowers as also likely to have had unclean hands. However, the IRS has acknowledged this possibility and is comfortable with it. Stephen Whitlock, the first director of the IRS Whistleblower Office, specifically stated that “the law recognizes that whistleblowers may have unclean hands, and that’s OK.” Similarly, in the context of innocent spouse relief, there will be times when a wife has benefited from the tax fraud or tax evasion; however, a parallel public policy rationale also justifies extending innocent spouse relief in the context examined in this Article.

What scholars do know is that factors such as “the level of moral outrage” and “the scale of the harm” motivate some whistleblowers to come forward. A wife who has dealt with a noncompliant spouse in a multi-year divorce proceeding and who ultimately finds out her spouse has been hiding offshore assets and accounts would be motivated by both of these factors. The usual impediments to whistleblowing could largely be overcome provided she receives innocent spouse relief. Yuval Feldman and Orly Lobel’s recent empirical study examines the legal factors that cut in favor of whistleblowing, including anti-retaliation measures and monetary incentives.

490 See supra Part II.A.
491 See Clarke Study, supra note 198, at 850.
492 See id. at 848–849.
493 INTERNAL REVENUE SERV., FISCAL YEAR 2011 REPORT TO THE CONGRESS ON THE USE OF § 7623, 13, http://www.irs.gov/pub/irs-utl/fy2011_annual_report.pdf. (explaining that some federal whistleblower laws prohibit retaliation but noting it is not prohibited in terms of tax whistleblowers since there is no federal law remedy although state law may provide otherwise).
494 See Aldinger, supra note 446, at 933.
495 Id.
496 Id. at 916.
497 Id.
498 Id. at 933–34.
499 Id. at 934.
In the context of a contentious, multi-year divorce proceeding, a primary motivating factor for the wife of a noncompliant spouse is shortening the proceedings. For example, if the wife is likely to be granted primary custody of children, she especially will want to end the proceedings as quickly as possible. The wife’s eligibility for a whistleblower award may help to significantly shorten the division of assets portion of the divorce proceedings. Once her forensic accountants are able to uncover hidden offshore assets, theoretically she could whistle blow and share in a portion of the assets through the granting of a whistleblower award. In other words, if the wife can secure a whistleblower award, the division of assets proceedings will be truncated. The IRS will likely receive not only a single lead in regard to the noncompliant spouse’s tax deficiencies but also several leads in terms of his partners and co-conspirators in defrauding the government. Again, a necessary element is that the wife could secure innocent spouse relief before blowing the whistle.\(^{501}\)

Granted, wives who did know or have reason to know about the noncompliant husband’s offshore tax fraud and/or evasion and who decided to look the other way should not receive innocent spouse relief.\(^{502}\) These wives may still choose to whistle blow, but of course, they would remain liable for the previously undisclosed tax liabilities.\(^{503}\) As stated above, the IRS has acknowledged some whistleblowers do have unclean hands, but it deems this acceptable given the role they may play in increasing tax enforcement.\(^{504}\) For example, there is a possibility that some wives who receive innocent spouse relief will in fact have conspired with their husbands against the government during the marriage and will choose to become whistleblowers. In order to minimize this possibility, the wife should be required to show the husband’s noncompliance during the proceedings and evidence of efforts and expenditures to uncover his offshore accounts during the proceedings, e.g., the hiring of forensic accountants, filings of motions to compel, etc. Of course, the hiring of accountants could be gamed to feign lack of knowledge but that should occur infrequently. The relatively small number of cases where a wife has taken the same actions as one who had no knowledge or reason to know is justified by the increase in tax enforcement and related tightening of the tax gap in terms of offshore evasion.

At the same time, regardless of the desire to shorten the proceedings or for a reward, the wives described in Part II may decide to whistle blow for moral or religious reasons, reflecting the need to expose the deceitful behavior of what are likely abusive spouses. Monetary incentives are not always the major factor

\(^{501}\) See supra Part II.C.

\(^{502}\) See supra Part II.D. (arguing that financial abuse should negate a finding that the wife had knowledge or reason to know).

\(^{503}\) See supra Part II.B.

\(^{504}\) Aldinger, supra note 446, at 916.
in a whistleblower’s decision, and “moral outrage, religion or faith, and revenge” may serve as primary motivators. Whistleblowers also state a sense of “legitimacy” serves as a motivating factor. Here, “legitimacy” means a “feeling of obligation to obey the law and to defer to the decisions made by legal authorities.” The factors from the Feldman and Lobel study certainly apply in the corporate or employment context, and some are also relevant to the divorce context. However, one must acknowledge other factors that are akin to the women who chose to report publicly in the #MeToo movement. Many of the women who stepped forward to expose sexual harassment in the #MeToo movement were motivated by a sense of justice and a desire to embolden other women to speak out about their experiences with harassment. These same motivating rationales would be present in a high-net-worth divorce involving abuse as well.

V. CONCLUSION

The Panama Papers have revealed that high-net-worth tax evaders use offshore accounts to hide money from the IRS as well as their spouses. As a result, offshore tax enforcement efforts must harness the potential of divorce proceedings to reduce the international tax gap. While the government and the IRS may lack the time and resources to find hidden offshore accounts, wives involved in high-net-worth divorce proceedings hire teams of forensic accountants for that very purpose. Currently, a wealthy husband who refuses to disclose offshore accounts to his wife is not held accountable in the tax context for his noncompliance in the divorce context. Given that willfulness must be proven to impose civil or criminal liability, family law discovery devices must be modified to ensure their knowing disregard of reporting obligations may be

505 Feldman & Lobel, supra note 500, at 1203 n.285.
506 See Eamon Javers, Religion, Not Money, Often Motivates Corporate Whistleblowers, CNBC (Feb. 12, 2011), http://www.cnbc.com/id/41494697 [https://perma.cc/4UF8-C4BQ] (noting that some whistleblowers are “deeply religious people” and thus their faith provides a distinct identity separate from their corporate careers).
510 See Bennett, supra note 10.
511 See id.
512 See supra notes 6–10 and accompanying text.
proven. Moreover, such spouses should be deemed ineligible for tax amnesty programs after continued noncompliance.

The current denial of innocent spouse relief to the wives of noncompliant offshore tax evaders creates an unjust outcome. Without the assurance of innocent spouse relief, these women are left vulnerable to civil and criminal liability. Often wives in omitted income cases are denied innocent spouse relief because of a mismatch in terms of the “knowledge” requirement as applied to husbands versus wives. Willfulness on the part of the husband requires knowledge of the tax reporting obligations. However, “knowledge” that income was received, even where the source of such funds is unknown, disqualifies wives from innocent spouse relief. To solve this problem, an approach that takes into consideration the nature of domestic abuse, including financial abuse, is necessary. Domestic abuse is likely present in the divorce proceedings at issue since the high-net-worth tax evaders are typically the primary earners, and their hiding of assets is evidence of financial control. Revised Treasury Regulations must provide guidance in terms of what constitutes abuse and confirm that financial control is indeed circumstantial evidence of abuse.

The majority of the wives described in Part II necessarily had undergone financial abuse as evidenced by their need to hire forensic accountants and to file motions to compel in the divorce proceedings. This Article contends that financial abuse should serve as an appropriate ground for granting wives innocent spouse relief in the context of high-net-worth divorces involving noncompliant spouses. The presence of financial abuse in this context demonstrates that the wives did not have “knowledge” of the hidden offshore funds.

Ensuring that the wives of high-net-worth tax evaders are granted innocent spouse relief will empower their reporting of offshore tax fraud and evasion. This will lead to the uncovering of vast networks of offshore evasion as the partners and business associates of the high-net-worth tax evaders are disclosed as well. Empowering wives of offshore tax evaders to whistle blow on their husbands’ misdeeds will lead to greater offshore tax enforcement and shorten divorce proceedings. The empowerment of these women will also result in an important step forward in how the United States perceives and treats victims of abuse.
Mixed reality and augmented reality (AR) are the way of the future. By 2020, the mixed and augmented reality industry is expected to be valued at $162 billion.¹ With the rise of wearable devices with AR capabilities² and the...
inclusion of AR features in new software such as iOS 12, mixed reality and augmented reality are sure to become more mainstream in American life. Patrons can enter into real-world venues and put on a pair of glasses that supplement their experiences by providing digital data and virtual displays of information. Applications such as Pokémon Go have brought AR to the mainstream and spurred the development of thousands of new applications. Additionally, most new smartphones and wearable devices have the ability to superimpose intellectual property, such as trademarked logos and identifiers, over real-world property on the device’s screen.

The advanced technology behind AR places it in a unique position to have unforeseen effects on three distinct areas of the law: traditional property law, trademark law, and copyright law. As such, various questions are being raised about the viability of the current laws within each field. First, are developers
responsible for real-world property damages that occur when players use their AR applications, or are developers insulated from liability through First Amendment or other protections? Second, are AR applications that use visual trademarks to trigger the display of other, competing trademarks protected under the fair use doctrine or parody protections, or are they not protectable under the current Lanham Act at all? Finally, does copyright law adequately protect hybrid works created by AR where new intellectual property is overlaid on top of existing copyrighted works?

Intended to serve as a lawmaker’s guide for protection of property rights, this Note will identify the most significant issue for each of these three areas of the law and suggest a framework for a modest legislative proposal in each Part designed to prevent the laws from becoming outdated within the next ten years. In Part II, this Note provides background information about mixed and augmented reality technologies, detailing the technology itself and issues that are certain to arise as AR advances further and further beyond what the current legal framework originally contemplated. In Part III, this Note examines real-world property laws and advocates for Congressional action to create a catchall real and intellectual property law (Virtual Invasion of Physical Land) that includes an opt-in and opt-out provision for landowners. After proposing a
solution for real property disputes, this Note transitions to the protection of intellectual property. In Part IV, this Note examines trademark law and advocates for revision of the Lanham Act to prevent AR applications from using visual trademarks to mislead or misdirect consumers. Finally, Part V examines copyright law and advocates for adopting an amendment to the Copyright Act to incorporate AR technologies and define the limits of derivative works and fair use. Part VI of this Note offers a brief conclusion.

II. THE RAPID RISE OF AN AUGMENTED AND MIXED REALITY WORLD

Augmented reality, sometimes referred to as “mixed reality,” involves the mixing of “virtual” and “actual” reality using specially designed software. AR has been around in some form since 1968. Harvard computer scientist Ivan Sutherland created the first AR device, a head-mounted display system that superimposed virtual information on the physical environment. Early AR devices were used primarily for aviation and military purposes; however, for the ordinary consumer AR is a relatively new phenomenon. The first commercially available AR application appeared in 2008, allowing for users to view a car in a magazine ad as a 3D model on their computer. Today, AR applications are becoming more and more commonplace. For example, Snapchat recently released a desktop app, Lens Studio, that allows any user to create AR graphics for usage in the Snapchat mobile app. Additionally, Apple and Google recently released ARkit2 and ARCore, respectively, allowing...
developers to add AR experiences to their applications, while iOS 12 brings AR features to Apple devices worldwide.

In fundamental terms, AR takes the real-world environment and “augments” or adds to it with extra layers of digital information. Typically, AR applications use one of three methods for the superimposition of images on top of the physical world. Simultaneous Localization and Mapping (SLAM) allows for devices to map the real world around them using sensors and various algorithms. The combination allows the device to render virtual images on a handheld device’s screen over real-world objects. Recognition-based AR uses a camera to identify visual markers or objects, which triggers the application to display a particular image. The visual object displayed on the screen moves as the user rotates the camera. Lastly, location-based AR relies on GPS, compass, velocity, and accelerometer data about a user’s location or movements to display a particular object on the screen on top of the real-world landscape when a particular location is reached. Location-based AR is used by the popular application Pokémon Go.

On November 16th, 2016, the Senate Committee on Commerce, Science, and Transportation held a hearing titled “Exploring Augmented Reality.” At the hearing, those in the mixed-reality space spoke about the implications of this technology.

---

21 Both of these desktop applications allow the developer to include AR elements in any application for Android or iOS. Apple Unveils ARKit 2, Apple (June 4, 2018), https://www.apple.com/newsroom/2018/06/apple-unveils-arkit-2/; AR Core Overview, Google (Aug. 12, 2018), https://developers.google.com/ar/discover/.

22 Etienne, supra note 3 (“Augmented reality, ARKit 2, sharing, and Shortcuts are some of the breakout features of iOS 12.”).


27 Id.

28 Id.

29 Id.


rapidly advancing field.\textsuperscript{32} Brian Blau, Research Vice President at Gartner, said that he believed hundreds of millions of AR devices would be in the hands of consumers within the next five years.\textsuperscript{33} Additionally, others, such as John Hanke, CEO of Niantic,\textsuperscript{34} spoke about the need for regulations that do not stifle innovation in the AR space.\textsuperscript{35}

While the technology has become increasingly popular over the past five years and shows no signs of slowing, this rapid rise also converges with a space that has relatively little regulation and did not exist when the current body of law was drafted.\textsuperscript{36} Thus, the current body of regulation is generally judge-made law,\textsuperscript{37} which is volatile and not sustainable in the current rapid technology boom. Legislators have recognized this fact as well.\textsuperscript{38} In May 2017, House members formed a “reality caucus” to consider issues related to virtual, augmented, and mixed realities.\textsuperscript{39}

Evidenced by the rapid increase and advancement of commercially available AR applications since 2008, these technologies are only on the cusp of their full potential.\textsuperscript{40} However, almost all existing property, trademark, and copyright laws were enacted before augmented and mixed reality technologies were thought to be feasible for everyday consumer usage. Keeping this in mind, the remaining Parts of this Note take an in-depth look into the legal issues that are likely to arise as these technologies become more advanced and commonplace.

\section*{III. AUGMENTED REALITY AND REAL PROPERTY RIGHTS}

AR applications are raising property disputes due to the uncharted legal area where the bounds of real and intellectual property meet. While there have been over thirteen million ARKit-created application downloads since the release of iOS11 in 2017,\textsuperscript{41} this Part will frequently refer to Pokémon Go as the primary example, as it has gained the most prominence, and consequentially, the most

\textsuperscript{32} Id.
\textsuperscript{33} Id. ("We forecast that in 5 to 10 years there will be hundreds of millions of HMD devices in the hands of users; split between see-through transparent display devices and those that provide full immersion, such as VR. There are many technology vendors competing for this opportunity, Microsoft, Google, ODG, Epson, DAQRI and many others.").
\textsuperscript{34} Niantic created the application Pokémon Go. Id.
\textsuperscript{35} Id.
\textsuperscript{36} Yavorsky & Culp, supra note 8.
\textsuperscript{37} Farifield, supra note 4, at 59.
\textsuperscript{38} Yavorsky & Culp, supra note 8.
\textsuperscript{39} Id.
\textsuperscript{40} Sarah Perez, ARKit-Only Apps Top 13 Million Installs, Nearly Half from Games, TECHCRUNCH (Mar. 2018), https://techcrunch.com/2018/03/28/arkit-only-apps-top-13-million-installs-nearly-half-are-games/ [https://perma.cc/HNZ4-AHJZ].
\textsuperscript{41} Id.
Pokémon Go and other related AR applications use location-based services that require players to travel to different predetermined real-world locations in order to collect virtual items that contribute to gameplay. For example, in Pokémon Go, the “trainers” or players travel to different real-world locations, the “Pokéstops,” in order to collect virtual Pokémon. Niantic, the developer of the game, sets the geographic coordinates of the “Pokéstops” near or on real-world property.

While many business owners have enjoyed economic benefits from the applications, the game’s requirement that players travel to real-world locations has also raised legal issues. For example, gamers have been found trespassing on private property, have been accused of damaging public and private property, have engaged in assault and battery of other players, and have cost cities large sums of money in order to protect public parks and provide extra law enforcement personnel.

A. Attempts to Regulate Augmented Reality Applications

In response to the real-world damage caused by the AR application’s players, some cities have attempted to implement local ordinances to deal with...
the negative effects. For example in *Candy Lab v. Milwaukee Cty.*, the developer of an AR application called “Texas Rope ‘Em” challenged a Milwaukee County ordinance which required the developers of any AR application to obtain a permit before operating in Milwaukee. The ordinance was in response to the negative effects of the Pokémon Go application, such as: inadequate bathrooms for park-goers, unauthorized vendors in the park, parking violations, and significantly increased traffic congestion. One member of the Board that passed the ordinance claimed that the County was forced to foot the bill for “tens of thousands” of dollars to keep up with the additional park traffic because of the app.

However, even with the increased costs to the county, the court in *Candy Lab* found that the First Amendment considerations outweighed the need for the ordinance. The *Candy Lab* court determined that AR applications are entitled to the same First Amendment protections as regular video games. The location-based nature of these applications, the court concluded, does not change the fact that the content itself cannot be regulated. Engaging in a First Amendment analysis, the court further stated that the ordinance requiring permits was an invalid restriction on speech because it treated AR applications as a separate category, distinguishing the games by their mode or channel of speech rather than their content.

In addition to the public park at issue in *Candy Lab*, private homeowners in numerous states filed a class action lawsuit against Niantic, accusing the

---


52 Candy Lab Inc. v. Milwaukee Cty., 266 F. Supp. 3d 1139, 1141 (E.D. Wis. 2017).

53 The ordinance read in pertinent part as follows:

> Virtual and location-based augmented reality games are not permitted in Milwaukee County Parks except in those areas designated with a permit for such use by the Director of the Department of Parks, Recreation, and Culture [ (the “DPRC”) ]. Permits shall be required before any company may introduce a location-based augmented reality game into the Parks, effective January 1, 2017.

*Id.* at 1143.

54 *Id.* at 1142–43.

55 *Id.* at 1143.

56 *Id.* at 1151–52.

57 *Id.* at 1146–47 (“The Supreme Court has instructed that video games, like other forms of expression, are entitled to First Amendment protection. Brown v. Entm’t Merchs. Ass’n, 564 U.S. 786, 790, 131 S.Ct. 2729, 180 L.Ed.2d 708 (2011). . . . Accordingly, the Court concludes that Texas Rope ‘Em qualifies for First Amendment protection and that the County’s motion to dismiss on that ground must be denied.”).


59 *Id.*
In a complaint filed in the Northern District of California, the plaintiff alleged that the defendant (Niantic) had designated Pokéstops and Pokémon Gyms on or directly adjacent to private property without the consent of the property owners. The homeowners further alleged that the players had been congregating in front of their property. As such, the homeowners brought claims of unjust enrichment and nuisance. Recently, it was announced that the two parties had reached a settlement. Part of the settlement agreement required Niantic to set up a web portal that would allow homeowners to complain about virtual Pokéstops and Gyms being too close to their property. While this solution certainly helps homeowners affected by Pokémon Go, it is little help when these issues arise in relation to similar location based applications.

The underlying question in these cases is whose rights dominate when someone’s intellectual property is overlaid on top of real-world property. Can a real-world owner or municipality force a developer, such as Niantic, to remove its intellectual property from a geographic location under the existing common law trespass or nuisance laws? Can developers, such as Niantic, be held liable for “virtual trespassing” under current common law? Examining these issues under current property and tort law principles demonstrates the need for an

---


61 Id. at ¶ 5, Marder v. Niantic, 4:16-cv-04300-KAW (N.D. CA 2016).

62 Id. at ¶ 6.

63 Id. at 13–14.


65 Id.

66 While the Candy Labs court was concerned with a public park, the underlying nuisance question remains for private landowners as well. For example, if Niantic places a virtual Pokémon outside of someone’s home, the players often congregate in front of the homeowner’s property on the street, which is still technically public land. Additionally, the underlying dispute in all of these cases will be whether placing intellectual property within the bounds of another’s GPS coordinates can be subject to liability.

updated catchall provision that will handle trespass, nuisance, and other claims caused by virtual property being overlaid on real-world property.68

**B. Inadequacy of Current Property Laws**

An individual can be held liable for trespass on private property if that individual intentionally enters land in possession of another, *causes a third person to do so*, remains on the land, or fails to remove from the land a thing which he or she is under a duty to remove.69 Examining the comments and illustrations to the Restatement, however, there is no mention of anything but “physical objects.”70 Additionally, the Supreme Court has hinted that for trespass to stand, a “physical-world invasion is required.”71 Real-world property owners could argue that AR application developers cause entry of a third person onto the land.72 The actor is liable for trespass if he or she has commanded or requested a third person to enter land in the possession of another; the actor is responsible for the third person’s entry if it is a trespass.73 However, developers, such as Niantic, include provisions in their standard form agreement, exculpating them from liability for these particular instances.74 In this instance,

68 The above examples demonstrate how different AR is from what has been previously contemplated by property laws. Developers of an AR application have the ability to place their intellectual property on thousands of owned properties at one time in different states across the country. See Fairfield, supra note 4, at 56–57.

69 *Restatement (Second) of Torts* § 158 (AM. LAW INST. 1965) (“One is subject to liability to another for trespass, irrespective of whether he thereby causes harm to any legally protected interest of the other, if he intentionally (a) enters land in the possession of the other, or causes a thing or a third person to do so, or (b) remains on the land, or (c) fails to remove from the land a thing which he is under a duty to remove.”).

70 Id.

71 United States v. Alabi, 943 F. Supp. 2d 1201, 1264 (D. N.M. 2013) (“The Supreme Court has not explicitly defined “physically intruding” as requiring an entity to invade a space in the physical—as opposed to virtual—world, but *United States v. Jones* and *Florida v. Jardines* hint that such a physical-world invasion is required.”).

72 A plaintiff could reasonably argue that the virtual placement of game pieces, such as Pokémon, on the plaintiff’s property is causing the players to enter the property because retrieval of those game pieces is required to advance in the game.

73 *Restatement (Second) of Torts* § 158 cmt. j (AM. LAW INST. 1965) (“If, by any act of his, the actor intentionally causes a third person to enter land, he is as fully liable as though he himself enters. Thus, if the actor has commanded or requested a third person to enter land in the possession of another, the actor is responsible for the third person’s entry if it be a trespass. This is an application of the general principle that one who intentionally causes another to do an act is under the same liability as though he himself does the act in question.”).

74 The Niantic terms of service read, in pertinent part:

You agree that in conjunction with your use of the Services, you will maintain safe and appropriate contact with other players and other people in the real world. You will not harass threaten or otherwise violate the legal rights of others. You will not trespass, or in any manner attempt to gain or gain access to any property or location where you do
the players would presumably remain responsible for the trespass, even if they were being led to private property by the game itself.

An alternative to trespassing under common law, as alleged by private homeowners in their complaint,75 could be nuisance. This appears to be the best route for claims that involve public lands. Under the Second Restatement of Torts, a private nuisance is defined as “a nontrespassory invasion of another’s interest in the private use and enjoyment of land[.]”76 and a public nuisance is an unreasonable interference with a right common to the general public.77 Plaintiffs could argue that application developers, such as Niantic, are creating either public or private nuisances by causing third parties to congregate near or around their private property and thus diminishing their use or enjoyment of the land. However, again, Niantic could likely defeat a nuisance claim by passing liability on to the player in the terms of agreement. Being forced to pursue claims against each individual player leaves real-world property owners with little recourse for violation of their property rights.

Finally, as some have suggested,78 negligence may be another route to hold developers, such as Niantic, liable under the current body of common law due to their licensing provisions presumably exculpating them from intentional torts. Plaintiffs could presumably allege that Niantic’s design of the application, which forces the players to travel to their pre-determined locations,79 causes unreasonable risk of damage of property. Plaintiffs could argue that Niantic should have been aware of the potential ramifications of dispatching thousands

not have a right or permission to be, and will not otherwise engage in any activity that may result in injury, death, property damage, nuisance, or liability of any kind. If you have a dispute with any third party relating to your use of Services, you release Niantic (and our officers, directors, agents, subsidiaries, joint ventures, and employees) from all claims, demands, and damages (actual and consequential) of every kind and nature, known and unknown, suspected and unsuspected, disclosed and undisclosed, arising out of or in any way connected with such disputes.


75 See supra notes 61–63 and accompanying text.

76 Restatement (Second) of Torts § 821D (Am. Law Inst. 1965).

77 Restatement (Second) of Torts § 821B (Am. Law Inst. 1965) (“(1) A public nuisance is an unreasonable interference with a right common to the general public. (2) Circumstances that may sustain a holding that an interference with a public right is unreasonable include the following: (a) Whether the conduct involves a significant interference with the public health, the public safety, the public peace, the public comfort or the public convenience, or (b) whether the conduct is proscribed by a statute, ordinance or administrative regulation, or (c) whether the conduct is of a continuing nature or has produced a permanent or long-lasting effect, and, as the actor knows or has reason to know, has a significant effect upon the public right.”).


79 See Warner, supra note 30.
of individuals to different real-world property locations. Developers like
Niantic could be found to have unreasonably created a risk of damage to
property when it dispatched unknown players to private property. Analogizing
to real-world examples, it would be similar to if an individual threw large
amounts of valuable coins on a private farm and that farm owner then sued the
individual who retrieved the money and subsequently ruined her crops.

C. Proposed Framework for a Hybrid Property Statute

Examining these three potential routes under the existing common law
framework and operating under the presumption that other courts will choose to
treat AR applications similar to the Candy Lab court, there will need to be
other alternative routes for dealing with real-world effects of AR applications.
The question is how to regulate the applications in order to protect real-world
property rights while simultaneously encouraging intellectual property
development. Should developers like Niantic foot the bill for the real-world
property damage caused by their intellectual property or should their intellectual
property remain protected under the First Amendment as free speech, holding
the individual players liable for the property damages?

The current common law legal framework proves inadequate to answer
these questions, primarily because of the inconsistencies in the application of
judge-made common law and the new hybrid property rights that are emerging
with the creation of these applications, which are not contemplated by
contemporary tort laws. Tensions between intellectual property and real-world
property owners will need a resolution within the next four to five years as AR
applications become more popular. Indeed, lawsuits have already been filed.
Continuing on the current common law regulation course would only produce
an inconsistent body of law in an area rapidly expanding.

Treating AR applications as pure free speech fails to consider the fact that
the placement of intellectual property on top of real-world geographic locations
is creating a conflict of competing property rights between owners where the
intellectual property owners hold all of the bargaining chips. Courts err in
treating AR applications similar to regular video games because AR produces
an array of issues not seen in traditional video games. As a result, real-world

80 See supra notes 60–62 and accompanying text.
81 See RESTATEMENT (SECOND) OF TORTS § 282 (AM. LAW INST. 1965).
82 See supra notes 51–59 and accompanying text.
83 There are very few cases that have dealt with these issues, as this is an emerging area
of the law. As such, it is unclear how judges will apply contemporary property laws when
they intersect with intellectual property laws.
84 See supra notes 30–33 and accompanying text.
85 See supra notes 60–63 and accompanying text.
86 For example, unlike traditional video games, AR overlays the digital content onto
geographic coordinates owned by those who do not choose to participate in the game. Know
the Augmented Reality Technology: How Does AR Work?, NEW GEN APPS (Nov. 23, 2017),
Property owners are experiencing uncontrollable damage to their land with no recourse, a stark contrast to the protections afforded under traditional property laws. However, making AR applications secondary to real-world property rights as attempted in *Candy Lab* will only lead to a halting of innovation, imposition on free speech rights, and a potential collapse of the AR application development. Thus, there must be a solution that operates within the existing framework of property laws, allowing for owners of property to have recourse against developers who are responsible for trespass onto their land.

Congress should consider issues such as virtual trespassing and real and intellectual property hybrid ownership. Any law must also be flexible and allow the real-world property owner to opt in to inclusion. The first step in this process would be to update laws with consideration given to the potential of non-physical invasions. As seen above, AR applications frequently result in the placement of intellectual property within the physical bounds of owned real property. In order to deal with this, Congress could pass legislation defining a new statutory law that others have described as “Virtual Trespass.”

https://www.newgenapps.com/blog/augmented-reality-technology-how-ar-works. In contrast, the traditional “video games” that were considered by the Supreme Court and subsequently afforded First Amendment protections involved no question of invasion of privacy or property rights. See Brown v. Entertainment Ass’n, 564 U.S 786, 794 (2011). The games were considered only from the freedom of expression and content lens. See id. (holding that the California statute that created a wholly new category of content-based regulation directed at children was barred by First Amendment protections).

87 See supra notes 45–49 and accompanying text.
88 See, e.g., *Restatement (Second) of Torts* § 158, 821D (AM. LAW INST. 1965) (providing clear statutory recourse for physical invasions onto an individual’s land).
89 See *Exploring Augmented Reality*, supra note 31 (discussing the implications of restrictive laws that may limit the ability of those in the AR field to innovate).
90 See *Candy Lab Inc. v. Milwaukee Cty.*, 266 F. Supp. 3d 1139, 1149–53 (E.D. Wis. 2017) (discussing free speech protections).
91 While others have proposed the creation of a do-not-locate registry, this solution fails to provide a realistic remedy to the landowners by itself. See William T. McClure, *When the Virtual and Real Worlds Collide: Beginning to Address the Clash Between Real Property Rights and Augmented Reality Location-Based Technologies Through a Federal Do-Not-Locate Registry*, 103 IOWA L. REV. 331, 358–64 (2017). But see Helaine Olen, *Congratulations! You Lost.*, SLATE (May 24, 2016), http://www.slate.com/articles/business/the_bills/2016/05/robo_calls_have_transcended_over_the_do_not_call_list_whose_fault_is_it.html [https://perma.cc/CR5N-FPHX] (discussing the failures of the do-not-call registry). For example, the do-not-call registry created by the FTC has been rendered largely ineffective. As such, any proposed solution must carefully balance the property rights of real-world and intellectual property owners. See McClure, supra, at 358–64. A do-not-locate registry would be more effective with a clear statutory remedy behind it. See Olen, supra.
92 See supra notes 40–45 and accompanying text. Additionally, AR applications can place intellectual property within the physical bounds of private real property in thousands of locations across all fifty states at one time. See generally Warner, supra note 30.
93 See Murphy, supra note 67; Yonah Reback, *Virtual Trespass: Not in My Backyard*, WASH. J. LAW, TECH., & ARTS BLOG (May 12, 2017), https://wjlta.com/2017/05/12/virtual-
Recognizing a new statutory provision would be relatively easy utilizing the existing framework under the Restatement of Torts. The trespass and nuisance framework could be utilized to create a statutory provision that codifies entries beyond those that are purely physical. For example, the proposed law could read:

*Virtual Invasion of Physical Land: One is subject to liability under this statute, irrespective of whether he or she thereby causes harm to any legally protected interest of the other, if he or she intentionally and without consent (a) enters land in the possession of the other, or causes a thing or a third person to do so due to the placement of virtual intellectual property within 25 feet of the geographic coordinates (“GPS coordinates”) of the real physical land and (b) fails to remove his virtual intellectual property from within 25 feet of the real world geographic coordinates of the land after notice from the owner of the land.*

The hypothetical statute includes an opt-in or opt-out provision for real-world owners. Benefactors of Pokémon Go applications could continue to allow applications to use their real-world locations to their benefits. For example, McDonald’s could provide consent to Niantic allowing the placement of trespass-not-in-my-backyard/ [https://perma.cc/TLF6-M5PZ]; *Virtual Trespassing: How ‘Pokémon Go’ Shakes up the Law*, WALL ST. J. (Apr. 5, 2017), http://www.wsj.com/podcasts/virtual-trespassing-how-pokemon-go-shakes-up-the-law/992F55C4-18FC-45A2-B38A-D97EA438E56.html [https://perma.cc/2ZBK-687P].

See generally *RESTATEMENT (SECOND) OF TORTS* (AM. LAW INST. 1965).

While states could in theory deal with this issue on their own, the ability for one AR developer to intrude on thousands of landowners’ property at one time makes a federal level solution more desirable.

The proposed text here is intended to serve as a framework for any legislative proposals. While a fully drafted statute would need much more detail, the underlying issues that would need to be fixed are addressed here: allowing property owners to retain control of their real property while also allowing AR developers to utilize the real-world landscape. The statute here differs from other proposed solutions in that it provides a statutory remedy for landowners in addition to providing an opt-in and opt-out provision.

The opt-in and opt-out provision would likely need to be implemented and maintained by an administrative agency, such as the FCC or FTC, via a national database. Such implementation steps are beyond the purview of this Note. Others have contemplated how such a database would work. See McClure, *supra* note 91, at 358–64. Presumably, the database could be set up online and be relatively easy to maintain. The opt-in and opt-out ability would be analogous to the web portal solution used in the Niantic settlement. See *supra* notes 64–65. However, the opt-in and opt-out ability would apply to more than just one AR-based application, as requiring landowners to use a separate web portal for each AR application would not be an effective solution. This would give notice to all AR developers of when they are not allowed to place their intellectual property within certain geographic coordinates. However, the creation of a do-not-locate registry on its own would be ineffective without a defined statutory remedy for landowners. The FTC do-not-call registry receives millions of complaints every year with limited benefits for consumers. See Olen, *supra* note 91.
of virtual Pokéstops within their restaurants. In return, Niantic would place
digital Pokémon on the real-world property to bring in customers for economic
benefit. However, homeowners who have experienced nothing but detrimental
effects from AR applications could opt out of use of their geographic
coordinates, placing an effective “no trespassing” sign on the geographic
coordinates of their property. This would give developers like Niantic notice
that they should not place intellectual property near the land of property owners
who opt out of the use of their geographic coordinates. It would also provide a
clear statutory framework for holding developers like Niantic accountable for
placement of intellectual property within the bounds of real property.

Thus, this solution would allow individuals to pursue claims against the
developers of an application rather than each individual user.98 The proposed
text simply places intellectual and real property on an even playing field.
Intellectual property owners could no longer take advantage of private
landowners’ property rights without their consent to do so. As historically seen
in property laws, the opt-in and opt-out provisions function the same way as
physical entry typically has.99 Landholders have traditionally maintained an
absolute right to control who comes in and out of their property, and the virtual
trespassing law aligns these basic principles with modern day technological
advances.100

For example, a real property owner would never be forced to allow a person
onto their property to collect a physical game piece placed there by the creator
of the game. However, if the maker of the game had first obtained their consent
to do so, traditional property laws would allow this use of the land.101 Therefore,
creation of a new form of invasion onto land, “virtual invasion,” would provide
a catchall solution for when real and intellectual property rights conflict.
Further, the proposed law would not harm innovation within the AR space
because commercial property owners could still allow the placement of the
intellectual property onto their land in exchange for the increased foot traffic
that applications, such as Pokémon Go, could bring.102 Finally, the proposed

98 With an established database providing notice to developers, property owners could
more easily pursue claims against these developers who still placed intellectual property on
the property owners’ real-world property. This would be a much more realistic route for
relief as opposed to being forced to pursue each player for claims of trespass or nuisance, for
example.
99 John Alan Cohan, Private and Public Necessity and the Violation of Property Rights,
83 N.D. L. Rev. 651, 658 (2007) (discussing status as a guest); RESTATEMENT (SECOND) OF
TORTS § 158 (AM. LAW INST. 1965) (trespass section).
100 RESTATEMENT (SECOND) OF TORTS § 158 cmt. c, e (AM. LAW INST. 1965).
101 RESTATEMENT (SECOND) OF TORTS § 158 cmt. e (AM. LAW INST. 1965) (“Conduct
which would otherwise constitute a trespass is not a trespass if it is privileged. Such a
privilege may be derived from the consent of the possessor . . . .”).
102 Sheeraz Raza, How Pokémon Go Influenced the Stock Market & Economy,
VALUEWALK (Sept. 19, 2016), http://www.valuewalk.com/2016/09/pokemon-go-
influenced-stock-market-economy-infographic/ [https://perma.cc/7QFK-FJGF] (discussing
the economic benefit to McDonald’s from advertising Pokémon Go).
statutory text would avoid First Amendment issues seen in Candy Lab altogether by regulating the geographic coordinates of where all intellectual property can be placed, rather than dealing with any restrictions on the content itself.

IV. AUGMENTED REALITY AND TRADEMARK INFRINGEMENT

In addition to physical world effects and property disputes, AR applications also present potential issues for areas of intellectual property, such as trademark law. To illustrate AR’s potential, imagine a scenario where a brand’s trademark triggers the display of other related products in an AR application. For example, a consumer enters a store wearing a pair of Google Glass and gazes upon the aisles, finding something that she wants to purchase. Instead of pulling out her smartphone and searching for reviews of the specific product, the trademarked logo on product X triggers her glasses to display five related brands on the screen, one with better online reviews, with an immediate option to purchase. Instead of purchasing product X in store, the consumer purchases product Y directly from Amazon and walks out of the store empty-handed. In this scenario, (1) the retailer has lost a sale and (2) product X lost out to product Y. Was the use of product X’s trademark to trigger the display of other related brands trademark infringement under the Lanham Act?

In a similar scenario, imagine an AR application that displays a constant stream of information on an individual’s Google Glass or car windshield as they drive down the street. When the software recognizes a Panera Bread trademark, the application displays related restaurants within a five-mile radius on the dashboard, one of which is a direct competitor of Panera—Potbelly Sandwiches. Seeing that Potbelly is only two miles down the road, the individual decides to go there instead of Panera. Was the display of other,

---

103 In this example, the AR application would recognize a brand’s trademark via the device’s camera and then display other related products based on that recognized trademark. There is also the possibility that another brand’s trademark could be superimposed on top of the real-world trademark within the device’s screen.

104 See Fairfield, supra note 4, at 56–57 and accompanying text. Google Glass is only an example here. There has been recent speculation that Apple may also release a pair of glasses that can overlay information over real world objects through the lens. See Gerald Lynch, Apple AR Glasses Release Date, News, and Rumors, TECHRADAR (Aug. 30, 2018), https://www.techradar.com/news/apple-ar-glasses-release-date-news-and-rumors [https://perma.cc/AZ86-ZWGL].

105 In this hypothetical, the consumer could have purchased product Y because it had better reviews, or alternatively, she thought (i.e., was confused) that it was a product by the same company and would rather just have it shipped to her house from Amazon instead of buying it in store.

106 AR displays within car windshields are a huge potential growth market for AR. These types of technologies have been contemplated within the past couple of years. See Darrell Etherington, WayRay’s AR In-Car HUD Convinced Me HUDs Can Be Better, TECHCRUNCH (2017), https://techcrunch.com/2018/01/09/wayrays-ar-in-car-hud-convinced-me-huds-can-be-better/ [https://perma.cc/7CJF-JEFX].
similar restaurants upon seeing Panera’s trademark infringement under the Lanham Act or was it equivalent to using the geographic coordinates of other restaurants to display the consumer’s options, similar to Google Maps?

A. Actionable Use and the Rescuecom Decision

The question in the above scenarios is whether the Lanham Act is sufficient to protect against an AR application’s use of a brand’s trademark to display competing trademarks.107 Under the Lanham Act, trademark infringement can occur in two primary ways: likelihood of confusion and dilution.108 There are other possible routes of infringement, such as initial interest confusion.109 However, utilizing the traditional likelihood of confusion test for trademark infringement may prove problematic for the hypothetical scenarios due to the requirement that a mark be used in connection with the sale of goods or services before any infringement can occur, otherwise known as the actionable use requirement.110

Under Sections 32 and 43 of the Lanham Act, infringement occurs when any person uses in commerce any registered mark in connection with the sale, offering for sale, distribution, or advertising of any goods or services on or in connection with which is likely to cause confusion.111 Each circuit court uses a

---

107 In these scenarios, AR applications are using the trademarks within the software itself. The software recognizes the trademark via the camera and then displays the related or competing results on the screen. See generally Brian Wassom, Copyright in an Augmented Reality, WASSOM.COM (Aug. 3, 2012), http://www.wassom.com/copyright-in-an-augmented-reality.html [https://perma.cc/4XCS-3MTJ].


109 See Gibson Guitar Corp. v. Paul Reed Smith Guitars, LP, 423 F.3d 539, 549 (6th Cir. 2005), cert. denied, 547 U.S. 1179 (2006) (“Initial-interest confusion takes place when a manufacturer improperly uses a trademark to create initial customer interest in a product, even if the customer realizes, prior to purchase, that the product was not actually manufactured by the trademark-holder.”).

110 DINWOODIE & JANIS, supra note 108, at 493.


(1) Any person who shall, without the consent of the registrant--
(a) use in commerce any reproduction, counterfeit, copy, or colorable imitation of a registered mark in connection with the sale, offering for sale, distribution, or advertising of any goods or services on or in connection with which such use is likely to cause confusion, or to cause mistake, or to deceive; or (b) reproduce, counterfeit, copy, or colorably imitate a registered mark and apply such reproduction, counterfeit, copy, or colorable imitation to labels, signs, prints, packages, wrappers, receptacles or advertisements intended to be used in commerce upon or in connection with the sale, offering for sale, distribution, or advertising of goods or services on or in connection with which such use is likely to cause confusion, or to cause mistake, or to deceive, shall be liable in a civil action by the registrant for the remedies hereinafter provided.
The separate “likelihood of confusion” test that examines different factors, such as similarity of the marks, sophistication of consumers, strength of the mark, and channels of commerce. Before the factor analysis is applied, however, the court must find that the defendant has met the “actionable use” requirement, at least in some circuits.

Each of the hypothetical scenarios involves AR applications that utilize trademarked logos to provide the user with related products or places that they want to visit. Essentially, the hypotheticals both illustrate the use of a brand trademark image as a “keyword” in order to trigger the display of other brands’ trademarks. Usage of trademarks as keywords, albeit in the text form, has proved problematic for the courts before. In Rescuecom Corp. v. Google, the Second Circuit found that Google’s program AdWords, which allowed for a

15 U.S.C. § 1114 (2012) (emphasis added). Therefore, under the plain text of the Act, presumably, a retailer could possibly be held liable for the use of another company’s trademark, but only if it caused consumer confusion or was used in connection with the sale of goods or services. Id.

112 The similarity of the marks factor is used in all the circuit tests and examines the degree of similarity between the two marks from a consumer perspective. DINWOODIE & JANIS, supra note 108, at 521–23. Courts often examine the sight, sound, and meaning of the work from the viewpoint of how the marks are seen by the consumer when the products are purchased. Id.; see also Virgin Enters., Ltd. v. Nawab, 335 F.3d 141, 149 (2d Cir. 2003) (discussing the similarity of the marks factor).

113 The sophistication of the consumers takes the level of consumer knowledge into account. For example, highly trained professionals know the market and are less likely to be misled or consumed by the similarity of the marks than someone purchasing a quick and cheap item, such as gum. See Virgin Enters., 335 F.3d at 151.

114 The strength of the mark examines both inherent and acquired distinctiveness. For example, the Virgin court found that the Virgin mark was stronger because of its inherent distinctiveness (arbitrary and distinctive), and it also had acquired distinctiveness because of its famous name recognition. Id. at 147–48. The stronger the mark, the greater the likelihood that the public will assume the second use comes from the same source as the first. Id.

115 The channels of commerce factor examines how the products are sold. For example, it would be easier to find likelihood of confusion if the two products are both sold at small electronics stores. Id. at 150.

116 The actionable use requirement examines whether the defendant has used a particular mark in connection with the sale of goods or services. See DINWOODIE & JANIS, supra note 108, at 510–14. Actionable use is a prerequisite intended to limit infringement causes of action. Id.; infra note 127.

117 The Adwords program by Google worked by displaying the advertiser’s ad when a term that they had purchased appeared. Rescuecom Corp. v. Google Inc., 562 F.3d 123, 126 (2d Cir. 2009) (“For example, using Google’s Adwords, Company Y, a company engaged in the business of furnace repair, can cause Google to display its advertisement and link whenever a user of Google launches a search based on the search term, ‘furnace repair.’ Company Y can also cause its ad and link to appear whenever a user searches for the term ‘Company X,’ a competitor of Company Y in the furnace repair business. Thus, whenever a searcher interested in purchasing furnace repair services from Company X launches a search of the term X (Company X’s trademark), an ad and link would appear on the searcher’s screen, inviting the searcher to the furnace repair services of X’s competitor, Company Y. And if the searcher clicked on Company Y’s link, Company Y’s website would open on the
company to purchase another company’s word-based trademark in order to gain more search appearances on Google, was a “use in commerce” under the Lanham Act.\textsuperscript{118} The court explained that the situation differed from traditional “product placement” because Google’s practices were not benign, in fact, consumer usage of one mark would intentionally direct them towards another mark, often resulting in business for the mark who paid for the placement.\textsuperscript{119} The court found that traditional product placement could result in infringement as well if it created consumer confusion and resulted in consumers purchasing an off-brand product when they meant to purchase a famous brand’s product.\textsuperscript{120}

While at first glance the AR hypothetics appear to fit directly within the holding in \textit{Rescuecom}, there are key differences, which may result in limited or no protection under the current Lanham Act. There are a number of courts and scholars that took issue with the line of reasoning used by the \textit{Rescuecom} court before it was decided.\textsuperscript{121} Primarily, the disagreement centered upon whether the triggering of Brand X’s trademark by a third-party app or even by Brand Y itself constitutes a “use in connection with the sale of goods or services” as required to advance to the infringement tests.\textsuperscript{122} For example, courts had frequently found, especially prior to the \textit{Rescuecom} holding, that keyword type purchases were not considered “actionable use.”\textsuperscript{123} These courts primarily relied upon the

\textsuperscript{118} \textit{Id.} at 127.

\textsuperscript{119} \textit{Id.} at 130–31. A hypothetical would be if Burger King bought advertising on Google and Google gave them the option to purchase the trademarked word “McDonald’s.” The result of this scenario would be that when a user searched for “McDonald’s” this would trigger the search engine to display results for Burger King in addition to results for McDonald’s. Thus, if that user ended up going to Burger King, then McDonald’s trademark would be providing Burger King with business and Google with ad revenue.

\textsuperscript{120} \textit{Id.}


\textsuperscript{123} See, \textit{e.g.}, \textit{S & L Vitamins, Inc., 521 F. Supp. 2d at 199–202; Merck, 425 F. Supp. 2d at 415.
reasoning used in a 2005 decision by the Second Circuit, *1-800 Contacts, Inc. v. WhenU.com.*124

In addition to the courts, scholars have been divided over whether to side with the reasoning found in *1-800 Contacts* or *Rescuecom.*125 Prior to the *Rescuecom* holding, authors Dinwoodie and Janis asserted that the balance of scholarly articles favored “a stringent actionable use requirement akin to that espoused in *1-800 Contacts.*”126 Additional scholars have advocated that defining use in a traditional sense under the Lanham Act would require courts to find that companies, such as Google, have not used the mark in commerce.127

While the *Rescuecom* reasoning is certainly still a volatile legal doctrine in terms of online advertising and metadata tags,128 application of the holding to non-verbal marks, such as those used by AR applications, creates an even more uncertain scenario. For example, the *Rescuecom* court’s analysis centered quite heavily on the fact that unlike in *1-800 Contacts*, Google was using the plaintiff’s trademark to trigger another brand’s trademark.129 In the same vein, the court relied upon the fact that Google was generating advertising revenue by recommending and selling the word “Rescuecom” to other companies in order to find that Google itself was using the mark “in commerce.”130 Examining the case in this light, it appears the reasoning could be somewhat limited to its facts. AR applications would not necessarily involve directly using a brand’s

---

124 *1-800 Contacts*, 414 F.3d at 407–09, 412 (finding that the defendant did not use, reproduce, or display the plaintiff’s mark at all to trigger the display of other competing marks, and therefore, no actionable use).

125 See supra notes 120, 121, 124 and accompanying text.

126 DINWOODIE & JANIS, supra note 108, at 511.

127 Barrett, *Finding*, supra note 121, at 977 (“The historical ‘trademark use’ prerequisite to infringement liability clearly remains in United States law today, and courts should construe and apply it in light of its original purpose and in light of modern circumstances and public policy concerns. While there may be other factors that courts might beneficially entertain, close, direct association, perceptibility, and ‘separate commercial impression’ are directly linked to the historical background and purpose of the trademark use doctrine and promote a range of public policy interests.”).


129 Rescuecom Corp. v. Google Inc., 562 F.3d 123, 128 (2d Cir. 2009) (“*1-800* suggested in dictum that is highly relevant to our case that had the defendant used the plaintiff’s trademark as the trigger to pop-up an advertisement, such conduct might, depending on other elements, have been actionable.”).

130 *Id.* at 126–27 (“Many of Rescuecom’s competitors advertise on the Internet. Through its Keyword Suggestion Tool, Google has recommended the Rescuecom trademark to Rescuecom’s competitors as a search term to be purchased. Rescuecom’s competitors, some responding to Google’s recommendation, have purchased Rescuecom’s trademark as a keyword in Google’s AdWords program, so that whenever a user launches a search for the term ‘Rescuecom,’ seeking to be connected to Rescuecom’s website, the competitors’ advertisement and link will appear on the searcher’s screen. This practice allegedly allows Rescuecom’s competitors to deceive and divert users searching for Rescuecom’s website.”).
trademark, but rather just recognizing it via preprogrammed or adaptive software.131

B. A Twenty-First Century Definition of “Actionable Use”

Current law is unclear what the outcome would be if a hypothetical like one proposed at the beginning of the Part was to make its way to one of the circuit courts and therefore, Congress should refresh the Lanham Act in order to consider the rapidly developing technology of AR. Scenarios like those proposed above are not that far off from being a reality;132 in fact, the technology for these scenarios is already being utilized in non-monetized situations133 and the technology exists to augment virtual advertisements on top of real-world advertisements or brand identifiers.134

Trademark law has not previously dealt with AR technologies. Within the past ten years, technology has grown at a rapid pace, requiring the laws to play catch-up.135 In addition to this historical aspect, Rescuecom and lack of clarity on the topic of actionable use as related to keyword advertising and metadata tags illustrates the need for a congressional refresh of the Lanham Act. This route would avoid each circuit handling the issue and creating a body of inconsistent laws governing AR and actionable use.136 This argument is bolstered when examining the broad differences between each circuit in their analyses and the general inconsistency when the factor analysis is applied.137 Thus, Congress should take preemptive action in order to preserve the integrity of the Lanham Act and preserve the value of trademarks in the virtual world.

131 The key difference here is that Google was actually selling the term “Rescuecom.” However, presumably applications could become so advanced that they recognize various trademarks by conducting real-time Internet searches triggered by their software, and then recommend related results based upon the results of that search. A company could pay an AR developer so that certain Internet searches produced certain results. This scenario does not fit in the text of the Lanham Act, and it does not appear to fit within the reasoning used by the Rescuecom court.

132 See supra notes 2–7 and accompanying text.

133 Id.

134 Id.


136 Some circuits, such as the Second Circuit, do not require “trademark use” to be liable for trademark infringement, while others, such as the Sixth and Eighth Circuits, do apply a “trademark use” requirement. PETER S. MENELL ET AL., INTELLECTUAL PROPERTY IN THE NEW TECHNOLOGICAL AGE: 2018, 984 (2018). The inconsistent application of the use requirement across the circuits bolsters the argument for a Lanham Act revision. Id.

137 See DINWOODIE & JANIS, supra note 108, at 521–23. For example, the factor analysis differs between each circuit, and circuits frequently assign different tests and analyses to deal with different factors. Id. (providing a chart that shows the different factors considered by each circuit court).
The result of Congress failing to update the Lanham Act would be costly, cumbersome, and confusing. If a court takes the more traditional 1-800 Contacts view on use in commerce, advocated by some scholars, then companies may not be able to protect their brand identifiers from usage in the internal processes of third-party applications or other companies’ applications. Big box retailers and automotive companies could use each trademark as a trigger for displaying competing trademarks under the guise of fair use. Alternatively, if the court fails to distinguish from the Rescuecom decision, AR application growth may be hurt because of the lack of innovation due to an amplified fear of trademark infringement, which is often costly litigation, especially for new startups. Thus, the solution must be one that prevents companies from using trademarks for monetary benefit, but still allows for informational or descriptive uses of the mark that are protected by fair use and do not result in misdirection or confusion of consumers.

Congress has previously updated the Lanham Act to periodically refresh what was meant by “use in commerce” under the Act. Additionally, circuit courts have recently asked Congress to update and clarify what in fact is meant by “use in commerce” under § 45 of the Lanham Act. Allowing for each

---

138 Under § 33(b)(4) of the Lanham Act, “the use of the name, term, or device charged to be an infringement is a use, otherwise than as a mark . . . of a term or device which is descriptive of and used fairly and in good faith only to describe the goods or services of such party, or their geographic origin . . . .” 15 U.S.C. § 1115 (2012). Presumably then, a company like Ford or Kroger could argue that their AR applications were merely describing the types of products and identifying them rather than causing any confusion to the consumer.


140 Trademark Law Revision Act of 1988, Pub. L. No. 100-667, 102 Stat. 3935 (effective Nov. 16, 1989) (codified at 15 U.S.C. § 1127 (2006)); see Summary: H.R 5372 – 100TH Congress (1987-1988), CONGRESS.GOV, https://www.congress.gov/bill/100th-congress/house-bill/5372 [https://perma.cc/46GQ-4254] (“Amends the Lanham Act to permit a person who has a bona fide intention to use a trademark in commerce to apply to register the trademark. (Current law provides only for registration of a trademark already in use in commerce.) Requires that such trademark actually be used in commerce before it becomes a registered trademark.”); see also Aycock Engineering, Inc. v. Airflite, Inc., 560 F.3d 1350, 1357 (Fed. Cir. 2009) (“Despite the seeming harmony and simplicity in the application of the use requirement to trademarks and service marks, opportunity exists for confusion in this area of the law . . . in 1988, Congress passed the Trademark Law Revision Act (“TLRA”). The TLRA altered the burden that applicants must meet before satisfying the use element by requiring an applicant to make a ‘bona fide use of [the] mark in the ordinary course of trade.’”).

141 See Rescuecom Corp v. Google., Inc., 562 F.3d 123, Appendix (2d Cir. 2009) (“We assumed in the body of the opinion, in accordance with the holding of 1-800, that the requirements of the second sentence of the definition of ‘use in commerce’ in § 1127 apply
circuit to handle this issue would be a mistake for a number of reasons. Continuing down the common law route for these highly complex issues provides inconsistent guidance to innovators in the AR field and results in expensive litigation for companies across the board. As seen in 1-800 Contacts and Rescuecom, trademark cases are often quite fact specific. Additionally, there are a number of scenarios beyond the hypotheticals here that may arise rapidly once the technology becomes more and more commonplace. Finally, AR application growth may be stunted if the makers of the applications are not clear on what constitutes an actionable use under the Lanham Act.

Thus, Congress should update the Lanham Act to consider new mediums and make it clear that usage of a registered trademark to trigger other trademarks for the purposes of sale of information or misdirection of consumers is a use in commerce and a violation of the Lanham Act. This would be an easy correction using the existing statutory definition and within the spirit of the Act itself.

For example, the amendment could read:

A person or entity that intentionally uses a registered or unregistered trademark’s image, text, being, or likeness externally or internally in software or programmed code to trigger the display of another brand’s trademark with intent to misdirect or mislead consumers from the original source of the trademark shall be found to have used the mark in commerce for the purposes of sections 32 and 43 of this Act.

This amendment to the Act would protect the brand’s trademark in the AR space and operate in the same way as the holding in Rescuecom did for online advertisements. Companies would fulfill the actionable use requirement if to infringing conduct and found that such use in commerce was adequately pleaded. It would be helpful for Congress to study and clear up this ambiguity.

---

142 See generally 1-800 Contacts, Inc., v. WhenU.Com, Inc., 414 F.3d 400 (2d Cir. 2005); Rescuecom, 562 F.3d 123.
143 See Krystil McDowall, A Critical Look at “Use” Under the Lanham Act, 4 N.Y.U. J. INTELL. PROP. & ENT. L. 227, 230 (2015) (“It is a fundamental rule of trademark law that creating or merely adopting a mark, on its own, is insufficient to create trademark rights.”); see also Aycock Engineering, Inc. v. Airflite, Inc. 580 F.3d 1350, 1358 (2009) (“The use provision of the Lanham Act in force in 1970 stated that a service mark was in use in commerce ‘when it is used or displayed in the sale or advertising of services, and the services are rendered in commerce, or the services are rendered in more than one State or in this and a foreign country and the person rendering the services is engaged in commerce in connection therewith.’ Pub. L. No. 87–772, 76 Stat. 769 (1962).”).
144 Of course, the proposed text here is not perfect. There are scenarios that may advance beyond the technology contemplated in this Note. However, the proposed text gives a basic principle that utilizing a trademark’s image for monetized ad revenue will not be allowed under the Lanham Act and will allow the courts to more easily interpret future AR cases.
145 Recall that the holding in Rescuecom essentially prevented Google from allowing misleading results to be displayed in their search engine because another brand had purchased a protected trademark. Rescuecom Corp. v. Google Inc., 562 F.3d 123, 130–31
they had used another’s trademark to intentionally funnel business to other companies. As such, the proposed amendment deals only with the actionable use requirement and would leave the likelihood of confusion test in place for each circuit.\textsuperscript{146} Thus, a trademark holder could sue an AR developer if that developer had used their trademark for the purpose of misdirecting or misleading consumers. However, the amendment would not guarantee that the AR developer was liable. The trademark holder would still have to prove that infringement had occurred.

The amendment also would allow AR developers to assert any traditional defense under trademark, such as fair use.\textsuperscript{147} The proposed amendment would only prevent companies from having their software recognize specific visual trademarks for the sole purpose of overlaying another company’s trademark on top of that real-world trademark or misdirecting consumers. Thus, a company could use a brand’s trademark in an AR application to provide information about the company, similar to the way Google Maps functions, as this would not be misdirecting or misleading consumers.\textsuperscript{148} In this sense, the proposed text merely brings the Lanham Act into the twenty-first century and prevents companies from causing consumer confusion by overlaying their brand identifiers over another.

V. AUGMENTED REALITY AND COPYRIGHT INFRINGEMENT

For full protection of intellectual property, copyright law must also be brought into the Twenty-First century. In fact, copyright law may be most impacted by the development of new AR technologies. To illustrate the need to refine the current copyright laws, imagine a scenario where a patron wearing Google Glass\textsuperscript{149} enters a museum or an art gallery filled with copyrighted works and designs. The patron paid money for entry to the museum and downloaded (2d Cir. 2009). Similarly, the proposed text here prevents AR developers from selling a company’s image trademark to competing companies.

\textsuperscript{146} As stated in Rescuecom, finding “use” of a mark is only one step of the infringement analysis. \textit{Id.} at 130. (“Needless to say, a defendant must do more than use another’s mark in commerce to violate the Lanham Act. The gist of a Lanham Act violation is an unauthorized use, which ‘is likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, … or as to the origin, sponsorship, or approval of … goods [or] services.’ \textit{citing} 15 U.S.C. § 1125(a); \textit{Estee Lauder Inc. v. The Gap, Inc.}, 108 F.3d 1503, 1508–09 (2d Cir. 1997).”).

\textsuperscript{147} 15 U.S.C. § 1115 (b)(4) (fair use provision); \textit{see Trademark Overview, supra} note 9 (discussing the two fair use defenses available under the Lanham Act).

\textsuperscript{148} For clarity, under the proposed text, an AR application that only presented digital information about the particular recognized trademark would still be allowed. For example, if the software recognized a Panera Bread trademark it could still present information, such as how to order online or reviews for the particular establishment. What the proposed text seeks to prevent is another company using that trademark to siphon business away from the trademark owner and confuse the person using the application.

\textsuperscript{149} \textit{See supra} note 104.
an AR application before entering. Browsing the museum, the patron stumbles upon a painting or model. At that moment, the downloaded application overlays both historical information as well as new images, sounds, and videos on top of the existing painting or model, creating a new digital work on the device’s screen. There are two interrelated questions that arise under this scenario, one of copyright infringement and one of copyrightability. First, assuming that the physical work was protected under the Act, does the new work on the device’s screen infringe on its copyright? Second, is the new work eligible for independent copyright protection by the AR application developer, or is it a derivative work of the original and thus protected by the original owner’s copyright?

A. Copyright Protection Requirements for AR

Software has been eligible for copyright protection since 1976.150 In 1976, Congress amended the Copyright Act (Act) to provide for protection of computer software, analogizing the software to literary works.151 However, since that amendment, there has been a body of inconsistent law resulting in certain elements of software to be protected while others are not. Naturally, the intricacies of the AR applications will raise a number of issues. First, it must be determined whether AR works fulfill the basic requirements of originality and fixation to be eligible for copyright protection under the Act.

In order for a work to be eligible for copyright protection under the Act, the work must be fixed and original. 152 A work is “fixed” in a tangible medium of expression when, “its embodiment . . . is sufficiently permanent or stable to permit it to be perceived, reproduced, or otherwise communicated for a period of more than transitory duration.” 153 As others have stated, digital works presented problems with the fixation requirement because of the inherent intangible nature of digital technology. 154 However, courts have generally found

151 Id. at 206–07 (discussing how software reflects creative decisions, like literary works, and Congress utilized this analogy in the 1976 Act).
152 JULIE E. COHEN ET AL., COPYRIGHT IN A GLOBAL INFORMATION ECONOMY 10 (Supp. 2012); see also U.S. COPYRIGHT OFFICE, COPYRIGHT BASICS (2017), available at https://www.copyright.gov/circs/circ01.pdf [https://perma.cc/44PB-3NDR] (“Copyright is a form of protection provided by the laws of the United States to the authors of ‘original works of authorship’ that are fixed in a tangible form of expression.”).
154 See Evan Brown, Fixed Perspectives: The Evolving Contours of the Fixation Requirement in Copyright Law, 10 WASH. J.L. TECH. & ARTS 17, 21 (2014) (“But as technology advanced and the panoply of expressive media expanded, a more fluid concept was required to keep pace.”).
the fixation requirement to be fulfilled even where the digital display changes from user to user.\textsuperscript{155}

In the context of AR, it is important to determine whether the works displayed on a device’s screen are considered “fixed” if the work is only shown on a screen when a user looks at a particular real world object or image.\textsuperscript{156} As stated, the threshold for the fixation requirement is relatively low.\textsuperscript{157} Courts examining similar issues have found that virtual elements can be considered fixed even though they are not permanent. In the early computing case of \textit{Williams Electronics, Inc. v Artic International, Inc.}, the court found that the change in visual experience from player to player still allowed for the underlying elements of the game to be fixed.\textsuperscript{158} Because the fixation requirement merely requires a work to exist for longer than a transitory duration, it is highly likely that digital AR works will fulfill the fixation requirement.\textsuperscript{159}

A work must also be “original” to be copyrightable.\textsuperscript{160} The originality requirement stems primarily from a policy perspective of requiring at least some amount of creativity in order to be eligible for copyright protection.\textsuperscript{161} Courts have been unclear on exactly how much creativity or originality is required in order to qualify for copyright protections,\textsuperscript{162} although courts have generally held that direct copies of objects in other mediums are not eligible for copyright

\footnotesize{
\textsuperscript{155} See \textit{Williams Elec., Inc. v. Artic Int’l, Inc.}, 685 F.2d 870, 874 (3d Cir. 1982) (finding that although the video game at issue created new images each time a particular mode was displayed, the fixation requirement was met because the underlying circuit board was sufficiently permanent or stable to permit it to be reproduced, or otherwise communicated for more than a transitory period).

\textsuperscript{156} An AR application would only show the superimposed image on a screen if that application was pointed at an image that it recognized. At that point, the application would overlay the digital content over the physical object on the device’s screen. When the user moved the screen away from the object, the object would no longer be displayed on the device’s screen.

\textsuperscript{157} Brown, supra note 154, at 24 (discussing how after the \textit{Williams} decision, fixation was generally “no longer a barrier to the development of digital works”).

\textsuperscript{158} See \textit{id.} (discussing the \textit{Williams} decision).

\textsuperscript{159} See \textit{MAI Sys. v. Peak Comput., Inc.}, 991 F.2d 511, 517–18 (9th Cir. 1993) (holding that the loading of software onto a computer’s RAM for only a brief period of time fulfilled the fixation requirement). Similarly, an AR application will likely show the underlying work on the device’s screen, if only for a brief period of time.

\textsuperscript{160} See \textit{supra} note 143 and accompanying text.

\textsuperscript{161} COHEN ET AL., supra note 150, at 61 (2015) (“[F]rom an economic perspective, the mere copyist has supplied nothing to justify the cost of a grant of copyright; from a noneconomic perspective, the copyist has supplied nothing of his or her ‘own.’”).

\textsuperscript{162} The Supreme Court has acknowledged that lower courts often misunderstood the originality requirement. \textit{See Feist Publ’n, Inc. v. Rural Tel. Serv. Co.}, 499 U.S 340, 351–53 (1991) (“Most courts construed the 1909 Act correctly, notwithstanding the less-than-perfect statutory language. They understood from this Court’s decisions that there could be no copyright without originality. . . . [B]ut some courts misunderstood the statute . . . [m]aking matters worse; these courts developed a new theory to justify the protection of factual compilations.”).
For example, in *Meshwerks v. Toyota*, the court determined that the replicated computer models of Toyota’s cars were not eligible for copyright protection irrespective of the large amount of effort and work required to create those models. As the court stated, “Meshwerk’s digital wire-frame computer models depict Toyota’s vehicles without any individualized features. . . . [i]n short its models reflect none of the decisions that can make depictions of things or facts in the world . . . .” Applying this same reasoning to AR, it is unlikely that a court would find exact digital replications of real-world objects or commonplace symbols to be eligible for copyright protection if digitally replicated via AR applications.

### B. Derivative Works or Original Works?

However, the scenario outlined at the beginning of this Part differs substantially from the *Meshwerks* case, as it potentially creates a “derivative work” instead of a new, original work. The original holder of a copyright maintains the right to prepare derivative works. Thus, if courts were to find that AR applications were creating derivative works, AR application developers would risk expensive copyright infringement suits unless they were protected by the fair use doctrine. In contrast, if courts were to find that AR applications were creating new, original works, then the AR application owner could potentially start copyrighting anything that crossed the originality threshold when the graphics are overlaid on top of the original work.

---

163 *Durham Indus., Inc. v. Tomy Corp.*, 630 F.2d 905, 910 (2d Cir. 1980) ("[T]he mere reproduction of the Disney characters in plastic, even though the adaptation of the preexisting works to this medium undoubtedly involved some degree of manufacturing skill, does not constitute originality as this Court has defined the term.").


165 *Id.* at 1265.

166 U.S. COPYRIGHT OFFICE, COPYRIGHT IN DERIVATIVE WORKS AND COMPILATIONS (2013), available at [https://www.copyright.gov/circs/circ14.pdf](https://www.copyright.gov/circs/circ14.pdf). The United States Copyright Office defines a derivative work as a work based on or derived from one or more already existing works. *Id.* Derivative works must incorporate some or all of the preexisting work and add new original copyrightable authorship to that work. *Id.*

167 17 U.S.C. § 106(2) (2012). Under Section 106 of the Act, the copyright owner has the exclusive rights to “prepare derivative works based upon the copyrighted work.” *Id.*

168 Essentially, holding that AR applications are creating derivative works would open developers up to litigation. This is because the right to create derivative works belongs to the copyright holder.

169 In contrast to the above, holding that AR applications are creating original works would allow developers to take existing copyrighted works and augment them with digital elements to obtain their own copyright protection on new work.
Derivative works are one of the most disputed areas of copyright law. Derivative works are protected by copyright under Section 106(2), and protection of derivative works is a fundamental right in copyright law. In addition, Section 103(a) provides that derivative works meeting the statutory standards of Section 102 are independently copyrightable. Whether AR is transformative enough to create a new original work or if AR devices are merely creating derivative works protectable by the original copyright owner is an undecided question.

While courts have not yet spoken directly on the issue of whether AR overlays create new, original works or derivative works, looking at the legal debate surrounding photographs provides insight into the difficulty resolving the issue without any statutory clarity. The Seventh Circuit has stated, “[W]hether photographs of copyrighted work are derivative works is the subject of deep disagreement among courts and commentators alike.” In Schrock v. Learning Curve International, Inc., the court examined whether photographs taken of toys were derivative works or original works eligible for their own copyright protection. That court first looked at the technical choices made by the photographer to determine that the photographs passed the ordinary test for originality. Second, that court rejected the contention that derivative works are subject to a higher level of originality and agreed that the relevant standard was whether a derivative work contained a “nontrivial” variation from the

---

170 See Pamela Samuelson, The Quest for a Sound Conception of Copyright’s Derivative Work Right, 101 GEO L.J. 1505, 1509–10, 1549–50 (2013) (discussing how even basic mediums, such as photography, which have been around since the introduction of the Copyright Act, have been subject to unclear case law about what makes them derivative works).

171 17 U.S.C. § 101 (2012) (“A derivative work is a work based upon one or more preexisting works, such as a translation, musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which a work may be recast, transformed, or adapted. A work consisting of editorial revisions, annotations, elaborations, or other modifications, which, as a whole, represent an original work of authorship is a ‘derivative work.’”). See generally Daniel Gervais, The Derivative Right, or Why Copyright Law Protects Foxes Better than Hedgehogs, 15 VAND. J. ENT. & TECH. L. 785 (2013).


174 Id. HIT, the copyright owner in the Schrock case, hired a photographer to take product photographs of its toys for promotional use. Id. at 516. The photographer took numerous photos over the course of four years as directed by the party’s contractual agreement, choosing the lighting, sets, etc. Id. The photographer then sought to register the photos for copyright protection. Id. The district court found that the lack of permission from HIT was a bar to copyright protection. See id. at 517.

175 Schrock v. Learning Curve Int’l, Inc., 586 F.3d 513, 519 (7th Cir. 2009). The court determined that the choices made by the photographer combined “to create a two-dimensional image that is subtly but nonetheless sufficiently his own.” Id.
Accordingly, the court held that because the photographs contained distinguishable changes, they qualified for derivative work copyright protection.

Some courts and scholars have attempted to further clarify what exactly qualifies as a derivative work. In *Ty Inc. v. Publications International Ltd.*, the court determined that collector’s guide was not a derivative work because “guides don’t recast, transform, or adapt the things to which they are guides.”

Courts have also found that a shift in medium without more is generally insufficient to satisfy the requirement of originality for copyright in a derivative work. Additionally, in *Micro Star v. FormGen*, the Ninth Circuit examined whether custom levels created within a video game where derivative works of the original video game. The defendant in the case used these user-created levels to create their own video game. The user-created levels utilized “MAP files” that triggered different audiovisual displays. That court examined the derivative work requirement noting that the Ninth Circuit had previously required that in order to qualify as a “derivative work” that work must exist in a “concrete or permanent form” and must *substantially incorporate protected material from the preexisting work*.

---

176 *Id.* at 520–22. The court distinguished this case from other decisions, which have held that derivative works should perhaps be subject to more stringent originality requirements. *Id.*

177 *Id.* at 522. The court held that because the photographs were highly accurate but “contain minimally sufficient variation in angle, perspective, lighting, and dimension to be distinguishable from the underlying works . . . the photos qualify for the limited derivative-work copyright.” *Id.*

178 *Ty, Inc. v. Publ’ns Int’l Ltd.*, 292 F.3d 512, 520 (7th Cir. 2002) (emphasis added).

179 See e.g., *Schrock v. Learning Curve Int’l, Inc.*, 586 F.3d 513, 519 n.3 (7th Cir. 2009) (citing Durham Indus., Inc. v. Tomy Corp., 630 F.2d 905, 910 (2d Cir. 1980); L. Batlin & Son, Inc. v. Snyder, 536 F.2d 486, 491 (2d Cir. 1976)).

180 *Micro Star v. FormGen Inc.*, 154 F.3d 1107, 1109 (9th Cir. 1998). FormGen created and obtained copyright protection for the game “Duke Nukem 3D,” which included a custom level-building program in the game. *Id.* Users were encouraged to create their own levels that were then playable by other players. *Id.* Micro Star took 300 user-created levels and sold them on a new disc titled “Nuke It.” *Id.* FormGen then sought to enforce its copyright protection and prevent Micro Star from using the user-created levels in their own game. *Id.* The court described the game at issue as having three separate components: the game engine, the source art library, and the MAP files. *Id.* at 1110. The MAP files, at issue in the case, contained the instructions that tell the game engine what to display in order to create the audiovisual display. *Micro Star*, 154 F.3d at 1110. FormGen alleged that the audiovisual displays generated when a user plays the Micro Star game were derivative works because although the MAP files were not identical, the Micro Star version still used the Duke Nukem 3D art library to generate the images. *Id.*

181 *Id.* at 1109.

182 *Id.* at 1110. The MAP files are what triggered the software to display certain audiovisual elements. *Id.*

183 *Id.* (emphasis added).
issue could be derivative works because they triggered the various audiovisual displays and incorporated the underlying software.\footnote{Micro Star v. FormGen Inc., 154 F.3d 1107, 1111–12 (9th Cir. 1998).}

C. Fair Use in the Augmented Reality Context

While authors of original and fixed works are afforded general copyright protections, including the ability to control derivative works, the fair use doctrine is a limitation on the rights of copyright owners.\footnote{COHEN ET AL., \textit{supra} note 150, at 563.} Section 107 of the Act provides the courts with four factors to consider when determining whether something is fair use: purpose of use, nature of the copyrighted work, amount and substantiality of the portion used in relation to the copyrighted work as a whole, and the effect of the use upon the potential market for or value of the copyrighted work.\footnote{17 U.S.C. § 107 (2012) (‘‘Notwithstanding the provisions of sections 106 and 106A, the fair use of a copyrighted work, including such use by reproduction in copies or phonorecords or by any other means specified by that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright. In determining whether the use made of a work in any particular case is a fair use the factors to be considered shall include—(1) the purpose and character of the use, including whether such use is of a commercial nature or is nonprofit educational purposes; (2) the nature of the copyrighted work; (3) the amount and substantiality of the portion used in relation to the copyrighted work as a whole; and (4) the effect of the use upon the potential market for or value of the copyrighted work.’’).} An important focus of the first factor of the test is whether the use is “transformative.”\footnote{COHEN ET AL., \textit{supra} note 150, at 615.} The Supreme Court has stated that the more transformative the new work, the less significant the other factors will be.\footnote{Campbell v. Acuff-Rose Music, Inc., 510 U.S 569, 579 (1994).} Each circuit uses this test as a general framework, although some have attempted to further clarify the fair use analysis resulting in a body of inconsistent case law.

In \textit{Cariou v. Prince}, the Second Circuit found that an artist was entitled to fair use protections when he took photographs and altered them by painting different images over top of the subject’s facial features and using various sizes of the images.\footnote{Cariou v. Prince, 714 F.3d 694, 706–08 (2d Cir. 2013).} The court primarily focused on whether the artist had transformed the original artist’s paintings into something “new and different.”\footnote{\textit{Id.} at 710 (“Prince used key portions of certain of Cariou’s photographs. In doing that, however, we determine that in twenty-five of his artworks, Prince transformed those photographs into something new and different and, as a result, this factor weighs heavily in Prince’s favor.”).} However, other circuits have disagreed with the Second Circuit’s approach.\footnote{Kienitz v. Sconnie Nation LLC, 766 F.3d 756, 758 (7th Cir. 2014).} As Judge Easterbrook has stated, “[T]he Second Circuit has run with the suggestion that transformative use is enough to bring a modified copy
within the scope of § 107.” The Seventh Circuit has stated that holding that any “transformative use” could be a “fair use” would essentially blur the lines of where derivative works start and end, because to transform is to essentially create a derivative work. Further, the Seventh Circuit has stated that the most important of the four factors is generally the market effect.

As demonstrated from these two cases, circuit courts are not uniform in their treatment of the fair use doctrine. Application of the fair use doctrine to AR in light of these decisions creates an uncertain scenario. First, AR applications are, by nature, highly “transformative.” An AR application could instantly overlay an unlimited amount of material on a user’s screen, making the underlying work unrecognizable. Second, AR applications are likely to utilize all of the underlying work when creating a new image, the second factor of the fair use test. Finally, treating the market effect factor as the most important, AR could have a dramatic effect on the market effect or long-range commercial opportunities of the author. Take the scenario at the beginning of this Part. If an artist had licensed her painting to a museum in 1990 before AR was contemplated, and that museum now provides its patrons with an AR application that allows them to digitally transform her painting at an additional cost, her long-range commercial opportunities may be substantially affected by the new AR application. From this brief overview, circuit courts would likely be inconsistent in their application of the current fair use doctrine to AR applications.

D. A Framework for Amending the Copyright Act

Courts and scholars have been unclear on whether traditional mediums, such as photographs, are derivative works or new original works. In fact, courts have correctly described the statutory language defining a derivative work as, “hopelessly overbroad.” Additionally, whether digital AR works will be protected by the fair use doctrine is unclear. Application of the various cases dealing with derivative works shows that it is likely that the federal circuits will be inconsistent in resolving even more complex AR cases.

---

193 See Kienitz, 766 F.3d at 758 (“We’re skeptical of Cariou’s approach, because asking exclusively whether something is ‘transformative’ not only replaces the list in § 107 but also could override 17 U.S.C. § 106(2), which protects derivative works.”).
194 Id.
195 This Note does not delve further into the fair use doctrine because the only point needed is that fair use has not enjoyed straightforward application in the lower courts and it is highly unlikely that the courts will be uniform in their application of the current test to AR works.
196 Micro Star v. FormGen Inc., 154 F.3d 1107, 1110 (9th Cir. 1998) (elaborating that because the language is so overbroad, courts have had to develop doctrines to limit it, such as the requirements that the work exist in concrete or permanent form and must substantially incorporate the protected material from an existing work).
197 See supra notes 186–194 and accompanying text.
Although shifts in medium alone have been found to be insufficient, using the reasoning from *Ty, Inc.*, it is likely that courts will find AR creates derivative works.\(^{198}\) As the House Report accompanying the 1976 Act states, “the infringing work must incorporate a portion of the copyrighted work in some form . . . .”\(^{199}\) Any AR application will naturally recast and transform the original image, easily surpassing this standard.\(^{200}\) Additionally, application of the “nontrivial” standard utilized by *Schrock* will likely mean that AR applications will almost always be creating derivative works when new digital items are overlaid on top of real-world copyrighted objects.\(^{201}\)

Similar to *Micro Star*, AR applications utilize the underlying work in order to create other works.\(^{202}\) For example, if an AR application only displays particular digital content when it recognizes an underlying original work, then like the MAP files in *Micro Star*, that underlying work is still a main component of the new digital work. In basic terms, without the underlying work, there would be no AR creation. Thus, a court applying the *Micro Star* reasoning would likely find that AR applications that utilize existing copyrighted works are creating derivative works.\(^{203}\)

Whether the courts take the view that new AR applications are creating derivative works or new original works, there are a number of undesired results. As Paul Goldstein has stated, “taken together, sections 102(a) and 103, and sections 106(1) and 106(2), give a prospective copyright owner the incentive to make an original, underlying work, the exclusive right to make new, successive works incorporating expressive elements from the underlying work . . . .”\(^{204}\)

---

\(^{198}\) Unlike *Ty, Inc.*, AR works “recast” the original work. See supra note 178 and accompanying text.

\(^{199}\) COHEN ET AL., supra note 150, at 333 (citing H.R. REP. NO. 94-1476, at 62 (1976)).

\(^{200}\) This is because AR by its nature utilizes the underlying work or landscape and “augments” it. This will always require displaying a copy of the original work on a device’s screen.

\(^{201}\) In *Schrock*, the court quoted the Nimmer treatise to determine that the relevant standard is whether a derivative work contains a “nontrivial” variation from the preexisting work “sufficient to render the work distinguishable from the prior work in a meaningful manner. Applying that test to AR, it is likely that the digital transformations made to the underlying works will often result in substantial and nontrivial changes.” *Schrock v. Learning Curve Int’l, Inc.*, 586 F.3d 513, 520 (7th Cir. 2009) (citing 1 MELVILLE B. NIMMER & DAVID NIMMER, NIMMER ON COPYRIGHT § 3.01 3-2 (1978)).

\(^{202}\) Like the technology in *Micro Star*, an AR application will use the underlying code and the original protected work to display images on a device’s screen; however, the actual images being displayed on screen will likely change from user to user. See supra notes 180–184 and accompanying text.

\(^{203}\) This is what makes AR technology especially tricky for copyright law. The amount of changes that are being made to an underlying work will never be consistent; they will vary from user to user. Thus, like the court in *Microstar*, a court will likely find that utilizing the underlying work results in a creation of a derivative work. See supra notes 180–184 and accompanying text.

\(^{204}\) COHEN ET AL., supra note 150, at 320 (citing Paul Goldstein, *Derivative Rights and Derivative Works in Copyright*, 30 J. COPYRIGHT SOC’Y U.S.A. 209, 217 (1983)).
Thus, if a court were to find that AR applications use the expressive elements of a work to create a derivative work, AR applications would constantly be infringing on copyrights unless they are protected by the fair use doctrine.\textsuperscript{205}

Alternatively, if AR applications meet the originality threshold categorizing them as new, original works, which seems unlikely given the previous case law, then original owners would lose one of their basic incentives to create. AR application developers could create relatively simple software that substantially changed a copyrighted painting. Those application developers would then have a new work that they could copyright themselves. Obviously, this scenario seems highly unfair to the original author; however, under current law, this scenario is not unthinkablenot unthinkablenot unthinkablerem.\textsuperscript{206}

Therefore, due to the inconsistent body of law dealing with derivative works and the application of the fair use doctrine, Congress must amend the Copyright Act to reflect the modern advent in ability to quickly create new derivative works that strikes the proper balance between original authors and developers. Congress has not been averse to amending copyright laws to consider technological advancements.\textsuperscript{207} For example, in 1976, Congress updated the Act to deal with the advent of computer software.\textsuperscript{208} Similarly, Congress must now act to refresh the Act to be effective in the current midst of the technological revolution. An effective update of derivative work and fair use protections would maintain the original author’s ability to control their original work, but also allow AR developers to continue innovating in the field. AR can be a powerful learning tool in places, such as museums; however, original authors must retain an incentive to create and must not lose commercial control of their works.

Congress has also updated the Copyright Act to limit the exclusive rights of the copyright holder in the past. For example, section 112 of the Act was included in the 1976 Act to allow the transmission of certain works as long as

\textsuperscript{205} This is because the copyright owner has the exclusive right to control derivative works. 17 U.S.C. § 106(2) (2012). Reliance on the fair use doctrine by AR developers would be an uncertain defense and likely result in less innovation in the field. As stated, the fair use doctrine is inconsistently applied because of the four-part test. See supra Part V.C. Reliance on this test alone in the AR field is inadvisable because there is a clear separation between AR applications that use the underlying work for monetary gain and those that do not.

\textsuperscript{206} A court could rationally hold that an AR application created a new digital work with enough original elements to be independently copyrightable. This is due to the uncertain nature of precedent in the derivative work sphere. See supra notes 167–170 and accompanying text.


\textsuperscript{208} See supra notes 150–151 and accompanying text (discussing the 1976 Act).
no copies of the work were made. However, Section 112 can operate as a framework for how the legislature should handle AR. AR works are often benign in their usage and seek only to supplement the experience of the underlying original work. However, there are instances where AR could be a detriment to the copyright holder and cause the loss of monetary gains or the incentive to create new works.

Thus, the new derivative work amendment should protect the original authors from AR applications attempting to monetize their works in a way that they did not originally intend. Conversely, AR applications should not be absolutely barred from utilizing any underlying works that may have copyright protections. Any amendment should utilize the fair use factor test to balance the interests of the original author and the subsequent uses of the work but also clearly distinguish between benign and monetary uses.

Therefore, the Augmented Reality Derivative Work Amendment could read:

Notwithstanding the provisions of section 106, and except in instances of contractual arrangement, it is not an infringement of copyright for an augmented reality ("AR") application to utilize a work protected under section 102 of the Act if—

The copy of the work is retained only within the software of the application for the purposes of digital overlay and no further copies are made or disseminated; and

209 H.R. REP. NO. 94-1476, at 14, 101–02 (1976); COHEN ET AL., supra note 150, at 252 (discussing how § 112(a) allows for an exception in certain cases where a “transmitting organization” can make one copy of a “transmission program” and not be liable for infringement).

210 For example, an AR application could use the underlying work for educational purposes only. When the application recognized a famous painting by Picasso, the application could augment a picture of Picasso, as well as historical and informational facts about his life. This is an example of a benign usage of AR.

211 In contrast, an AR application could recognize that same Picasso painting and allow the user to transform the image on the device’s screen using image editing tools. The user could then save the new creation to the device’s memory—for a fee. This usage of copyrighted works would be problematic because the AR developer is charging money and the user is able to save the altered work for further dissemination.

212 Of course, any amendment to the Act would need to cater more to the intricacies and nuances of copyright law and AR. Additionally, what was included under the term “augmented reality application” would need to be defined under Section 101 of the Act. Due to the limited space, the text proposed here is a mere starting point for lawmakers to identify and solve the issues that will arise as AR becomes more mainstream. The amendment has two main goals: (1) ensure that owners do not lose control over their works due to advancements in technology and (2) utilize the traditional fair use analysis to separate AR applications that are using original works for monetary purposes versus purely educational or supplemental means.
The copy of the work is used solely for the purposes of overlaying new information within a determined service area and the use is within that originally contemplated by the copyright owner to be determined by the factors outlined in section 107 of this Act; and

The copy of the work is not used for the monetary or economic gain of the application developer unless otherwise provided by contractual arrangement.

The proposed text seeks to maintain the integrity and underlying goals of the Act while also allowing for reasonable innovation within the AR field. Thus, the example at the beginning of this Part would only be actionable as infringement if the AR application or the museum had started to exploit the underlying work and create new works for monetary gain, which would not have been contemplated by the original copyright owner.213 Alternatively, AR applications that merely added supplemental information to the underlying work would not be found to be infringing on the work.214 The proposed text attempts to utilize the existing fair use framework while also acknowledging that the current test by itself is not entirely suitable for AR applications.215

The amendment ensures that AR applications that utilize underlying copyrighted works are not liable for infringement as long as developers follow reasonable restrictions. Developers are free to create educational or supplemental applications, as long as the copyrighted work is not continuously copied or disseminated and sold for monetary gain, which is similar to the current way section 107 operates.216 If a developer does wish to utilize the underlying work for monetary gain or distribution, then that developer must obtain a license or permission from the copyright owner. In this sense, the proposed text brings the treatment of AR into the twenty-first century while still maintaining the underlying justifications and rationales of copyright protection.217

213 An artist who placed their work in a museum would have expected that the public would view the work. However, it is unlikely that the artist would have imagined that a patron could walk into the museum with a paid AR application on their phone and augment new digital elements onto their work. The proposed text seeks to deal with this issue by separating monetary and non-monetary uses.

214 For example, if the museum or third-party developer only used the work in order to add supplemental information, such as facts from a site like Wikipedia, this would not be considered infringement, unless the application was using the underlying work for monetary gain without a contractual license with the author.

215 The fair use defense is often unclear in application. See supra Part V.C. Specifically, for AR, fair use presents a host of unforeseen issues due to the dynamic experience that changes from user to user and also the possibility that AR developers can use the underlying works for monetary gain in some instances and not in others.

216 See supra note 186 and accompanying text for a discussion of the current fair use test. In this sense, the proposed text aims to maintain the author’s ability to make a profit of their works but also seeks to keep the integrity of the fair use test.

217 The proposed text seeks to allow the copyright holder to maintain their rights and incentives to create but also allow benign uses of their works as is expected under current
VI. CONCLUSION

The rapid development of new technologies in the midst of the current technological revolution is beginning to put a strain on both real and intellectual property laws. The time has come for comprehensive legislative action to avoid the gray areas that are certain to arise over the next five to ten years when the bounds of real and virtual worlds meet. As addressed in this Note, three areas of the law will be impacted in previously unforeseen ways by the forthcoming surge of AR development: real property law, trademark law, and copyright law. While the impacts will certainly be felt in the courts, Congress can take modest steps to alleviate the problems.

Enacting a new statute that provides real property owners with recourse against a virtual intrusion will place real property owners on an even playing field in an age where intellectual property can be placed in thousands of locations simultaneously. Likewise, updating the Lanham Act’s definition of actionable use to consider new technological capabilities of AR and mixed reality will prevent trademark holders from losing the value of their brand identifier while still allowing for AR applications to use trademarks for informational purposes. Finally, amending copyright law protections to clarify what constitutes an infringing use of an underlying work in the AR context will allow creators to retain the traditional incentives under copyright law while also allowing for innovation in the AR space. These measures will comprehensively protect innovation yet still provide incentives for the owners and creators of property. Additionally, these measures are more cost effective than relying on retroactive judge-made law to handle the issues and will provide much needed stability and clarity in the laws.

These approaches will allow the courts to adjudicate in an effective, informed manner and provide clear guidance to innovators in the AR field. Commercial AR is relatively new and rapidly growing as an industry, while current statutory law remains stagnant and silent on the issue. The current technological revolution is growing at a pace never before seen in human history. Thus, legal questions surrounding the new technology must be resolved with modest revisions to existing property laws before they become outdated and ineffective.

copyright laws. See COHEN ET AL., supra note 150, at 7 (“[C]opyright law provides a legal entitlement to the copyright owner to exclude others from enjoying certain benefits of the work . . . Copyright law exists to prove a marketable right for the creators and distributors of copyrighted works, which in turn creates an incentive for production and dissemination of new works.”).
The Decontextualization of Music in Political Settings: An Argument for Moral Rights for Musical Works

CHANCE JOHNSON*

TABLE OF CONTENTS

I. INTRODUCTION ..................................................................................620
II. BACKGROUND ..................................................................................623
   A. History of Unauthorized Uses of Music in Political Campaigns .........................................................623
   B. Trump Controversies ...........................................................................................................................624
   C. What Are Moral Rights? ....................................................................................................................626
III. GAPS IN U.S. MORAL RIGHTS LAW .................................................627
   A. Statutory Inadequacy ..........................................................................................................................627
   B. Contractual Protections ....................................................................................................................629
IV. BROWNE V. MCCAIN: ARGUING FOR THE POLITICIANS ..................632
   A. Copyright Infringement ......................................................................................................................633
   B. Trademark Infringement ....................................................................................................................634
   C. Right of Publicity ...............................................................................................................................635
   D. Reflections on Browne .......................................................................................................................636
V. URGENCY: THE TROUBLE OF DECONTEXTUALIZATION IN A TURBULENT POLITICAL CLIMATE ................................................637
IV. PROPOSED SOLUTION ......................................................................639
   A. Previous Proposals ...........................................................................................................................640
   B. Finding a Proper Starting Point ........................................................................................................641
   C. Proposed Legislative Text ................................................................................................................643
   D. Contractual Waiver ..........................................................................................................................644
   E. Standards of Review ........................................................................................................................645
   F. Remedies ...........................................................................................................................................646
   G. Reconciliation with Existing Moral Rights Doctrine .......................................................................647
   H. Resolving Decontextualization of Music in Political Settings ........................................................................648
VII. CONCLUSION .................................................................................648

* Articles Editor, Ohio State Law Journal; Juris Doctor Candidate, The Ohio State University Moritz College of Law, 2019; Bachelor of Arts, Oklahoma City University, 2016.

I would like to thank the staff of the Ohio State Law Journal that reviewed my work and helped me bring it to publication quality. I would also like to thank my parents, Greg and Ann; my sister, Clarissa; and my girlfriend, Kyndal Jones, for their support and encouragement.
I. INTRODUCTION

It is hard to imagine what could bring an artist to symbolically and, to some extent literally, destroy his own creation. Such was the case with Matt Furie and Pepe the Frog. Furie created Pepe more than a decade ago as a character in his comic *Boy’s Club*.1 At the time he was created, Pepe could best be described as “an anthropomorphic frog that lives with a party wolf, a bear-like creature, and then kind of a muppety, dog-like creature . . . in a one-room apartment. And [they] kinda just party together and pull pranks on one another and hug each other . . . .”2 By 2015, however, the harmless “everyman” that Furie envisioned had morphed into something more troubling: the insignia for “alt-right” extremist groups, a dog whistle for white nationalists, and a badge of honor for disaffected Internet trolls.3 In September 2016, the Anti-Defamation League (ADL) designated Pepe a hate symbol.4 After concerted efforts by Furie and the ADL to reclaim Pepe and restore his image failed, Furie laid Pepe to rest, depicting his funeral in a one-page comic.5

Pepe’s story is just one dramatic example of the power of social forces to transform the meaning of pieces of popular culture into something dramatically different than what the author intended. For other artists, the threat continues to loom that their work might be appropriated by individuals, groups, or social movements with which they do not agree. One purpose of this Note is to show that an increasingly likely source of problems like these is the unauthorized use of popular music by political candidates and groups in their activities and discourse.

To that end, it is worthwhile to look at another example, involving one of America’s largest pop stars, Taylor Swift, and groups similar to those that co-

---

2 Id.
3 Id. (“[T]he meaning of Pepe as kind of a white nationalist or alt-right symbol kind of exploded. It was considered by many to be a tactic of dog-whistling from the Trump campaign to that sect of white nationalists online, and it became a new symbol for white nationalists maybe not online.”).
4 *ADL Adds “Pepe the Frog” Meme, Used by Anti-Semites and Racists, to Online Hate Symbols Database*, ADL (Sept. 27, 2016), https://www.adl.org/news/press-releases/adl-adds-pepe-the-frog-meme-used-by-anti-semites-and-racists-to-online-hate#.V-rqlvkrJaQ [https://perma.cc/65K3-35WV] (explaining that the “Hate on Display” database was founded in 2000 as part of the ADL’s effort to track hate groups and help law enforcement and education efforts).
5 Jacey Fortin, *Pepe the Frog Is Dead, or So His Creator Hopes*, N.Y. TIMES (May 8, 2017), https://www.nytimes.com/2017/05/08/us/pepe-the-frog-comic.html [https://perma.cc/S7GV-CTCX] (describing Furie’s personal struggles with how his character has been used and explaining how Furie’s dramatic attempt to lay his character to rest may not ultimately be successful).
opted Pepe. In late 2017, the left-leaning blog, PopFront, published a piece in response to Swift’s new music video, “Look What You Made Me Do.”\textsuperscript{6} The piece suggested that Swift’s music video represented her latest covert message to white supremacists that she supports the “re-awakening” of their movement.\textsuperscript{7} PopFront was building on a narrative, that has gained traction in recent years, that Swift is a closeted racist.\textsuperscript{8} Former Breitbart columnist, Milo Yiannopoulos, traced the origin of this narrative back to 2013 and a Pinterest account that began posting images of Swift accompanied by quotes from Adolf Hitler, supposedly doing so to draw attention to the problem of quotes being misattributed to celebrities.\textsuperscript{9} This narrative has been embraced by some members of the alt-right as well, most notably Andrew Anglin, who runs the white supremacist blog, the \textit{Daily Stormer}.\textsuperscript{10} Anglin has published dozens of posts about Swift, often referring to her as a an “Aryan Goddess.”\textsuperscript{11}

Without speculating on Swift’s political leanings,\textsuperscript{12} a number of things about this story should be concerning to present and future musicians. First, the
association between Swift and white supremacists may well have been predicated on careless, but not necessarily nefarious, actions by third parties. 13

Second, Swift may not have done anything to warrant this association, other than making some questionable and arguably insensitive creative choices in past music videos. 14

Third, it is not just her reputation but also the meaning of her work that is being affected by this narrative. 15

Concerns such as these are the driving motivation for this Note. Its purpose is to show that the unauthorized use of music in political campaigns and activities presents a unique risk to the moral rights of musicians. As is evident in the cases of Furie and Swift, artists can see their creations diminished and their meaning called into question based on careless associations with problematic ideas. Political campaigns are, perhaps more than anything, vehicles for ideas; some noble, some legitimate, some questionable, and some troubling. 16

When a piece of music is played in a political setting, an association is created between that work and the ideas promoted in that setting. The results of that association have the potential to be detrimental to the work and its author. Previous commentators have assigned a term to this phenomenon, “decontextualization.” 17

For the remainder of this paper, “decontextualization” will be used to refer to the use of music without an artist’s consent or in settings contrary to the music’s intended meaning.

[https://perma.cc/PRN5-3CEL]. The post contained a fairly lengthy caption, in which Swift acknowledged her prior reluctance to wade into politics; endorsed two Democratic candidates in Tennessee, Phil Bredesen and Jim Cooper; and encouraged her followers to vote. Id. Swift also spoke on issues of discrimination, saying, “I believe that the systemic racism we still see in this country towards people of color is terrifying, sickening and prevalent. I cannot vote for someone who will not be willing to fight for dignity for ALL Americans, no matter their skin color, gender or who they love.” Id.

13 See Yiannopoulos, supra note 9.

14 See Prachi Gupta, Taylor Swift’s Music Video Is Uncomfortable, but Is It Really Racist?, SALON (Aug. 20, 2014), https://www.salon.com/2014/08/19/is_taylor_swifts_new_music_video_offensive/ [https://perma.cc/C84J-3PYG] (analyzing some controversial scenes from Swift’s “Shake It Off” music video in which she is depicted wearing gold chains and singing as a crew of black female backup dancers twerk around her).

15 Swiftly, supra note 6 (“Taylor’s are lyrics that connect with whites that are concerned with what they see as the white dispossession of power. . . . The lyrics validate those who feel that [they] have been wronged, e.g. white people angry about a black president.”).

16 See WILLIAM L. BENOIT, COMMUNICATION IN POLITICAL CAMPAIGNS vii–viii (2007) (“Elections are inherently and essentially communicative in nature.”).

The unfortunate consequences of decontextualization can best be avoided by the adoption of a meaningful moral rights\(^{18}\) doctrine for musical works in the United States. Part II provides necessary background information; namely, the history of unauthorized uses of popular music in campaign settings and a brief overview of moral rights. Part III discusses the inadequacy of current moral rights law in the United States. Part IV includes a case illustration of \textit{Browne v. McCain}, arguably the most notable example of an artist attempting to stop the unauthorized use of his music in a campaign, which should reinforce the critique offered in Part III and offer a glimpse of the typical arguments offered by unauthorized users in response to these allegations of decontextualization. Part V discusses how the statutory inadequacies highlighted in Parts III and IV coupled with an increasingly polarized and toxic political environment create an urgent need for moral rights legislation for music in the United States. Part VI provides a statutory proposal for new moral rights legislation for musical works in the United States. Part VII will briefly conclude.

\section*{II. Background}

\subsection*{A. History of Unauthorized Uses of Music in Political Campaigns}

Oddly enough, the use of popular music in political campaigns is a relatively recent phenomenon.\(^{19}\) President Reagan in his 1984 presidential campaign is widely considered to be the first to make use of popular music in political settings when he started playing Bruce Springsteen’s “Born in the U.S.A.” at his rallies in order to convey a sense of “energy and patriotism.”\(^{20}\) Prior to that point, campaign music was specially written for the given election.\(^{21}\) Much like his modern-day counterparts, Reagan’s use of “Born in the U.S.A” was non-permissive.\(^{22}\) Springsteen did not approve of Reagan’s use of the song, refusing to endorse either Reagan or his opponent, Walter Mondale.\(^{23}\) But since Reagan started the trend, “the practice of a political campaigns using popular music

\footnotesize
\(^{18}\) Moral rights theory is a European concept built around the beliefs that artists have a relationship with their work that does not end upon its completion or sale and that any harm that befalls their work translates into personal harm to the artist. \textit{See infra} notes 37–42.


\(^{20}\) \textit{Id.} (“Reagan’s re-election campaign also made extensive use of a song by country singer Lee Greenwood, ‘God Bless the U.S.A.,’ and played the song in an introductory video which ran prior to President Reagan’s speech at the 1984 Republican National Convention.”).

\(^{21}\) \textit{Id.} at 139.

\(^{22}\) \textit{Id.}

without authorization has become a feature taken almost for granted in the contemporary political landscape.”

The trend continued in 1988. Democratic candidate Michael Dukakis utilized Neil Diamond’s “America” at the Democratic National Convention and Creedence Clearwater Revival’s “Fortunate Son” and Michael Jackson’s “Man in the Mirror” at campaign stops. Republican heir apparent George H.W. Bush also made use of Lee Greenwood’s “God Bless the U.S.A.” and Bobby McFerrin’s “Don’t Worry, Be Happy.” The presidential candidates in 2016 built on this tradition as well. Hillary Clinton heavily utilized Rachel Platten’s hit song, “Fight Song.” Then-candidate Donald Trump made use of a variety of songs during his campaign that gave rise to a fair amount of controversy. His selections and the subsequent controversies will be discussed below.

B. Trump Controversies

Candidate Trump became embroiled in a number of controversies due to his unauthorized uses of popular music in campaign activities. The most notable instance came in the summer of 2016, when Trump ignited a controversy with the renowned British band, The Rolling Stones, by playing their hit song, “Start Me Up,” following his victory in the Indiana Republican primary. Shortly thereafter, Fran Curtis, the band’s publicist stated, “The Rolling Stones have never given permission to the Trump campaign to use their songs and have

24 Id. at 137.
25 Gunderson, supra note 19, at 140.
26 Id.
27 Id. (noting that McFerrin was a supporter of the Dukakis campaign and did not approve of Vice President Bush’s use of his song).
28 See infra notes 28, 30–40.
29 Alyssa Rosenberg, What Hillary Clinton’s Campaign Songs Say that She Can’t, WASH. POST (July 29, 2016), https://www.washingtonpost.com/news/act-four/wp/2016/07/29/what-hillary-clintons-campaign-songs-say-that-she-cant/?utm_term=.d191317c955b [https://perma.cc/W22P-EPKD]. Platten did an interview about the use of her song by the Clinton campaign, during which she stated, “I was a little scared at first just because I knew the song meant a lot to a lot of people – and politics, no matter how important, divide us. I was a little frightened about that. But I’m proud of how it’s been used. I don’t have any regrets about it.” Mikael Wood, Rachel Platten on Hillary Clinton’s Use of ‘Fight Song’: ‘I Was a Little Scared at First,’ L.A. TIMES (Nov. 8, 2016), http://beta.latimes.com/entertainment/music/la-et-ms-rachel-platten-fight-song-hillary-clinton-20161108-story.html [https://perma.cc/LBC9-GWGU].
30 See infra notes 30–40.
31 Id.
33 Id.
requested that they cease all use immediately.”34 Trump also had run-ins with Adele,35 Neil Young,36 Steven Tyler,37 and R.E.M.38 In each case, the Trump campaign was utilizing the music without permission from the author or the copyright owner.39 This growing trend of unauthorized use and increasing hostility between candidates and artists is one of the primary motivations for this Note.

The controversies have continued into Trump’s presidency. On October 27, 2018, hours after a mass shooting at Tree of Life synagogue in Pittsburgh, Pennsylvania that left eleven people dead, Trump played Pharrell Williams’ hit song “Happy” at a political event for the upcoming midterm elections.40 Two days later, through counsel, Pharrell sent President Trump a cease-and-desist letter, in which the artist indicated that the song was inappropriate given the circumstances, that he had not and would not grant Trump permission to use the song, and that the unauthorized use constituted copyright and trademark infringement.41 On November 4, 2018, Trump received criticism from two other artists, Rihanna and Axl Rose of Guns N’ Roses, for using their music at campaign events without permission.42

34 Id. Days after this explicit denial of permission, Trump used another one of the band’s songs, “You Can’t Always Get What You Want,” at a rally in West Virginia. Id.
37 Zaru & Acosta, supra note 32.
39 See supra notes 27–33.
41 Id.
C. What Are Moral Rights?

Before preceding any further, a brief introduction to the concept of moral rights is necessary. *Droit Moral*, or moral rights theory, is a European concept,43 predicated on the belief “that an artist’s relationship with his creation does not end upon its completion.”44 Unlike a factory worker who is responsible for the creation of a cog that is mass-produced, an artist is responsible for the creation of a work that is “created from [a] unique vision.”45 That unique relationship between the artist and their work makes the artist “vulnerable to certain personal harms.”46 An artist’s work is, in many ways, an extension of herself, and thus when her work is subject to action that might be considered prejudicial or harmful, the harm is not isolated to the work but translates to the artist as well.47 In this way, moral rights are fundamentally different from economic rights, which are alienable and transferable.48

Despite being fundamentally different from economic rights, moral rights, like economic rights, exist primarily to incentivize creation.49 Moral rights seek to “protect the artist’s creative process by protecting the artist’s control over that process and the finished work of art.”50 In a world where artists have confidence about the treatment they and their works will receive, they are more inclined to create.51

In Europe, four distinct moral rights are recognized: paternity, disclosure, withdrawal, and integrity.52 Presently in the United States, only two of these rights are recognized, integrity and paternity (otherwise known as the right of

44 *Id.* at 156.
45 *Id.* (describing how works of art are not fungible).
46 Susan P. Liemer, *Understanding Artists’ Moral Rights: A Primer*, 7 B.U. PUB. INT. L.J. 41, 42–43 (1998) (likening the harm suffered by artists whose moral rights are violated to individuals who have theirs rights of personality or personal civil rights violated).
47 *Id.* at 43 (“When an artist creates, she produces something that allows others a glimpse into her individual human consciousness. . . . The artist stands uniquely open to attack upon her psyche because she is so closely connected to the creative process and the creative product. . . . The artist’s reaction [to harm to her work] may even resemble her reaction to a physical injury to herself or someone very close to her.”).
48 *Id.* at 44 (“Moral rights, which protect a unique extension of the self, remain personal to the artist. The artist cannot sell them, give them away, or bequeath them.”).
49 *See id.*
50 *Id.*
51 *Id.*
52 Rosen, *supra* note 43, at 155. Moreover, France has created an additional “resale right,” which allows an artist to receive compensation each additional time the work is sold. *Id.* Some commentators do not conceive of the resale right as being a moral right due to its economic character, but it shares some similarities with moral rights in that it evinces a continuing relationship between the work and the artist, so it warrants mentioning here. *Id.* at 155–56.
attribution). The only existing moral rights law in the United States exists in the Visual Artists Rights Act (VARA), which creates a right of integrity and attribution for works of visual art. See 17 U.S.C. § 106 (2012) (providing authors of certain works the rights to “attribution and integrity”). VARA will be discussed in the greater detail in the following Parts. See infra notes 67–70.

For the sake of clarity, the right of disclosure allows artists to refuse to expose their work to the public before they feel it is satisfactory. Henry Hansmann & Marina Santilli, Authors’ and Artists’ Moral Rights: A Comparative Legal and Economic Analysis, 26 J. LEGAL STUD. 95, 96 (1997). The right of withdrawal, sometimes referred to as the right of retraction, allows artists to withdraw their work, even after it has left their hands. Id.

Id. at 99 (citing Berne Convention for the Protection of Literary and Artistic Works art. 6bis(1), Sept. 9, 1886, S. Treaty Doc. No. 99-27 [hereinafter Berne Convention] (as amended on Sept. 28, 1979)).

Id. at 130 (citing 17 U.S.C. § 106A).


Danoff, supra note 57, at 185.

See id. at 185–86. One of greatest benefits of membership in the Berne Union is that every signatory enjoys the copyright protections of all other signatories. Id. at 186.

Berne Convention, supra note 55, at art. 6bis(1).

Id. at art. 2(1).
requirements of Article 6bis. Congress ultimately concluded that the United States could meet its obligations under Article 6bis based on an existing “patchwork” of state and federal laws. This patchwork of remedies relies on three crucial threads. The first is Section 43(a) of the Lanham Act, which addresses false designations of origin and false descriptions and could, in some limited circumstances, be applied in attribution disputes over copyrighted works. The second includes a number of provisions of the Copyright Act, which protect authors’ exclusive rights in derivatives of their work, place limits on licensees’ rights to alter and arrange musical compositions, and allow for the termination of licenses and transfers. The third comprises various state and local laws addressing rights of publicity, contractual relations, fraudulent activity, unfair competition, defamation, and privacy.

In 1990, Congress implicitly acknowledged that this patchwork did not provide adequate protection of moral rights when it passed the Visual Artists Rights Acts (VARA). VARA grants waivable rights of attribution and integrity to authors of “works of visual art.” While VARA constitutes the most substantial commitment to moral rights by the United States to date, it still falls noticeably short of the obligations the United States incurred by becoming a signatory to the Berne Convention. The Act’s most significant shortcoming is evident in its title: it only applies to visual works, and not even all visual works but rather a few narrowly defined categories. VARA’s limited scope leaves authors of “musical compositions,” mentioned in Article 2(1) of the Berne Convention, without any moral rights protections.

---

64 Id. (citing 15 U.S.C. § 1125(a) (2012)).
65 Id. (citing 17 U.S.C. §§ 106(2), 115(a)(2), 203 (2012)).
66 Id. (citing H.R. Rep. No. 100-609, at 34 (1988)) (noting the important role that contract law plays for authors attempting to control aspects of their economic and moral rights).
67 See id. at 7871–72. See 17 U.S.C. § 106A (providing morals rights to authors of certain works in the form of attribution and integrity).
69 Id. § 101.
70 Id. According to the Act, a “work of visual art” is

(1) a painting, drawing, print, or sculpture, existing in a single copy, in a limited edition of 200 copies or fewer that are signed and consecutively numbered by the author, or, in the case of a sculpture, in multiple cast, carved, or fabricated sculptures of 200 or fewer that are consecutively numbered by the author and bear the signature or other identifying mark of the author; or (2) a still photographic image produced for exhibition purposes only, existing in a single copy that is signed by the author, or in a limited edition of 200 copies or fewer that are signed and consecutively numbered by the author.

Id.
The United States Copyright Office seems to have taken notice of these deficiencies. In January 2017, the Office issued a Notice of Inquiry, inviting public comment on the status of moral rights law in the United States. The Copyright Office stated that part of its goal was to determine “whether any additional protection is advisable in [the area of moral rights].” Prior to issuing the Notice, the Copyright Office organized a symposium that covered the history of moral rights, their value to authors, the extent to which they are protected by current law, and the effect of technological innovation on moral rights. Interestingly, the issue of unauthorized use of music in political campaigns was briefly addressed during the symposium.

The enactment of VARA in 1990 and the 2017 Notice of Inquiry highlight an important reality. At the time the United States became a signatory to the Berne Convention and even still today, the statutory schemes that predated the BCIA were and are inadequate to protect the moral rights of authors of musical works.

B. Contractual Protections

While statutory provisions give rise to more uniform protection of authors’ moral rights, authors are not left entirely helpless in the absence of such laws. In negotiating licensing agreements and contracts with record labels, some authors may be able to contract for their moral rights. American copyright law has given rise to a fairly complex music licensing regime. While a variety of licenses are provided for in this system, the most important among them are performance licenses, which allow the licensee to perform a work publicly.

According to the Copyright Act, “[t]o perform or display a work ‘publicly’

---

71 Notice of Inquiry, supra note 62, at 7874 (“The Copyright Office seeks public comments addressing how existing law, including provisions found in title 17 of the U.S. Code as well as other federal and state laws, affords authors with effective protection of their rights, equivalent to those of moral rights of attribution and integrity.”).

72 Id. at 7870.

73 Id. at 7874 (“As part of its effort to begin a dialogue about moral rights protections in the United States, the Copyright Office organized symposium entitled ‘Authors, Attribution, and Integrity: Examining Moral Rights in the United States,’ which was held on Apr. 18, 2016.”). The results of the symposium were mixed, with some participants remarking that the existing patchwork of laws does provide adequate protection and others indicating that the patchwork is under-inclusive and ineffective. Id.

74 Chris Castle et al., Authors, Attribution, and Integrity: New Ways to Disseminate Content and the Impact on Moral Rights, 8 GEO. MASON J. INT’L COM. L. 125, 137 (2016) [hereinafter Symposium]. Specifically, Scott Martin, Executive Vice President of Intellectual Property for Paramount Pictures, remarked that the risk of decontextualization that might run afoul of an artist’s moral rights is greater with musical works. Id. at 125, 137.

75 See Desai, supra note 17, at 4–10.

76 For a thorough discussion of music licensing in the United States, see id.

77 Id. at 7 (“The performance right is the most important right for songwriters and music publishers, with one-half of total music publishing returns arising from revenue associated with public performances.”).
means—(1) to perform or display it at a place open to the public or at any place where a substantial number of persons outside of a normal circle of a family and its social acquaintances is gathered . . . .”

Thus, public performances would include things like “radio and television broadcasts, the playing of a record, or the singing of a song.”

While performance rights are the most important to musicians and other licensors, policing public performances remains an incredibly difficult task. This enforcement problem has given rise to institutions known as “performing rights societies,” which assume the responsibility for safeguarding these rights. In the United States, the two most popular performing rights societies are the American Society of Composers, Authors and Publishers (ASCAP) and Broadcast Music, Inc. (BMI). An artist or other copyright owner can contract with one of these societies to sublicense his or her work to others. Individuals seeking to use the music in a public setting would pay the society for either an annual, blanket license or a per program license. Upon receiving payment for the license, the society then distributes royalties to the artist.

Performing rights societies provide a valuable resource to artists in policing their economic rights, but they are presently not well constituted to protect moral rights and may, in some circumstances, jeopardize them further. Thus, with respect to performing rights societies, artists are left in an uncomfortable position. They must join in order to protect their economic interests, but in doing

---

78 17 U.S.C. § 101; see also id.
79 Desai, supra note 17, at 7. But see 17 U.S.C. § 110 (describing limitations on the exclusive right to public performances, including exceptions for educational purposes, religious purposes, and public broadcasting).
80 Desai, supra note 17, at 7 (“[Musical work owners] would have a very difficult time policing performances in restaurants, stadiums, bars, or any other public place to retain their economic interest in the performance right.”).
81 Id. (explaining that the role of performing rights societies is to “license use of musical works, police their use, and distribute royalties based on use of these works”). If the society finds evidence of unauthorized uses, it is authorized by its members to bring suit against suspected infringers. Id. at 8.
82 See id. at 7 (listing ASCAP and BMI as performance rights societies in the United States). Outside the United States, the Society of European Stage Authors and Composers, now known only as SESAC, Inc., is a prominent performing rights society. Id.
83 Id. at 8.
84 Desai, supra note 17, at 8 (“A person or entity that desires to obtain a performance license from a performing rights society can pay an annual fee for a blanket license that allows the licensee to perform one or more titles in the society’s music catalog. A per program license is also available to television stations seeking a license from a performing rights society.”).
85 Id.
86 Id. at 8, 21 (“[A]ny musician would be wise to join a performance rights society, but in doing so, the musician allows another entity to decide in what context the public performance of his or her song occurs. A song could be played out of context in a stadium, convention center, bar, radio broadcast, or anywhere else ASCAP and BMI can license public performances.”).
so, they sacrifice control of the contexts in which their works are used. The societies would likely say these concerns are overblown, at least with respect to the use of music in political settings. According to guidelines issued by ASCAP, its performance licenses for most venues exclude uses at conventions and other political events. While that is technically true, the venues may also simply purchase a license specifically for conventions and other similar meetings.

Theoretically, an artist could contract for restrictions on how his or her works are licensed by a performing rights society, but presently, this does not appear to be a common, or even uncommon, occurrence. Additionally, artists would not have much leverage in requesting these restrictions. Artists cannot effectively police the use of their work without ASCAP or BMI, and these organizations likely would not be willing to accept the inclusion of specific restrictions on individual works because they would interfere with the uniform treatment the organizations accord to their entire catalog within their licenses.

That being said, there is some evidence suggesting that artists have sought greater protection for their moral rights in negotiations with record labels and publishing companies. In fact, artists typically request “marketing restrictions,” which prevent these entities from licensing their work for things like advertising or use in motion pictures. While some restrictions have become commonplace, if an artist has an interest in preventing any particular type of use, it becomes purely a matter of her ability to negotiate for such a restriction.

Most commentators, however, discount the effectiveness of these contractual safeguards. Chief among their concerns is a lack of awareness on behalf of disadvantaged authors who are so eager to sell their work that they might be willing to sign away their moral rights. This risk is substantially greater when the publishing company is allowed to use form purchase agreements that require an author to surrender his or her rights of attribution and integrity.

---

87 Id. at 21 (“A musician would act foolishly by not enrolling in one of these groups, and likely, a record company would act foolishly if it allowed an artist on its label to not join one of these groups.”).
90 See Symposium, supra note 74, at 135–36.
91 Id. at 135.
92 Id. at 135–36. (describing leverage dynamics between artists and record labels in negotiating for non-standard market restrictions).
93 See Ross, supra note 57, at 373–74.
94 See id. at 373.
95 Comment, Toward Artistic Integrity: Implementing Moral Right Through Extension of Existing American Legal Doctrines, 60 GEO. L.J. 1539, 1560 (1972) (describing how “commercial giants” in the music industry often utilize form contracts with granting clauses
In conclusion, with respect to contractual safeguards for moral rights, they seem to suffer from a few fatal flaws. First, contracting for them will inevitably decrease the value of the artists’ economic rights. Second, most artists would be precluded from negotiating for them due to insufficient bargaining power.

IV. BROWNE V. MCCAIN: ARGUING FOR THE POLITICIANS

In the past, some artists have employed these tactics and legal theories in attempts to curtail acts of decontextualization by political candidates and campaigns. However, these cases are rarely ever decided on the merits and instead are resolved in settlements out of court.96 Even so, some courts have been forced to address the relevance of the aforementioned legal doctrines in deciding preliminary motions.97 Hopefully, in reviewing Browne v. McCain, arguably the most famous instance of this type of litigation, the uncertainty in this area of law will become clearer in a few specific ways. First, both the parties and the courts must jump through tremendous hoops in an attempt to shoehorn the essence of these complaints into the legal frameworks Congress deemed sufficient to protect moral rights. Second, despite their great efforts, these primarily economic doctrines cannot effectively resolve moral rights questions. Finally, this case will provide an adequate summary of the types of defenses that have been and likely will be asserted by political candidates in these disputes, should the current legal regime remain unchanged.

In August of 2008, Senator John McCain was in the midst of a campaign for the presidency of the United States against Senator Barack Obama.98 In anticipation of a visit to Ohio by Obama, the Ohio Republican Party (ORP), acting on behalf of Senator McCain and the Republican National Committee (RNC), produced a web video attacking Senator Obama’s proposed energy policy.99 In keeping with the theme of the advertisement, the ORP added select clips from Jackson Browne’s iconic song “Running on Empty” to the advertisement.100 The ORP first published the advertisement on YouTube, but


97 See, e.g., Browne, 611 F. Supp. 2d at 1075 (C.D. Cal. 2009) (’Order Re Senator McCain’s Motion to Dismiss for Failure to State a Claim’).

98 Id. at 1076.


100 See sources cited supra note 99; see also JACKSON BROWNE, Running on Empty, on RUNNING ON EMPTY (Asylum Records 1977) (including lyrics such as “Running on-running on empty, Running on-running blind, Running on-running into the sun, But I’m running behind”).
it also aired on television and cable networks across Ohio and Pennsylvania.\textsuperscript{101} After the advertisement aired, “Browne [] received numerous inquiries expressing concern about Defendants’ use of [Running on Empty . . . ].”\textsuperscript{102} Browne then brought a suit in the United States District Court for the Central District of California against Senator McCain, the RNC, and the ORP alleging, among other things, (1) copyright infringement, (2) violation of the Lanham Act’s prohibitions on false association or endorsement, and (3) violation of California’s common law right of publicity.\textsuperscript{103}

A. Copyright Infringement

In July 2009, the parties settled this case out of court,\textsuperscript{104} but before a settlement was reached, the defendants filed a motion to dismiss all of Browne’s claims.\textsuperscript{105} In response to Browne’s allegations of copyright infringement, Senator McCain argued that the claim should be dismissed because the advertisement was covered by the fair use doctrine.\textsuperscript{106} Fair use was a common law doctrine that was codified in the Copyright Act; it exempts from infringement claims, uses of copyrighted works “for purposes such as criticism, comment, news reporting, teaching, . . . scholarship, or research.”\textsuperscript{107} The court ultimately concluded that it did not have enough facts at the time to make a proper ruling on fair use and consequently denied Senator McCain’s motion to dismiss the copyright infringement claim.\textsuperscript{108}

\begin{flushright}
\textsuperscript{101} Browne, 611 F. Supp. 2d at 1077 (“The commercial was also aired on and discussed by the national news media, including MSNBC.”).
\textsuperscript{102} Id.
\textsuperscript{103} Id.
\textsuperscript{105} Browne, 611 F. Supp. 2d at 1075.
\textsuperscript{106} Id. at 1077.
\textsuperscript{107} Id. (citing 17 U.S.C. § 107). In evaluating claims of “fair use,” courts consider the following factors: (1) purpose and character of the use, including whether the use is commercial or for non-profit educational purposes; (2) nature of the copyrighted work; (3) amount and substantiality of the portion of the work used in relation to the work as a whole; and (4) effect of the use on the potential market for or value of the work. 17 U.S.C. § 107 (2006). Interestingly, the fair use doctrine functions as an exception not only to the exclusive economic rights granted to copyright owners in § 106 but also to the moral rights granted to authors of visual works in § 106A.
\textsuperscript{108} Browne, 611 F. Supp. 2d at 1078.
\end{flushright}
B. Trademark Infringement

More enlightening was the court’s discussion of Browne’s claim of false endorsement under Section 43(a)(1)(A) of the Lanham Act.\(^{109}\) Senator McCain offered three arguments in his motion to dismiss: (1) the provisions of the Lanham Act only apply to commercial speech, not political speech; (2) the claim is barred by the First Amendment and artistic relevance test; and (3) Browne cannot, as a legal matter, establish a likelihood of confusion.\(^{110}\) The court did not find Senator McCain’s argument about commercial speech compelling, concluding that the statute’s “in commerce” language was not intended as a limit on the type of speech that the Lanham Act applies to.\(^{111}\) Relying on Second Circuit precedent, the court stated definitively that the Lanham Act applies to both commercial and noncommercial speech, including political speech.\(^{112}\)

The court then turned to Senator McCain’s argument that Browne’s claim should be dismissed because it is barred under the First Amendment.\(^{113}\) The First Amendment arguments were essentially an extension of Senator McCain’s noncommercial speech argument; since the advertisement is an act of noncommercial, political expression, it should not be constrained by trademark infringement claims.\(^{114}\) As the court already stated, the Lanham Act can be applied to noncommercial speech, and thus, without more compelling reasons, the First Amendment cannot function as a bar to Browne’s trademark infringement claims.\(^{115}\)

Senator McCain made one final argument that the trademark infringement claim should be dismissed because the advertisement clearly identifies its source as the ORP and thus there is no likelihood of confusion as to where it came from.

---

\(^{109}\) Id. at 1078–81.

\(^{110}\) Id. at 1078–79.

\(^{111}\) Browne, 611 F. Supp. 2d at 1079 ("The Act’s reference to use “in commerce” actually “reflects Congress’s intent to legislate to the limits of its authority under the Commerce Clause” to regulate interstate commerce. The interstate commerce jurisdictional predicate for the Lanham Act merely requires a party to show that the defendant’s conduct affects interstate commerce, such as through diminishing the plaintiff’s ability to control use of the mark, thereby affecting the mark and its relationship to interstate commerce.")

\(^{112}\) Id. at 1079 (“Indeed, the Act’s purpose of reducing consumer confusion supports application of the Act to political speech, where the consequences of widespread confusion as to the source of such speech should be dire.”).

\(^{113}\) Id. at 1080. Senator McCain also argued that the claim was barred under the “artistic relevance” test, a doctrine adopted by certain jurisdictions regarding the use of trademarks in artistic works. Id. The artistic relevance arguments will not be discussed here because of the test’s limited jurisdictional scope.

\(^{114}\) See Memorandum of Points and Authorities in Support of Defendant John McCain’s Motion to Dismiss, at 15–19; Browne v. McCain, 611 F. Supp. 2d 1062 (C.D. Cal. 2009).

\(^{115}\) Browne, 611 F. Supp. 2d at 1080.
However, as the court pointed out, the Senator’s argument misunderstands the confusion requirement of 15 U.S.C. § 1125(a)(1)(A). Even though a viewer may not be confused by the actual source of the advertisement, given the explicit identifier, there is a still a reasonable likelihood that a viewer might be confused as to whether Browne endorsed Senator McCain.

C. Right of Publicity

Browne’s final cause of action was a common law Right of Publicity Claim, which alleged, among other things, that Senator McCain’s “usurpation of Browne’s identity has caused and will cause irreparable harm to Browne that cannot be fully compensated by money.” Browne further alleged that, because of this reputational harm, he was entitled to injunctive relief prohibiting the Defendants from showing the advertisement in the future and punitive damages sufficient to deter similar conduct in the future. In response, Senator McCain filed an “Anti-SLAPP” (Strategic Lawsuits Against Public Participation) motion, which are designed to prevent lawsuits intended to chill the valid exercise of constitutional speech rights. California’s Anti-SLAPP statute deploys a burden shifting framework to adequately balance the interests of the parties. The initial burden is placed on the defendant to show that the plaintiff’s claims arise from an act made in connection with an issue of public

---

116 Id.
117 Id.; see 15 U.S.C. § 1125(a)(1)(A) (2012) (prohibiting uses of trademarks “in commerce . . . which [are] likely to cause confusion, or to cause mistake, or to deceive as to the affiliation, connection, or association of such person with another person, or as to the origin, sponsorship, or approval of his or her goods, services, or commercial activities.”).
118 Browne, 611 F. Supp. 2d at 1080–81. The court also took issue with Senator McCain’s failure to address what are known as the Sleekcraft factors, which are used in determining whether a likelihood of confusion exists and include

(1) the strength of the mark, (2) proximity or relatedness of the goods, (3) similarity of the marks, (4) evidence of actual confusion, (5) marketing channels used, (6) degree of care customers are likely to exercise in purchasing the goods, (7) defendant’s intent in selecting the mark, and (8) likelihood of expansion into other markets.

Id. (citing KP Permanent Make-Up, Inc. v. Lasting Impression I, Inc., 408 F.3d 596, 608 (9th Cir. 2005)).
119 Complaint at 9, Browne v. McCain, 611 F. Supp. 2d 1062 (C.D. Cal. 2009) (No. CV08-05334 RGK) [hereinafter Browne Complaint]. The prima facie case for a claim under California’s common law right of publicity requires a showing of “(1) the defendant’s use of the plaintiff’s identity; (2) the appropriation of the plaintiff’s name or likeness to defendant’s advantage commercially or otherwise; (3) lack of consent; and (4) resulting injury.” Browne, 611 F. Supp. 2d at 1069 (citing White v. Samsung Electronics Am., Inc., 971 F.2d 1395, 1397 (9th Cir. 1992)).
120 Browne Complaint, supra note 119, at 9.
121 Browne, 611 F. Supp. 2d at 1065, 1067.
122 Id.
interest.\textsuperscript{123} If the defendant meets their burden, the burden shifts to the plaintiff to establish a probability of success on the merits of his claim at trial.\textsuperscript{124} The court did find that the action that prompted the complaint related to an issue of public interest\textsuperscript{125} but ultimately concluded that Browne had shown a probability of success at trial.\textsuperscript{126} Thus, the court denied Senator McCain’s motion to dismiss the right of publicity claim.\textsuperscript{127}

D. Reflections on Browne

As mentioned earlier, the value of this case comes from its ability to illuminate the deficiencies of the so-called “patchwork” of laws that Congress deemed sufficient to account for authors’ moral rights. First, it makes clear that these economic-minded legal doctrines are poorly suited to the primarily non-economic interests of the parties in these suits.\textsuperscript{128} This is best reflected in the court’s discussion of Browne’s trademark infringement claim. The court notes that other circuits have determined that the Lanham Act applies to both commercial and noncommercial speech, but in resolving this dispute the court returns the most basic purposes of the Act and trademark law in general, to “reduce consumer confusion.”\textsuperscript{129} Thus, even if it is true that the Lanham Act was intended to regulate both commercial and noncommercial speech, its interest in doing so is still primarily, if not purely, economic.\textsuperscript{130} While trademark legislation that is economically-focused is not problematic in the area of traditional trademark disputes, that focus can become problematic when it is applied to non-economic claims.\textsuperscript{131} When the court is required to do this much work merely to show the applicability of the Lanham Act to the claim in question, it should be a strong indication that the Act is not well-suited to that claim.

The claim that seemed most similar to a moral rights claim was Browne’s right of publicity claim. A right of publicity claim acknowledges, at least implicitly, that the author’s identity is tied up in their work.\textsuperscript{132} At the very least, this indicates an awareness of the reputational harm that accompanies actions like those of Senator McCain. Even so, the right of publicity fails to adequately

\textsuperscript{123} Id.
\textsuperscript{124} Id. at 1067–68.
\textsuperscript{125} Id. at 1068–69.
\textsuperscript{126} Browne, 611 F. Supp. 2d at 1071.
\textsuperscript{127} Id. at 1073.
\textsuperscript{128} See Ross, supra note 57, at 364. (discussing the United States’ preoccupation with economic interests in intellectual property law).
\textsuperscript{129} Browne, 611 F. Supp. 2d at 1079.
\textsuperscript{130} See id.
\textsuperscript{131} See Ross, supra note 57, at 364.
\textsuperscript{132} Browne Complaint, supra note 119, at 9 (“Browne’s distinct and readily identifiable voice is widely known and closely associated with Browne. As such, Defendants’ unauthorized use of Browne’s voice in the Commercial invoked Browne’s identity in the minds of the public.”).
protect moral rights for a number of reasons. First, there is still a preoccupation with present and future economic harm.\textsuperscript{133} But more importantly than that, the right of publicity is a common law doctrine that can be subject to differences from state to state, with some providing stronger enforcement mechanisms than others,\textsuperscript{134} making the patchwork more vulnerable to holes than it would be in the presence of federal legislation.

V. URGENCY: THE TROUBLE OF DECONTEXTUALIZATION IN A TURBULENT POLITICAL CLIMATE

In addition to the clear deficiencies of the existing patchwork of protections of moral rights for musical works, the increasingly turbulent political climate underscores the need for a new moral rights doctrine for musical works. This Part describes the growing trend of political polarization and discusses how this trend exacerbates the risk of personal and reputation harm to artists resulting from decontextualization of music in political campaigns and settings.

Presently, there is a growing divide among the American public on the basis of political affiliation, with respect to fundamental political values, including the role of government, race relations, immigration, and environmental protection.\textsuperscript{135} For example, according to the Pew Research Center, political polarization reached then-record levels during the presidency of Barack Obama.\textsuperscript{136} However, in the first year of Donald Trump’s presidency, the political divide has grown even wider.\textsuperscript{137} Presently, a vibrant debate is taking

\begin{itemize}
  \item \textsuperscript{133} Id. ("Defendants usurpation of Browne’s identity has caused and will cause irreparable harm to Browne that cannot be fully compensated by money.").
  \item \textsuperscript{135} See THE PARTISAN DIVIDE ON POLITICAL VALUES GROWS EVEN WIDER, PEOW RES. CTR. (2017), http://www.people-press.org/2017/10/05/the-partisan-divide-on-political-values-grows-even-wider/ [https://perma.cc/C7L4-2Y7N] (finding that the magnitude of the divisions between Republicans and Democrats on key political issues “dwarfs other divisions in society, along such lines as gender, race and ethnicity, religious observance or education”).
  \item \textsuperscript{136} Id.
  \item \textsuperscript{137} Id.
\end{itemize}
place regarding the cause of this polarization, and whether it is a passing or permanent phenomenon.

Understanding the relationship between this political divide and reputational concerns for artists is slightly more complicated though. It begins with the understanding that the political party has become an increasingly important form of social identity. As might be expected, when political affiliation becomes a form of social identity, individuals begin to harbor positive feelings toward members of their party and similarly intense hostile feelings toward members of the alternative party. Furthermore, it is clear that these attitudes have increased in intensity in recent decades. The particularly unfortunate thing about these divides, commonly referred to as affective polarization, is that they are not constrained by social norms in the same ways as gender and race-based divides. In fact, the divide is often encouraged by

---

138 See, e.g., Lexi Boxel et al., Greater Internet Use Is Not Associated with Faster Growth in Political Polarization Among US Demographic Groups, 114 (40) PROC. NAT’L ACADEM. SCI. U.S.A. 10612, 10612 (2017) (arguing that greater Internet use is not the cause of increasing polarization); John V. Duca & Jason L. Saving, Income Inequality, Media Fragmentation, and Increased Political Polarization, 35 (2) CONTEMP. ECON. POL’Y 392, 392 (2016) (attributing polarization to fragmentation in American news media and income inequality); Kristin N. Garrett & Alexa Bankert, The Moral Roots of Partisan Division: How Moral Conviction Heightens Affective Polarization, BRIT. J. POL. SCI. (2018) (arguing that political polarization is caused and amplified in part by individuals’ willingness to moralize partisan political stances).


140 Shanto Iyengar & Sean J. Westwood, Fear and Loathing Across Party Lines: New Evidence of Group Polarization, 59 (3) AM. J. POL. SCI. 690, 690 (2014) (“While early studies viewed partisanship as a manifestation of other group affiliations . . . more recent work suggests that party is an important form of social identity in its own right . . ..”).

141 Id. at 692 (“[D]espite only mixed evidence of sharp ideological or partisan divergence in their policy preferences, Americans increasingly dislike people and groups on the other side of the political divide and face no social repercussions for the open expression of these attitudes.”); see also The Partisan Divide on Political Values Grows Even Wider: Partisan Animosity, Personal Politics, Views of Trump, PEW RES. CTR. (2017) (“Among members of both parties, the shares with very unfavorable opinions of the other party have more than doubled since 1994.”).

142 Iyengar & Westwood, supra note 140.

143 Id. (“Unlike race, gender, and other social divides where group-related attitudes and behavior are constrained by social norms . . . there are no corresponding pressures to temper disapproval of political opponents.”).
and reflected in national political discourse.\textsuperscript{144} As political affiliation has grown in importance as a form of social identity, what was once merely a political divide has morphed into a social divide.\textsuperscript{145} Thus, affiliation of oneself or one’s work with a particular political ideology has the capacity to seriously and negatively impact one’s social identity.

Political polarization does not, in and of itself, pose a risk to artists, though. It really only stands to intensify a negative response to their association with a particular ideology.\textsuperscript{146} There must be some sort of associating act that spurs the negative response. This is where decontextualization in the realm of political campaigns becomes important. When a candidate plays a song at their rally or a local political party uses a piece of music in a partisan advertisement, that association is created.\textsuperscript{147} As was noted by the court in \textit{Browne v. McCain}, observers of these practices could very well be confused as to whether the artist has endorsed the candidate or campaign.\textsuperscript{148} Upon the occurrence of that association, the artist has then been made a party, unwillingly, to a caustic political struggle that has the capacity to tangibly affect their social and economic interactions and permanently affect the meaning of their work.\textsuperscript{149} In light of these realities, the need for substantive moral rights for musical artists is clear.

\section*{IV. Proposed Solution}

Given these turbulent political dynamics and the increasing pressure they create for artists, a new moral rights framework for musical rights is necessary. Such a framework will require creating new statutory rights and addressing the contractual relationship between musicians, performing rights associations like ASCAP, and potential licensees. In doing so, a myriad of secondary issues will need to be addressed as well, including: contractual waiver of moral rights;

\begin{footnotesize}
\begin{itemize}
\item \textsuperscript{144} \textit{Id.}
\item \textsuperscript{145} \textit{Id.} ("[P]artisan cues now also influence decisions outside of politics and that partisanship is a political and social divide."); Christopher McConnell et al., \textit{Research: Political Polarization Is Changing How Americans Work and Shop}, \textsc{Harvard Bus. Review} (May 19, 2017), https://hbr.org/2017/05/research-political-polarization-is-changing-how-americans-work-and-shop [https://perma.cc/42ap-8ZRQ] (describing how political polarization and negative sentiments between members of different parties have begun to shape economic as well as political behavior).
\item \textsuperscript{148} \textit{Browne}, 611 F. Supp. 2d at 1081.
\item \textsuperscript{149} See LeDonne, \textit{supra} note 146.
\end{itemize}
\end{footnotesize}
reconciliation with existing statutes; appropriate remedies; and standards of review. Though this is an inherently difficult enterprise, it is imperative that Congress take action. This proposal will begin with a discussion of some preliminary issues, such as the appropriate philosophical and practical starting point and previous proposals by other commentators. It will then offer a potential legislative text. Finally, it will conclude with a discussion of how the proposed text addresses the primary and secondary issues mentioned above.

A. Previous Proposals

Previous commentators have proposed the creation of moral rights for musical works. Rajan Desai was one of the first to discuss the decontextualization of music and propose moral rights as a potential remedy for this problem. Desai was preoccupied with music licensing, and his proposal focused primarily on two changes to existing law. First among those changes is an amendment to the copyright code that would require artist consent for synchronization ("synch") licenses. This new right would be waivable, if the artist is comfortable doing so. The second prong of Desai’s proposal is meant to address the loss of control by artists over how their music is used in performances and involves the creation of a cause of action for artists "based on the moral right of integrity in order to control how their music is used and prevent the use of their music in a context they find objectionable.” With respect to remedies, Desai proposed injunctive relief against both licensors and licensees as the primary means of recourse and “monetary damages” if violators repeatedly violated an artist’s rights.

In the years since Desai’s original proposal, his licensing-focused approach has been subject to a fair amount of criticism. For example, Sarah Anderson objected to the lack of clarity in Desai’s proposal. The scheme, Anderson wrote, is entirely devoid of any clear standards that courts can use to assess alleged violations of an artist’s moral rights. Second, and more importantly, both rights created under his system would be subject to waiver. Anderson astutely points out that given the inherent disparity in bargaining power between artists and publishers, leaving open the possibility of waiver effectively destroys any

150 Desai, supra note 17, at 19–23.
151 Anderson, supra note 17, at 888–89.
152 Desai, supra note 17, at 21. “Synchronization, or ‘synch,’ licenses . . . allo[w] the licensee to use (or synchronize) a musical work in an audiovisual work, such as a motion picture or television show.” Id. at 9.
153 Id. at 21.
154 Anderson, supra note 17, at 888–89. This right would be waivable as well. Id.
155 Desai, supra note 17, at 22–23.
156 See, e.g., Anderson, supra note 17, at 890–93.
157 Id. at 890.
158 Id. at 891–92.
rights that might have been created. These critiques make clear that any new proposal would need to contain clearer standards and rights that are not entirely subject to contractual waiver.

B. Finding a Proper Starting Point

In crafting this new proposal, there are a number of clear potential foundations on which to build. Among the options would be the Berne Convention, the Visual Artists Rights Act, and the moral rights provisions of some foreign jurisdictions, like France. For these purposes, the Berne Convention appears to be the obvious choice. Article 2 of the Berne Convention already includes “musical compositions with or without words” in its definition of protected works. This inclusion is an indication that the drafters of the moral rights provisions in Article 6bis were mindful of the special challenges presented by musical works and still considered them compatible with the rights conferred. As will be discussed below, that mindfulness is reflected in certain distinctions between the Berne Convention and these other frameworks, which ultimately makes the Berne Convention more advantageous.

While it does not identify them as such, the Berne Convention creates both a right of attribution and a right of integrity. Substantively, these rights are very similar to those granted to authors of visual works under VARA. However, there are some important differences, namely the catch all phrases at the end of the lists describing changes that might constitute a violation of an author’s rights. The Berne Convention’s inclusion of “other derogatory action” in addition to distortion, mutilation, and modification is valuable for the protection of musical works from decontextualization. All three of those terms carry with them a connotation of more tangible alteration of a work, which would seem to place decontextualization outside the scope of actionable conduct. However, “other derogatory action” is an incredibly broad term, sufficiently open to interpretation to cover acts of decontextualization. The Berne Convention provides this greater coverage, while still being functionally

---

159 Id. at 892.
160 Berne Convention, supra note 55, at art. 2(1).
161 Id. at art. 6bis(1).
162 Compare id. at art. 6bis(1) (“[T]he author shall have the right to claim authorship of the work and to object to any distortion, mutilation or other modification of, or other derogatory action in relation to, the said work, which would be prejudicial to his honor or reputation.”), with 17 U.S.C. § 106A(a) (1990) (“[T]he author of a work of visual art shall have the right to claim authorship of that work . . . and . . . to prevent . . . intentional distortion, mutilation, or other modification of that work which be prejudicial to his or her honor or reputation . . . .”).
163 Compare Berne Convention, supra note 55, at art. 6bis(1) (including “other derogatory action” that would be prejudicial to the author’s honor or reputation), with 17 U.S.C. § 106A(a) (including “other modification” that would be prejudicial to the author’s honor or reputation).
compatible with the rights created by VARA and the jurisprudence that has developed since its enactment.

In addition to the scope of actionable conduct, Anderson has pointed out some compelling reasons why extending VARA to cover musical works would not resolve the issue of decontextualization.164 First, Congress intended VARA to provide protection for artists’ professional rather than personal reputations.165 Second, VARA was primarily designed for, and expressly limited to, “works created in single copies or in limited editions.”166 This limitation would seem to exclude musical works due to the fact that they are essentially infinitely reproducible.167 Finally, VARA contains a number of exceptions for conduct that would normally be considered violative of the right of integrity.168 One such exception is for public presentation. The exception states that the “modification of a work that is the result of ‘the public presentation . . . of the work is not a destruction, distortion, mutilation, or other modification . . . unless the modification is caused by gross negligence.’”169 While revising the definition of works covered by VARA might seem like the simplest and most expeditious method for extending moral rights to musical works, a closer look at the nuances of the Act reveal that it would not be a sound starting point for the creation of moral rights for musical works.

Commentators often point to France’s highly developed and progressive moral rights regime as an exemplar.170 The French moral rights regime comprises four distinct rights.171 In addition to the rights of attribution (droit à la paternité) and integrity (droit au respect de l’oeuvre), France recognizes two other moral rights. The droit de divulgation allows an artist to decide whether to publish, and the droit de retrait ou de repentir allows an author to withdraw or modify a work that has already been published.172 Together, the extent of the control created by these four rights would be unheard of in the United States and seem almost absurd given the American preoccupation with economic rights.173 Any attempt to translate those rights to American jurisdictions, given the

164 Anderson, supra note 17, at 893–97.
165 Id. at 894. Any claim involving decontextualization, particularly of the form discussed in this note, would necessarily involve concerns about the artist’s personal reputation, but Congress expressly disclaimed any interest in resolving cases where “the general character of the plaintiff is at issue,” deeming it “irrelevant.” Id. (citing H.R. REP. No. 101-514, at 15 (1990), reprinted in 1990 U.S.C.C.A.N. 6915, 6925).
166 Id. at 894; see 17 U.S.C. § 101 (explaining that works of visual art “exist[] in single copy” or “in limited edition”).
167 Anderson, supra note 17, at 894–95.
168 Id. at 895.
169 Id.
171 Id. at 3.
172 Id.
173 Ross, supra note 57, at 364.
philosophical disparities between the two countries, would be difficult to reconcile with existing law and hard to justify from practical standpoint.

For the foregoing reasons, the substantive rights described in the Berne Convention will serve as the basis for this proposal. Even so, it will draw significantly from parts of VARA in order to create a moral rights regime for musical works that is compatible with that of visual works and easily interpreted in light of American jurisprudence. Article 6bis, though, leaves unaddressed some of the significant doctrinal issues discussed above, namely contractual waiver, standards of review, and remedies. Those issues will be addressed by the proposed legislative text in the next subpart. Following the proposed text will be an explanation of how it addresses those remaining questions. Finally, this part will conclude with a discussion of how this proposed legislation would reconcile with existing moral rights protections in the United States and how it is well-tailored to address the forms of decontextualization discussed in this note.

C. Proposed Legislative Text

Below is a proposed statutory text that would create rights for authors of musical works sufficient to guard against the harms of decontextualization. In addition to creating these rights, it contains provisions that address contractual modification of those rights and enforcement mechanisms.

Rights of authors of musical works to attribution and integrity:

(a) Rights of attribution and integrity--The author of a musical work--

(1) Shall, independent of their economic rights, have the right--

(A) to claim authorship of the work, and

(B) to prevent the use of his or her name as the author of any musical work which he or she did not create;

(2) Shall have the right to prevent any distortion, mutilation or other modification of, or other derogatory action in relation to, the said work, which would be prejudicial to his or her honor or reputation.

(b) Scope and exercise of rights--Only the author of a musical work has the rights conferred by subsection (a) in that work, whether or not the

174 Id. at 369.
175 See Berne Convention, supra note 57, at art. 6bis(1).
176 The Berne Convention does not contain this specific language. It is one of the ways in which the provisions of VARA go beyond the substantive rights described in the Berne Convention. See 17 U.S.C. § 106A(a)(1)(B) (1990). However, this extension of the right of attribution is not, in any way, contradictory to the provisions of the Berne Convention.
177 When describing the right of integrity, the Berne Convention states that the artist has the right to “object to” any distortion, mutilation, modification, or other derogatory action. Berne Convention, supra note 55, at art. 6bis(1). This language is noticeably softer than the “prevent” language used in VARA. See 17 U.S.C. § 106A(a). To reinforce the strength of the right created under this provision, the prevent language was substituted for the object language.
author is the copyright owner. The authors of a joint work are co-
owners of the rights conferred by subsection (a) in that work.

(c) Transfer and waiver. The rights conferred in subsection (a)--
(1) May not be transferred or waived through a written instrument
signed by the author.\textsuperscript{178}
(2) Ownership of the rights conferred in subsection (a) with respect to
a musical work is distinct from ownership of any copy of that work, or
of a copyright or any exclusive right under a copyright in that work.
Transfer of ownership, or of a copyright or any exclusive right under a
copyright, shall not constitute a waiver of the rights conferred by
subsection (a).\textsuperscript{179}

(d) Duration of rights. With respect to musical works created on or after
effective date of this Act, the rights conferred by subsection (a) shall
endure for a term consisting of the life of the author.

(e) Remedies. Any court having jurisdiction of a civil action arising under
this Act may--
(1) grant temporary and final injunctions on such terms as it may deem
reasonable to prevent or restrain infringement of the rights conferred
therein;
(2) grant compensatory damages in accordance with any reputational
harm suffered by the plaintiff; and
(3) award punitive damages as needed to vindicate the rights of authors
of musical works.

The following subparts contain more thorough explanations how these
statutory provisions will resolve lingering concerns about the creation and
enforcement of moral rights for authors of musical works.

D. Contractual Waiver

Subsection (c) of this proposal is arguably its most important and
controversial element. When Desai attempted to provide a solution for the
problem of decontextualization, his proposal made the artists’ rights
waivable.\textsuperscript{180} However, as others have pointed out, reliance on waivable rights
in an industry where there are significant disparities in bargaining power in the

\textsuperscript{178} This provision is one of the most important and substantial diversions from VARA.
See 17 U.S.C. § 106A(e) (providing that moral rights “may not be transferred, but those
rights may be waived if the author expressly agrees to such waiver in a written instrument
signed by the author.”).

\textsuperscript{179} This exact provision appears in VARA. Id. § 106A(e)(2). However, it contains an
explicit exception allowing an author to transfer of moral rights through written agreement.
Id. Effectively, it is a statutory acknowledgement of the separability of moral and economic
rights and the inalienable nature of moral rights. See supra notes 42–47 and accompanying
text.

\textsuperscript{180} Desai, supra note 17, at 19–23.
negotiation of marketing and licensing agreement is an ineffectual approach.\textsuperscript{181} While this would certainly be a substantial diversion from existing moral rights doctrines, it is necessary in order create functional protections for musical works. Desai even acknowledges that it would be difficult for most artists to seek protection through contractual provisions because they are often so desperate to be published that they will make significant concessions to ensure a recording deal.\textsuperscript{182} This problem is particularly acute in the case of newer musicians who lack significant prior success.\textsuperscript{183} While there may be some instances where sufficiently powerful musicians are able to negotiate substantial moral rights protections in their licensing and publishing agreements,\textsuperscript{184} statutory limitations are necessary to constrain publishers and performance rights societies from extracting rights from artists.

E. Standards of Review

Taken as a whole, VARA is not suitable for extension to musical works, but it still holds tremendous value in for musical works in that it has given rise to a substantial body of case law on moral rights.\textsuperscript{185} Having been in place for nearly thirty years, VARA has been discussed, at least in part, by most federal circuit courts.\textsuperscript{186} Courts have had the opportunity to discuss the meaning of specific provisions of VARA.\textsuperscript{187} But more importantly, courts have had a chance to grapple with the values and principles underlying moral rights doctrine.\textsuperscript{188}

Thus, courts will not only have VARA precedents to draw on for certain factual situations but they will also generally be more comfortable interpreting

\textsuperscript{181} See supra notes 149–51 and accompanying text.
\textsuperscript{182} Desai, supra note 17, at 18.
\textsuperscript{183} Id.; Symposium, supra note 74, at 131–32.
\textsuperscript{184} Symposium, supra note 74, at 136.
\textsuperscript{185} See, e.g., Kelley v. Chi. Park Dist., 635 F.3d 290, 303 (7th Cir. 2011) (explaining that a local garden did not have the type of authorship and stable fixation necessary to qualify for protection under VARA); Mass. Museum of Contemp. Art Found., Inc. v. Büchel, 593 F.3d 38, 41–42 (1st Cir. 2010) (discussing whether unfinished works qualify for protection under VARA); Phillips v. Pembroke Real Estate, Inc., 459 F.3d 128, 129 (1st Cir. 2006) (explaining that VARA does not provide protection for site-specific works); Pollara v. Seymour, 344 F.3d 265, 265–66 (2d Cir. 2003) (discussing how a hand-painted banner that commissioned to draw attention to a lobbying effort falls outside the scope of VARA).
\textsuperscript{186} See cases cited supra note 185.
\textsuperscript{187} See, e.g., Carter v. Helmsley-Spear, Inc., 71 F.3d 77, 81 (2d Cir. 1995) (“The right of integrity allows the author to prevent any deforming or mutilating changes to his work . . . .”).
\textsuperscript{188} See, e.g.,

The rights spring from a belief that an artist in the process of creation injects his spirit into the work and that the artist’s personality, as well as the integrity of the work, should therefore be protected and preserved. . . . Because they are personal to the artist, moral rights exist independently of an artist’s copyright in his or her work.

\textit{Id.}
the substantive provisions of this new legislation, given that the rights conferred under it are so similar to those created under VARA.189

F. Remedies

The inclusion of a particularized remedy section might seem somewhat unusual, given that violations of other rights associated with copyrightable works are consolidated in one chapter of Title 17.190 However, given the unique nature of the works in question, and that the goal for this note is to propose the best possible solution for decontextualization of musical works, adjusting and adding to traditional copyright remedies is necessary. Injunctive relief is both a traditional and unobjectionable remedy, necessary to curtail any present or impending violations of an author’s rights.191 Compensatory damages are a common remedy for copyright violations, but they are typically meant to address economic losses.192 The damages described in this proposal, though, are non-economic and intended to compensate the plaintiff for reputational harm in the same way plaintiffs in defamation suits are compensated for reputational harm.193 Given that the rights in question here are non-economic, the inclusion of non-economic compensatory damages in place of economic compensatory damages is a reasonable approach and necessary to vindicate the rights of musicians.

The real potential sticking point with respect to remedies in this proposal, however, will be the inclusion of punitive damages. Punitive damages are inherently controversial topic, and many parties are naturally averse to them.194 As such, their inclusion in a statutory proposal to vindicate a set of rights that are neither well-known nor well-settled is naturally controversial. Punitive

---

189 See supra notes 167–68 and accompanying text.
191 See, e.g., 17 U.S.C. § 502 (2006). Under the Copyright Act, injunctions may be granted in order to “prevent or restrain” copyright infringement, indicating that they are used to address both presently occurring and future violations. See id.
192 See 17 U.S.C. § 504 (2006) (“The copyright owner is entitled to recover the actual damages suffered by him or her as a result of the infringement, and any profits of the infringer that are attributable to the infringement and are not taken into account in computing the actual damages.”).
193 50 AM. JUR. 2D, Libel and Slander § 353 (2017) (stating that defamation suit plaintiffs are often entitled to “general damages, or those which the law presumes to be the natural, proximate, and necessary result of the publication and which represent such effects of the defamation as loss of reputation, shame, mortification, and hurt feelings”).
194 See generally Dan B. Dobbs, Ending Punishment in “Punitive” Damages: Deterrence Measured Remedies, 40 ALA. L. REV. 831, 834 (1989) (arguing that punitive damages are not subject to measurement or effective limits); Cass R. Sunstein et al., Assessing Punitive Damages (With Notes on Cognition and Valuation in Law) (Coase-Sandor Inst. for Law & Econ. Working Paper No. 50, 1997) (describing the award of punitive damages as arbitrary and unpredictable).
damages are often valued for their deterrent effect.\textsuperscript{195} The harm that inspired this note, the decontextualization of music in political settings, is particularly difficult to control. Injunctive relief, while adequate to constrain the unauthorized uses of music, comes with inherent delays. Plaintiffs must not only jump through the procedural hurdles of filing a claim in court, which would require that they be notified of the unauthorized use, but also be able to demonstrate a “likelihood of success on the merits,”\textsuperscript{196} which would be difficult in a relatively unsettled area of law. Furthermore, injunctive relief only constrains future harm, which in cases where there has already been an unauthorized use, may be wholly ineffective. Therefore, the best and perhaps only way to resolve the issue of unauthorized uses of music is to deter the practice altogether through the use of punitive damages.

G. Reconciliation with Existing Moral Rights Doctrine

Presently, the biggest concern with respect to reconciliation involves making sure that this new legislation would not disrupt the existing protections for visual works in VARA. The substantive rights created under this new act are easily recognizable as very similar to those in VARA,\textsuperscript{197} which should mean that the judicial interpretations of those rights would be undisturbed. The most substantial differences between VARA and this new legislation relate to more ancillary issues, such as contractual waiver\textsuperscript{198} and remedies.\textsuperscript{199} While not insignificant, these differences should not interfere with or complicate the enforcement of rights created under VARA.


\textsuperscript{196}O’Toole v. O’Connor, 802 F.3d 783, 788 (6th Cir. 2015) (describing a four-part test for injunctive relief that requires the plaintiff to show (1) a likelihood of success on the merits, (2) that she will likely suffer irreparable harm without the injunction, (3) that the balance of equities favors her, and (4) that injunctive relief would serve the public interest).

\textsuperscript{197}See supra notes 67–69 and accompanying text. It should be emphasized again, though, that the right of integrity created under this new legislation is somewhat broader than that created under VARA due to the inclusion of the “other derogatory action” language. See supra note 159 and accompanying text.

\textsuperscript{198}See supra notes 180–84 and accompanying text.

\textsuperscript{199}See supra notes 190–96 and accompanying text.
H. Resolving Decontextualization of Music in Political Settings

The foregoing proposal was created in response to and with the intention of resolving decontextualization of music in political settings. To that end, one of its most important characteristics remains the inclusion of the “other derogatory action” language from Article 6bis of the Berne Convention in its articulation of the right of integrity. Looking at the other terms that precede that catch-all phrase; distortion, mutilation, and modification; it could be argued that playing a particular musical work in a political context would not be covered by the Act. Even the broadest of the three, modification, would need to be stretched to its logical limits to cover this particular type of conduct.

After creating suitable substantive rights, the proposal’s next most important quality has to be the statutory prohibition against waiver of those rights through written agreements. Contractual relationships, from record deals to licensing agreements, are utilized heavily in the music industry.200 Given the serious disparities in bargaining power between most artists and the entities with which they negotiate these contracts, a statutory limit on the waiver of an artist’s moral rights is indispensable.201 Otherwise, the creation of those rights would be a pointless enterprise.

Finally, in order for any right to be valuable, it must carry a legitimate prospect of enforcement. To that end, the proposal utilizes a three-tiered remedy structure, which provides for injunctive relief, non-economic relief, and punitive damages, to curtail unauthorized uses and, to the extent possible, restore the artist to a point preceding the violation of their rights. Injunctive relief is necessary to stop both known and prospective violators, thus preventing or confining the damage done to the artist’s work and reputation.202 Non-economic compensatory damages, while not a perfect solution, provide a means of restoring the artists to a point prior to the violation.203 And given the serious, persistent, and omnipresent threat of decontextualization, punitive damages will be an important part of enforcing any moral rights legislation by deterring potential bad actors.204

VII. CONCLUSION

Presently there is an absence of suitable doctrines to resolve the issue of unauthorized uses of music in political campaigns. Establishing a functional moral rights doctrine that applies to musical works should go a long way toward fixing this problem. Attempting to mold artists’ complaints to fit within longstanding intellectual property doctrines simply is not a feasible approach.

200 See Desai, supra note 17, at 3–11.
201 Id. at 8, 11; Symposium, supra note 74, at 37.
202 See supra note 191 and accompanying text.
203 See supra notes 192–93 and accompanying text.
204 See supra notes 194–95 and accompanying text.
moving forward.205 Furthermore, relying on the ability of authors to contract for their moral rights simply does not account for the interests of authors who lack significant bargaining power.206 If the United States ever wants to live up to its obligations under the Berne Convention, it must commit to a shift in its paradigm regarding the rights of authors of copyrightable works.

The true value of this Note may come not from its proposed statutory reforms but rather from its contribution to that effort to raise awareness of moral rights. As was noted in the Copyright Office’s Notice of Inquiry, there is a general lack of awareness on behalf of both artists and art consumers of the doctrine of moral rights.207 A statutory remedy is helpful only if people are aware and understand what it is designed to accomplish. Such being the case, if this note can contribute to the public discourse on and help raise awareness of moral rights, it may have some value independent of its proposed legislative remedy.

205 See supra notes 124–27 and accompanying text.
206 See supra notes 75–95 and accompanying text.
207 Notice of Inquiry, supra note 62, at 7872 (indicating that the Copyright office was unable to assess some of VARA’s provisions because artists and art consumers were generally unaware of moral rights).