BERKELEY TECHNOLOGY LAW JOURNAL

VOLUME 38, ISSUE 2

2023

Pages

609–864

Production: Produced by members of the *Berkeley Technology Law Journal.* All editing and layout done using Microsoft Word.

Printer: Joe Christensen, Inc., Lincoln, Nebraska.
Printed in the U.S.A.
The paper used in this publication meets the minimum requirements of American National Standard for Information Sciences—Permanence of Paper for Library Materials, ANSI Z39.48—1984.

Berkeley Technology Law Journal
University of California
School of Law
3 Law Building
Berkeley, California 94720-7200
editor@btlj.org
https://www.btlj.org

BERKELEY TECHNOLOGY LAW JOURNAL

VOLUME 38 ISSUE 2 2023

ARTICLES

SUBSCRIBER INFORMATION

The *Berkeley Technology Law Journal* (ISSN1086-3818), a continuation of the *High Technology Law Journal* effective Volume 11, is edited by the students of the University of California, Berkeley, School of Law and is published in print three times each year (March, September, December), with a fourth issue published online only (July), by the Regents of the University of California, Berkeley. Periodicals Postage Rate Paid at Berkeley, CA 94704-9998, and at additional mailing offices. POSTMASTER: Send address changes to Journal Publications, Law Library, LL123 South Addition, Berkeley Law, University of California, Berkeley, Berkeley, CA 94720-7210.

Correspondence. Address all correspondence regarding subscriptions, address changes, claims for non-receipt, single copies, advertising, and permission to reprint to Journal Publications, Law Library, LL123 South Addition, Berkeley Law, University of California, Berkeley, Berkeley, CA 94720-7210; (510) 643-6600; JournalPublications@law.berkeley.edu. *Authors*: see section titled Information for Authors.

Subscriptions. Annual subscriptions are $65.00 for individuals and $85.00 for organizations. Single issues are $30.00. Please allow two months for receipt of the first issue. Payment may be made by check, international money order, or credit card (MasterCard/Visa). Domestic claims for non-receipt of issues should be made within 90 days of the month of publication; overseas claims should be made within 180 days. Thereafter, the regular back issue rate ($30.00) will be charged for replacement. Overseas delivery is not guaranteed.

Form. The text and citations in the *Journal* conform generally to THE CHICAGO MANUAL OF STYLE (16th ed. 2010) and to THE BLUEBOOK: A UNIFORM SYSTEM OF CITATION (Columbia Law Review Ass'n et al. eds., 21st ed. 2020). Please cite this issue of the *Berkeley Technology Law Journal* as 38 BERKELEY TECH. L.J. ___ (2023).

BTLJ ONLINE

The full text and abstracts of many previously published *Berkeley Technology Law Journal* articles can be found at https://www.btlj.org. Our site also contains a cumulative index; general information about the *Journal*; the *BTLJ Blog*, a collection of short comments and updates about new developments in law and technology written by BTLJ members; and *BTLJ Commentaries*, an exclusively online publication for pieces that are especially time-sensitive and shorter than typical law review articles.

INFORMATION FOR AUTHORS

The Editorial Board of the *Berkeley Technology Law Journal* invites the submission of unsolicited manuscripts. Submissions may include previously unpublished articles, essays, book reviews, case notes, or comments concerning any aspect of the relationship between technology and the law. If any portion of a manuscript has been previously published, the author should so indicate.

Format. Submissions are accepted in electronic format through Scholastica online submission system. Authors should include a curriculum vitae and resume when submitting articles, including his or her full name, credentials, degrees earned, academic or professional affiliations, and citations to all previously published legal articles. The Scholastica submission website can be found at https://btlj.scholasticahq.com/for-authors.

Citations. All citations should conform to THE BLUEBOOK: A UNIFORM SYSTEM OF CITATION (Columbia Law Review Ass'n et al. eds., 21st ed. 2020).

Copyrighted Material. If a manuscript contains any copyrighted table, chart, graph, illustration, photograph, or more than eight lines of text, the author must obtain written permission from the copyright holder for use of the material.

SPONSORS
2023–24

The *Berkeley Technology Law Journal* and the Berkeley Center for Law & Technology acknowledge the following generous sponsors of Berkeley Law's Law and Technology Program:

ALLEN & OVERY LLP

ARENTFOX SCHIFF LLP

AXINN, VELTROP & HARKRIDER LLP

BAKER BOTTS L.L.P.

CHARLES RIVER ASSOCIATES

COOLEY LLP

CORNERSTONE RESEARCH

COVINGTON & BURLING LLP

CROWELL & MORING LLP

DESMARAIS LLP

DLA PIPER

DURIE TANGRI LLP

FENWICK & WEST LLP

FISH & RICHARDSON P.C.

GENENTECH, INC.

GEN LAW FIRM

GIBSON, DUNN & CRUTCHER LLP

GILEAD SCIENCES, INC.

GOODWIN PROCTER LLP

GREENBERG TRAURIG, LLP

GTC LAW GROUP PC

HAYNES AND BOONE, LLP

HOGAN LOVELLS

IRELL & MANELLA LLP

JINGTIAN & GONGCHENG

JONES DAY

KEKER, VAN NEST & PETERS LLP

KILPATRICK TOWNSEND & STOCKTON LLP

KING & SPALDING LLP

KING & WOOD MALLESONS

SPONSORS
2023–24

KIRKLAND & ELLIS LLP

KNOBBE MARTENS

LATHAM & WATKINS LLP

MARKS & CLERK

MCDERMOTT WILL & EMERY

MICROSOFT

MORGAN, LEWIS & BOCKIUS LLP

MORRISON & FOERSTER LLP

MUNGER, TOLLES & OLSEN LLP

OCEAN TOMO

ORRICK HERRINGTON & SUTCLIFFE LLP

PAUL HASTINGS, LLP

QUALCOMM TECHNOLOGIES, INC.

QUINN EMANUEL URQUHART & SULLIVAN, LLP

ROBINS KAPLAN LLP

ROPES & GRAY LLP

SIDLEY AUSTIN LLP

TENSEGRITY LAW GROUP LLP

VAN PELT, YI & JAMES LLP

VIA LICENSING CORPORATION

WANHUIDA INTELLECTUAL PROPERTY

WEIL, GOTSHAL & MANGES LLP

WESTERN DIGITAL CORPORATION

WHITE & CASE LLP

WILMER CUTLER PICKERING HALE AND DORR LLP

WILSON SONSINI GOODRICH & ROSATI

WINSTON & STRAWN LLP

WOMBLE BOND DICKINSON

BOARD OF EDITORS
2023–24

Executive Board

BOARD OF EDITORS
2023–24

Editorial Board

Articles Editors

GULNUR BEKMUKHANBETOVA
XUEJIAO CAO
ALEX CHOI
MICHELLE D'SOUZA
GARIMA KEDIA
JOSHUA KUHN
MARLEY MACAREWICH
JOSH MIMURA
BANI SAPRA
SANDEEP STANLEY
BHAVIA SUKHAVASI
NICOLE ZEINSTRA

Notes & Comments Editor
WILLIAM CLARK

Student Publication Editors
MAYA DARROW
JOHN MOORE

Submissions Editors
WILLY ANDERSON
JENNIFER CHENG
VERNON ESPINOZA VALENZUELA
HYEMI PARK

Technical Editors
ASHLEY FAN
EDLENE MIGUEL
BEN PEARCE
ANDREW STONE
CARESSA TSAI

Alumni Relations Editor
EMMA BURKE

External Relations Editor
HUNTER KOLON

Member Relations Editors
JAEYOUNG CHOI
CYRUS KUSHA

Podcast Editors
ERIC AHERN
JULIETTE DRAPER
MEGHAN O'NEILL

Symposium Editors
MARIT BJORNLUND
NICOLE BOUCHER

Production Editors
BEN CLIFNER
SARAH DAVIDSON
KELSEY EDWARDS
ANGELICA KANG
LAUREL MCGRANE

Web & Technology Editors
EMILY WELSCH
LISA YOUNES

LLM Editor
FERNANDA GONZAGA

MEMBERSHIP
2023–24

Members

AYESHA ASAD	AISHWARYA ATHAVALE	CHELSEA BENEDIKTER
DAVID BERNSTEIN	ROMA BHOJWANI	NICOLE BLOOMFIELD
HANNAH BORROWS	OSMANEE CAILLEMER	ALYSON CHIE
ANGELA CHUNG	PETER COE	TIM DABROWSKI
EVELINA DASH	VIVIANA PAOLA DIAZ BAQUERO	HALA EL SOLH
IMAN ESLAMI	SARAH FAROOQ	MAX FRIEND
NADIA GHAFFARI	MRINALINI GOYAT	DAN GRUSHKEVICH
RUI HAN	ANNIKA HANSEN	MARIA HARRAST
ANGELO HERBOSA	MENGRUO HUANG	DYLAN HUGHES
MARIA LUISA ILHARREBORDE	MONICA JEUNG	CORINNE JOHNSTON
YSAMEEN JOULAEE	AARON KAMATH	NAT KAVALER
SRISHTI KHEMKA	TYLER KOTCHMAN	JOSEPH KYBURZ
GAURAV LALSINGHANI	JOSHUA LEE	IRENE LI
KARISSA LIN	WANYI LIN	SARAH LUNT
LILLY MAXFIELD	ZAC MCPHERSON	MAXWELL MELNIK
MARIA MILEKHINA	KIYAN MOHEBBIZADEH	SEAMUS MORIARTY
LEA MOUSTAKAS	GRACIE MURPHY	SAIAISWARYA NAGENDRA

MEMBERSHIP
2023–24

Members (continued)

NIYATI NARANG	NICHOLAS NAVARRO	TUONG-VI NGUYEN
ANTONY NOVAK	YUNFEI QIANG	DEVANGINI RAI
UDAYVIR RANA	SANIDHYA RAO	EMILY REHMET
DELARAI SADEGHITARI	KARINA SANCHEZ	ABBY SANDERS
JULIAN SANGHVI	MASON SEDEN-HANSEN	DHANYA SETLUR KRISHNAN
JACOB SHOFET	AATMAN SHUKLA	GAYATHRI SINDHU
VANSHIKA SINGH	ANKUR SINGHAL	MATT SIOSON
SARAH SISNEY	COLIN STACKPOOLE	HAILEY STEWART
LORENZ STRUB	LESLEY SUN	AMANDA SUZUKI
TRISTAN THREATT	ERIC TING	ITAI TISMANZKY
AMANDA TODD	LINH TRUONG	AARUSHI BAINSLA VERMA
OM SUDHIR VIDYARTHI	SIMON WAGNER	JESSE WANG
SOPHIA WANG	XINRUI WANG	DANIEL WARNER
TIANQI WEI	ETHAN WISEMAN	PAUL WOOD
LIANG-CHU (LUCAS) WU	YING YAO	TWINKLE YE
DUANE YOO	VINCENT ZHAI	TERRY ZHAO
	FAYE ZOU	

BERKELEY CENTER FOR LAW & TECHNOLOGY
2023–24

WAYNE STACY
Executive Director

Staff

MARK COHEN
Senior Fellow & Director, BCLT Asia IP Project

ALLISON SCHMITT
Fellow & Director, BCLT Life Sciences Project

JANN DUDLEY
Associate Director

RICHARD FISK
Assistant Director, Events & Communications

JUSTIN TRI DO
Media Coordinator

ABRIL DELGADO
Events Specialist

Fellow

YUAN HAO
Senior Fellow

KATHRYN HASHIMOTO
Copyright Law Fellow

RAMYA CHANDRASEKHAR
Biometric Regulatory Fellow

ROBERT BARR
BCLT Executive Director Emeritus

BERKELEY CENTER FOR LAW & TECHNOLOGY
2023–24

Faulty Directors

KENNETH A. BAMBERGER
The Rosalinde and Arthur Gilbert Foundation Professor of Law

CATHERINE CRUMP
Robert Glushko Clinical Professor of Practice in Technology Law & Director, Samuelson Law, Technology and Public Policy Clinic

CATHERINE FISK
Barbara Nachtrieb Armstrong Professor of Law

CHRIS JAY HOOFNAGLE
Professor of Law in Residence

SONIA KATYAL
Roger J. Traynor Distinguished Professor of Law & Associate Dean, Faculty Development and Research

ORIN S. KERR
William G. Simon Professor of Law

PETER S. MENELL
Koret Professor of Law

ROBERT P. MERGES
Wilson Sonsini Goodrich & Rosati Professor of Law

DEIRDRE K. MULLIGAN
Professor in the School of Information

TEJAS N. NARECHANIA
Robert and Nanci Corson Assistant Professor of Law

BRANDIE NONNECKE
Associate Research Professor at the Goldman School of Public Policy

OSAGIE K. OBASOGIE
Haas Distinguished Chair, Professor of Law & Professor of Bioethics

ANDREA ROTH
Professor of Law

PAMELA SAMUELSON
Richard M. Sherman Distinguished Professor of Law

PAUL SCHWARTZ
Jefferson E. Peyser Professor of Law

ERIK STALLMAN
Assistant Clinical Professor & Associate Director, Samuelson Law, Technology & Public Policy Clinic

JENNIFER M. URBAN
Clinical Professor of Law & Director, Samuelson Law, Technology & Public Policy Clinic

MOLLY SHAFFER VAN HOUWELING
Harold C. Hohbach Distinguished Professor of Patent Law and Intellectual Property

REBECCA WEXLER
Assistant Professor of Law

HIPAA v. DOBBS

Wendy A. Bach[†] *& Nicolas Terry*[††]

ABSTRACT

Following the Supreme Court's decision in *Dobbs v. Jackson Women's Health*, the Biden administration issued guidance seeking to reassure doctors and patients that the federal HIPAA Privacy Rule would allow women to feel confident that they could still seek reproductive healthcare without worrying that the information in their medical records would end up in the hands of police. This Article disagrees with the administration's assessment and emphasizes how, rather than revealing the strength of healthcare privacy protections in U.S. law, *Dobbs* and the Biden administration's highlighting of limited HIPAA protections and seriously inadequate protection of mobile app data draw crucial attention to what has always been a relatively weak set of privacy models. Tragically, and long before *Dobbs*, this weakness has facilitated thousands of prosecutions related to reproductive conduct. After *Dobbs* this will likely only escalate. The Article describes the United States' long history of criminalizing reproductive conduct, describe the nature of the likely escalation of these harms and the informational privacy harms at stake after the *Dobbs* ruling, and inquire into whether HIPAA or other federal laws can be expanded to better protect reproductive information. The Article concludes by acknowledging the uncertainties and harms that lie ahead and the urgent need for federal corrective action. It is our hope that in the aftermath of *Dobbs* there might be sufficient political will to revisit informational and healthcare privacy, and to build far more robust barriers to the use of healthcare data to reduce the criminalization of women and support their reproductive choices.

TABLE OF CONTENTS

DOI: https://doi.org/10.15779/Z38WC4T

 We thank Anya Prince for her helpful comments on an earlier draft.

† Professor of Law, University of Tennessee College of Law. wbach@utk.edu.

†† Hall Render Professor of Law, Executive Director, Hall Center for Law and Health, Indiana University Robert H. McKinney School of Law. npterry@iu.edu.

I. INTRODUCTION

Just days after the Supreme Court's decision in *Dobbs v. Jackson Women's Health Organization*,[1] the Biden administration issued guidance[2] seeking to reassure doctors and patients that the Health Privacy Rule, often simply referred to as HIPAA,[3] would allow women to feel confident that they could still seek reproductive healthcare without worrying that the information in their medical records would end up in the hands of law enforcement. The contents of our medical records and the conversations patients have with their doctors, the administration seemed to be saying, would remain protected.

Dobbs draws attention to the serious health privacy gaps in U.S. law. Justifiably, patients in traditional care settings, those who manage their own health using technology such as apps, or persons just using web services to become better informed about health issues and resources, may be surprised to learn of HIPAA's deficiencies. After all, for the past two decades, every American's initial engagement with a healthcare provider has included the receipt of a strongly worded "Notice of privacy practices for protected health

1. 142 S. Ct. 2228 (2022).

2. U.S. Dep't Health & Human Servs., Guidance on HIPAA Privacy Rule and Disclosures of Information Relating to Reproductive Health Care, https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/phi-reproductive-health/index.html (last reviewed June 29, 2022).

3. 45 C.F.R. §§ 160–164 (2013).

information" that addresses the uses and disclosures that may be made by the covered entity, the patient's rights, and the covered entity's legal duties.[4]

Even as the earliest ripples from *Dobbs* spread, however, it became clear that the decision not only would exacerbate the criminalization of poverty and reproductive conduct but also jeopardize the confidentiality of the physician-patient relationship and, particularly, of reproductive health privacy. In short, the Biden administration's guidance was not reassuring. This Article emphasizes how, rather than revealing the strength of healthcare privacy protections in U.S. law, the Biden administration's highlighting of HIPAA protections and protection of mobile app data draws crucial attention, alongside *Dobbs*, to what has always been a relatively weak set of privacy models.

Tragically, and long before *Dobbs*, this weakness has facilitated thousands of prosecutions related to reproductive conduct. After *Dobbs*, this will likely only escalate. Although the primary purpose of this Article is to highlight the grave informational privacy issues that *Dobbs* has revealed, it argues that in the aftermath of *Dobbs*, there might be sufficient political will to revisit informational and healthcare privacy, and to build far more robust barriers to the use of healthcare data to reduce the criminalization of women and their reproductive choices.

To make this point and sketch out this possibility, this Article proceeds in five Parts after this Introduction (Part I). Part II starts with the United States' long history of criminalizing reproductive conduct and describes the nature of the likely escalation of these harms. Part III turns directly to privacy and catalogs the privacy harms at stake after the *Dobbs* ruling and the passage of state legislation antithetical to reproductive freedoms. Part IV examines HIPAA itself by drawing a sharp contrast between what people assume it does and its far less protective reality, especially in the context of post-*Dobbs* criminalization. Part V briefly surveys some of the federal and state guidances, statutes, and executive orders designed to lessen the impact of *Dobbs*. Part VI asks whether HIPAA or other federal laws can be expanded to better protect reproductive information and discusses the potential passage of the bipartisan and bicameral American Data Privacy and Protection Act. The Article concludes by acknowledging the uncertainties and harms that lie ahead and the urgent need for federal corrective action.

4. *Id.* § 164.520 (2013).

II. THE SPECTER AND THE REALITY OF CRIMINALIZATION POST-*DOBBS*

Post-*Dobbs*, the reality of criminalization of reproductive conduct has become brutally clear. The news is filled with accounts of doctors fearing prosecution,[5] patients being denied essential care,[6] and the prospect and reality of prosecutors seeking information from people's Facebook accounts[7] and period trackers.[8] Those who can become pregnant are being counseled to use encrypted apps[9] and to delete search histories, all in the name of keeping their private conduct away from the prying eyes of police. The prospect that a wide range of actors—doctors, nurses, counselors, parents, friends, and even pregnant people—will be prosecuted for conduct related to reproductive healthcare is all too real.[10] But while the possibility of many abortion-related prosecutions is certainly evident, neither prosecutions related to reproductive conduct nor the use of presumptively private healthcare information to support prosecutions is new. In fact, both have been happening for decades.

---

5. *See, e.g.*, Jessica Winter, *The Dobbs Decision Has Unleashed Legal Chaos for Doctors and Patients*, NEW YORKER (July 2, 2022), https://www.newyorker.com/news/news-desk/the-dobbs-decision-has-unleashed-legal-chaos-for-doctors-and-patients; Ariana Eunjung Cha, *Physicians Face Confusion and Fear in Post-Roe World*, WASH. POST (June 28, 2022), https://www.washingtonpost.com/health/2022/06/28/abortion-ban-roe-doctors-confusion/.

6. *See, e.g.*, Carrie Feibel, *Because of Texas' Abortion Law, Her Wanted Pregnancy Became a Medical Nightmare*, NPR (July 26, 2022), https://www.npr.org/sections/health-shots/2022/07/26/1111280165/because-of-texas-abortion-law-her-wanted-pregnancy-became-a-medical-nightmare; Laura Kusisto, *Doctors Struggle with Navigating Abortion Bans in Medical Emergencies*, WALL ST. J. (Oct. 13, 2022), https://www.wsj.com/articles/doctors-struggle-with-navigating-abortion-bans-in-medical-emergencies-11665684225.

7. Jason Koebler & Anna Merlan, *This Is the Data Facebook Gave Police to Prosecute a Teenager for Abortion*, MOTHERBOARD (Aug. 9, 2022), https://www.vice.com/en/article/n7zevd/this-is-the-data-facebook-gave-police-to-prosecute-a-teenager-for-abortion.

8. Michela Moscufo, MaryAlice Parks & Jeca Taudte, *Period-tracking Apps May Help Prosecute Users, Advocates Fear*, ABC NEWS (July 1, 2022), https://abcnews.go.com/Health/abortion-advocates-fear-period-tracking-apps-prosecute-abortion/story?id=85925714.

9. Geoffrey A. Fowler & Tatum Hunter, *For People Seeking Abortions, Digital Privacy is Suddenly Critical*, WASH. POST (June 24, 2022), https://www.washingtonpost.com/technology/2022/05/04/abortion-digital-privacy/.

10. For example, the Indiana doctor who performed a then lawful abortion on a 10-year-old rape victim from Ohio is being actively investigated by the Indiana Attorney-General. *See* Megan Messerly, *Doctor Who Performed Abortion for 10-year-old Sues Indiana AG, Alleges 'Fishing Expedition'*, POLITICO (Nov. 3, 2022), https://www.politico.com/news/2022/11/03/doctor-who-performed-abortion-for-10-year-old-sues-indiana-ag-over-fishing-expedition-00065001. In South Carolina a woman has been arrested for an attempt to end her pregnancy with abortion pills that occurred prior to the reversal of *Roe*. Poppy Noor, *South Carolina Woman Arrested for Allegedly Using Pills to End Pregnancy*, GUARDIAN (Mar. 3, 2023), https://www.theguardian.com/us-news/2023/mar/03/south-carolina-woman-arrested-abortion-pills; *see also infra* notes 29–30 and accompanying text.

Historically, pregnant people and people who have given birth have been prosecuted for a wide variety of crimes from the most serious, including murder, to a wide range of lower-level felonies and misdemeanors. Prosecutions have involved a wide range of allegations. Although these prosecutions are notoriously difficult to count, various advocates and academics have documented at least 1,700 forced interventions, through either criminal prosecution or civil commitment, between 1973 and 2020.[11] While the vast majority of these cases involved charges arising from allegations that a fetus was harmed by the person's drug use during pregnancy, allegations have also targeted other conduct, including fighting, failing to wear a seatbelt,[12] attempting suicide, and mishandling fetal remains.

Although these criminal cases cover a vast range of alleged conduct, to get a sense of the breadth, it makes sense to look at three categories of crimes that are charged against pregnant people. The first category involves circumstances in which the state alleges that the pregnant person attempted a self-managed abortion; the second and sometimes overlapping category involves miscarriages; the third involves live births.

First, individuals have been prosecuted when the state believed that they had attempted to induce their own abortion. If/When/How, an advocacy group that, for many years, has documented the criminalization of abortion, released a report in August 2022 documenting sixty-one cases between 2000 and 2020 of individuals who were criminally investigated or arrested for ending their own pregnancies or helping someone else do so.[13]

Second, in the last several years, journalists, academics, and policy advocates have highlighted several prosecutions across the country that arose out of a miscarriage and/or stillbirth. Women have been charged with murder, feticide, and manslaughter. To take just a few examples, in 2018 prosecutors in Indiana brought charges against Kelli Leever-Driskel for feticide and involuntary manslaughter, alleging that Ms. Driskel's drug use during

11. *Arrests and Prosecutions of Pregnant Women, 1973–2020*, NAT'L ADVOC. FOR PREGNANT WOMEN (2021), https://www.nationaladvocatesforpregnantwomen.org/arrests-and-prosecutions-of-pregnant-women-1973-2020/.

12. Ed. Bd., *When Prosecutors Jail a Mother for Miscarriage,* N.Y. TIMES (Dec. 28, 2018), https://www.nytimes.com/interactive/2018/12/28/opinion/abortion-pregnancy-pro-life.html.

13. LAURA HUSS, FARAH DIAZ-TELLO & GOLEEN SAMARI, SELF-CARE CRIMINALIZED, AUGUST 2022 PRELIMINARY FINDINGS 2, IF/WHEN/HOW (Aug. 2022), https://www.ifwhenhow.org/wp-content/uploads/2023/06/22_08_SMA-Criminalization-Research-Preliminary-Release-Findings-Brief_FINAL.pdf.

pregnancy caused her miscarriage.[14] Similarly, in 2013, a court in Indiana sentenced Purvi Patel to twenty years in prison for feticide and felony child neglect.[15] The prosecution in that case alleged that Ms. Patel induced her own abortion with the use of medication.[16] In 2010, Bei Bei Shuai was charged with murdering her fetus.[17] She originally faced the possibility of twenty-five years to life in prison, but, after public outcry, she was offered and accepted a plea to criminal recklessness and was sentenced to 178 days in jail.[18] Women who miscarried have also been charged with a variety of crimes concerning how they handled the fetal remains.[19]

Finally, although the charges involving self-managed abortion, miscarriage, and/or stillbirth have been some of the most notorious—and in terms of extent of punishment, the most serious—far more frequent are prosecutions of new parents in cases in which their infants survived but the state alleged that they were harmed because of the pregnant person's conduct. For example, between 2014 and 2016, the State of Tennessee prosecuted at least 120 women for the crime of fetal assault, which the state at the time defined as in-utero transmission of narcotics resulting in harm.[20] Similarly, in Alabama, the state charged at least 479 women with chemical endangerment of a fetus,[21] and prosecutors in South Carolina charged at least 182 women with a variety of crimes based on conduct during pregnancy.[22] Every case involved an allegation of drug use.

14. TheIndyChannel.com Staff, *Woman Charged with Baby's Death After Police Say She Admitted to Drug Use During Preg*nancy, WRTV INDIANAPOLIS (Feb. 15, 2018), https://www.wrtv.com/news/local-news/madison-county/woman-charged-with-babys-death-after-police-say-she-admitted-to-drug-use-during-pregnancy.

15. Emily Bazelon, *Purvi Patel Could Be Just the Beginning*, N.Y. TIMES MAG. (Apr. 1, 2015), https://www.nytimes.com/2015/04/01/magazine/purvi-patel-could-be-just-the-beginning.html.

16. *Id.*

17. Diana Penner, *Woman Freed After Plea Agreement in Baby's Death*, USA TODAY (Aug. 2, 2013), www.usatoday.com/story/news/nation/2013/08/02/woman-freed-after-plea-agreement-in-babys-death/2614301/.

18. *Id.*

19. *See* Ed. Bd., *How My Stillbirth Became a Crime,* N.Y. TIMES (Dec. 28, 2018), https://www.nytimes.com/interactive/2018/12/28/opinion/stillborn-murder-charge.html); Ed. Bd., *When Prosecutors Jail a Mother for Miscarriage,* N.Y. TIMES (Dec. 28, 2018), https://www.nytimes.com/interactive/2018/12/28/opinion/abortion-pregnancy-pro-life.html.

20. WENDY A. BACH, PROSECUTING POVERTY, CRIMINALIZING CARE 189 (2022).

21. Nina Martin, *Take a Valium, Lose Your Kid, Go to Jail*, PRO PUBLICA (Sept. 23, 2015), https://www.propublica.org/article/when-the-womb-is-a-crime-scene.

22. *See* Grace Elizabeth Howard, *The Criminalization of Pregnancy: Rights, Discretion, and the Law* 62 (Oct. 2017) (unpublished Ph.D. dissertation, Rutgers University) (on file with authors).

Criminalization, when broadly defined to include other forced interventions by the state in pregnancy, does not stop with prosecutions. States also frequently turn to civil commitment to control the movements and conduct of pregnant people. For example, in three states (Minnesota, Wisconsin and South Dakota) substance use during pregnancy is a ground for civil commitment.[23] Similarly, child welfare systems (which are more aptly termed family regulation[24] or family policing[25] systems) regularly intervene in families based on the conduct of pregnant people. While there are scattered cases involving other allegations,[26] most of these cases involve allegations of fetal harm based on the conduct of the pregnant person during pregnancy. The latter cases generally involve allegations of substance misuse. With one notable statutory exception,[27] these cases are generally initiated at or shortly after birth. The child welfare agency typically alleges that the newborn child is dependent or neglected because of the pregnant person's drug use during pregnancy and takes temporary custody of the infant. Currently, twenty-four states and the District of Columbia consider substance exposure to be abuse or neglect,[28] laying a sufficient basis to terminate parental rights. Finally, it is important to understand that while the laws underlying these prosecutions and forced intervention are neutral on their face, the actual cases have targeted—disproportionately—low-income women and women of color.[29]

---

23. *Substance Use During Pregnancy*, GUTTMACHER INST. (Feb. 1, 2023), https://www.guttmacher.org/state-policy/explore/substance-use-during-pregnancy.

24. Nancy D. Polikoff & Jane M. Spinak, *Strengthened Bonds: Abolishing the Child Welfare System and Re-Envisioning Child Well-Being*, 11 COLUM. J. RACE & L. 427, 431 (2021).

25. Dorothy Roberts, *How I Became a Family Policing Abolitionist*, 11 COLUM. J. RACE & L. 455, 462–63 (2021).

26. *See, e.g.*, Jefferson v. Griffin Spalding Cnty. Hosp. Auth., 274 S.E.2d. 457 (Ga. 1981) (where mother, in her 39th week of pregnancy, had a complete placenta previa, making it, in her doctor's opinion, 99% likely that child would not survive vaginal delivery, and mother's chances of surviving were less than 50%, where doctor opined that both would have almost 100% chance of living if woman were to undergo cesarean delivery, but mother refused, on basis of religious beliefs, and also refused any blood transfusion; court ordered the surgery and placed fetus in temporary custody of Georgia Department of Human Resources).

27. *See* TEX. FAM. CODE ANN. § 161.102 (permitting the filing of a petition for termination of parental rights on behalf of an unborn child). *But see* TEX. DEP'T OF FAM. & PROTECTIVE SERVS., STATEWIDE INTAKE POL'Y & PROC. 4510 (2020), https://www.dfps.state.tx.us/handbooks/SWI_Procedures/Files/SWP_pg_4000.asp#SWP_4510.

28. GUTTMACHER INST., *supra* note 23.

29. *See* Huss et al., *supra* note 13, at 2 (among those investigated or prosecuted for conduct concerning self-managed abortion "people of color are disproportionately represented; [and] . . . the majority of adult cases . . . involved people living in poverty."); BACH, *supra* note 20, at 86 (noting that the majority of prosecutions for fetal assault in Tennessee involved low income women.); Lynn M. Paltrow & Jeanne Flavin, *Arrests of and Forced Interventions on Pregnant Women in the United States, 1973–2005: Implications for Women's Legal*

Post-*Dobbs* we are likely to see not only an escalation of these types of prosecutions but also prosecutions of a wider range of actors and conduct. First, it is entirely possible that healthcare professionals will be prosecuted for performing abortion. In Alabama, for example, the Alabama Human Life Protection Act bans abortion except to save a woman's life or to prevent a serious health risk.[30] Performing an abortion in violation of this statute is a Class A felony with a possible sentence of ten to ninety-nine years in prison. States across the country have similar statutes. The Indiana attorney-general's pursuit of a board-certified obstetrician-gynecologist who performed a legal abortion on a ten-year-old rape victim has garnered national attention.[31] Also subject to potential prosecution are other individuals who assist pregnant people to travel to states where abortion is legal, individuals who assist women in obtaining abortion-inducing medication, and anyone who can be charged with other crimes associated with the unlawful disposal of fetal remains. Finally, we are likely to see additional prosecutions in the context of miscarriage and stillbirth. Those prosecutions could not only target the patient but could also target anyone who assisted the pregnant person in any alleged attempt to terminate the pregnancy. In addition to prosecutions, many states already classify fetal harm as a form of child abuse, which already does and could heighten the vulnerability of pregnant people.

While the constitutionality and legality of this anticipated flood of prosecutions will be litigated in the coming years,[32] there is no doubt that many of these cases will rely on a combination of two basic kinds of healthcare related data. First, they will rely on data contained in medical records—data that is often, but not always, classified as protected health information under HIPAA. A wide variety of presumptively confidential protected health information—including testing results, diagnostic notes, the contents of statements by the patient to medical personnel, and the results of medical testing—could be evidence of these crimes. Second, a wide variety of personal information on computers, cell phones, and other devices will also be relevant to these cases and sought by prosecutors and police. Considering this, to the

Status and Public Health, 38 J. OF HEALTH POL., POL'Y & L. 299, 310 (2013) (noting that between 1973 and 2005, prosecutions and forced interventions targeted disproportionately poor women, the vast majority of whom were African American).

30. ALA. CODE § 26-23H-4 (2019).

31. Tom Davies, *Indiana AG Seeks Punishment for Doctor Who Provided Abortion to 10-year-old Rape Survivor*, PBS (Nov. 30, 2022), https://www.pbs.org/newshour/health/indiana-ag-seeks-punishment-for-doctor-who-provided-abortion-to-10-year-old-rape-survivor.

32. David S. Cohen, Greer Donley & Rachel Rebouché, *The New Abortion Battleground*, 123 COLUM. L. REV. 1, 22–42 (2023).

extent one believes that healthcare records should be private, ensuring that we have sufficient protections in place is crucial.

III. POST-*DOBBS* HEALTH PRIVACY HARMS

The *Dobbs* dissenters were under no illusion as to the harms that would follow the decision:

> Enforcement of all these draconian restrictions will also be left largely to the States' devices. A State can of course impose criminal penalties on abortion providers, including lengthy prison sentences. But some States will not stop there. Perhaps, in the wake of today's decision, a state law will criminalize the woman's conduct too, incarcerating or fining her for daring to seek or obtain an abortion. And as Texas has recently shown, a State can turn neighbor against neighbor, enlisting fellow citizens in the effort to root out anyone who tries to get an abortion, or to assist another in doing so.[33]

In a relatively short period of time since the decision in *Dobbs* (or the leak of its draft), several of the informational privacy implications of state laws unleashed by *Dobbs* have surfaced together with deep concerns over what privacy issues may arise in the future. It is quite clear that state total or near-total bans are only the first step in the upheaval of the *Roe* world. Until they realize a federal legislative ban, antiabortion activists, legislators, and prosecutors will concentrate on shutting down the supply of out-of-state abortion medications and the travel of their domiciliaries for out-of-state abortion services. Advocates are already promoting dramatically expanded prohibitions and enforcement.[34] As David Cohen, Greer Donley, and Rachel Rebouché have argued, "Antiabortion states and cities will not wait for the U.S. Supreme Court to give them permission to apply their laws extraterritorially."[35] The gasoline that will fuel these prosecutions is medical information and informational privacy increasingly will be viewed as necessary collateral damage.

The Biden Administration swiftly issued sub-regulatory guidance on HIPAA protections of healthcare reproductive information[36] and protecting

33. Dobbs v. Jackson Women's Health Org., 142 S. Ct. 2228, 2318 (2022) (Breyer, J., Sotomayor, J., and Kagan, J., dissenting).

34. *See, e.g.*, Letter from James Bopp, Jr., NRLC General Counsel, Courtney Turner Milbank & Joseph D. Maughon to Nat'l Right to Life Comm. and Whom it May Concern (June 15, 2022), https://www.nrlc.org/wp-content/uploads/NRLC-Post-Roe-Model-Abortion-Law-FINAL-1.pdf.

35. Cohen et al., *supra* note 32, at 30.

36. HIPAA Privacy Rule and Disclosures, *supra* note 2.

non-HIPAA information residing on personal devices such as phones.[37] The former stressed the responsibilities of healthcare providers but noted the broad exceptions that apply in the case of law enforcement. The latter admitted the long-known deficiencies in our broader protection of health data. Neither was particularly reassuring. Part IV examines in detail defects in the HIPAA informational privacy model and contrasts the popular conception of the extent to which health privacy is safeguarded and its far less protective reality.

To better understand these harms, this Article works from an established taxonomy. Daniel Solove identified "four basic groups of harmful activities" that affect informational privacy: "(1) information collection, (2) information processing, (3) information dissemination, and (4) invasion,"[38] all of which seem implicated by trigger or post-*Dobbs* abortion laws.[39] Specifically in this context, "collection" refers to the collection of personal health information by HIPAA-covered entities (and their typical storage in electronic health records systems) or other sensitive data collected by mobile devices and apps or search engines. "Processing" refers to the aggregation of health information, medically-inflected data, and other data to create profiles of categories or of individual persons. "Dissemination" is the disclosure of HIPAA-protected personal health information because of the myriad of HIPAA exceptions or the sale or disclosure of non-HIPAA protected health information (PHI) such as by data aggregators. "Invasion" refers to the tools of modern healthcare, from electronic health records (EHR) to on-device health data being repurposed by states or their agents as tools of surveillance.

Importantly—as should become clear—in the context of health information, it is helpful to separate that information into the two basic categories identified above: (1) information that is at least presumptively protected by HIPAA or other health privacy laws, and (2) information that falls outside the scope of those protections.

A. COLLECTION

Not surprisingly, collection of personal health information has been an immediate concern for women of reproductive age in states with highly

37. *Guidance on Protecting the Privacy and Security of Your Health Information When Using Your Personal Cell Phone or Tablet*, U.S. DEP'T HEALTH & HUMAN SERVS. (June 29, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/cell-phone-hipaa/index.html.

38. Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 489 (2006).

39. Abortion "trigger" laws were restrictive abortion laws passed by some states that were automatically "triggered" if Roe was reversed. *See* Elizabeth Nash & Isabel Guarnieri, *13 States Have Abortion Trigger Bans—Here's What Happens When Roe Is Overturned*, GUTTMACHER INST. (June 6, 2022), https://www.guttmacher.org/article/2022/06/13-states-have-abortion-trigger-bans-heres-what-happens-when-roe-overturned.

restricted abortion laws.[40] This anxiety focuses both on information categorized as protected health information (PHI) under HIPAA and information outside of those protections.

In the category of PHI, it is quite clear that medical records will contain a plethora of information that is potentially relevant to pregnancy related prosecutions. To take just one relatively recent example, in a recently completed study on the prosecution of about 120 women for the "crime" of fetal assault in Tennessee,[41] the research team gathered the complete criminal court files for sixty-three of the defendants. Fifty-seven of those files contained detailed information clearly obtained through medical testing or in conversations between the defendant and medical personnel. This included a wide range of information—from test results, to diagnosis, to statements by the women to nurses and doctors. An additional three case files contained allegations concerning medical facts, but there was no clear indication of the source of that information. Only three charging documents contained information solely based on nonmedical sources, such as an admission by the defendant to the Department of Children's Services DCS or investigative personnel.

Similarly, in *Policing the Womb*, Professor Michele Goodwin carefully documented the ways in which, in cases she terms the "criminalization of motherhood," medical providers have played a significant role in both policing the conduct of their pregnant patients and conveying information to police and other government officials.[42]

It seems clear that a direct prosecution against a medical provider for performing what the state alleges was an unlawful abortion will similarly rely heavily on information in those records. Prosecutors will mine health records to investigate whether life-saving abortions were truly necessary and to flag doctors who performed abortions at a higher rate.[43] Beyond this, in cases involving miscarriage in which there is suspicion of a self-managed abortion, medical records may contain relevant statements as well as other evidence. In fact, some reports have suggested that most of these potential prosecutions

40. *Tracking the States Where Abortion Is Now Banned*, N.Y. TIMES (Feb. 10, 2023), https://www.nytimes.com/interactive/2022/us/abortion-laws-roe-v-wade.html.

41. BACH, *supra* note 20, at 130.

42. MICHELE GOODWIN, POLICING THE WOMB: INVISIBLE WOMEN AND THE CRIMINALIZATION OF MOTHERHOOD 78–97 (2020).

43. *See* Kavitha Surana, *"We Need to Defend This Law": Inside an Anti-Abortion Meeting with Tennessee's GOP Lawmakers*, PRO PUBLICA (Nov. 15, 2022), https://www.propublica.org/article/inside-anti-abortion-meeting-with-tennessee-republican-lawmakers.

will follow the script laid down in the past and rely on PHI to prove their cases.[44]

Outside of PHI, significant concerns have been raised about data surveillance.[45] One of the first types of technology identified as problematic were fertility and period tracking apps.[46] These apps used by an estimated 50 million women worldwide[47] could reveal the date of last menstruation to a subpoena-wielding prosecutor. This class of apps already has a somewhat checkered past regarding protecting user privacy.[48] While some are more respectful of their users, even avoiding apps that use cloud storage may not be enough. Apps such as Planned Parenthood's "Spot On"[49] may save all data locally, but that will not protect the data if a prosecutor acquires the user's phone.[50] In the wake of *Dobbs*, Google announced that it will make it easier for Google Fit and Fitbit users to delete menstruation logs.[51]

The immediate future of abortion in abortion-hostile states will involve either travel to abortion-friendly states or mail-order facilitated medication abortions.[52] As to the former, Justice Kavanaugh asked and answered the following hypothetical in his *Dobbs* concurrence: "[M]ay a State bar a resident

---

44. Eleanor Klibanoff, *Lawyers Preparing for Abortion Prosecutions Warn About Health Care, Data privacy*, TEX. TRIB. (July 25, 2022), https://www.texastribune.org/2022/07/25/abortion-prosecution-data-health-care/.

45. *See generally* Anya E. R. Prince, *Reproductive Health Surveillance*, 64 B.C. L. REV. 1077, 1085 (2023).

46. *See generally* Leah R. Fowler & Michael R. Ulrich, *Femtechnodystopia*, STAN. L. REV (forthcoming 2023), http://dx.doi.org/10.2139/ssrn.4099764.

47. Lauren Worsfold, Lorrae Marriott, Sarah Johnson & Joyce C. Harper, *Period Tracker Applications: What Menstrual Cycle Information are They Giving Women?*, 17 WOMENS HEALTH 1, 1 (2021).

48. *Developer of Popular Women's Fertility-Tracking App Settles FTC Allegations that It Misled Consumers About the Disclosure of their Health Data*, FED. TRADE COMM'N (Jan. 13, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/01/developer-popular-womens-fertility-tracking-app-settles-ftc-allegations-it-misled-consumers-about (reporting settlement with the Federal Trade Commission of allegations that a period-tracking app developer shared the health information of users with outside data analytics providers after promising that such information would be kept private).

49. *Spot On Period Tracker*, PLANNED PARENTHOOD, https://www.plannedparenthood.org/get-care/spot-on-period-tracker (last accessed June 18, 2023).

50. Giulia, Carbonaro, *Could Period-Tracking Apps Be Dangerous in a Post-Roe v. Wade U.S.?*, NEWSWEEK (May 6, 2022), https://www.newsweek.com/could-period-tracking-apps-dangerous-post-roe-v-wade-us-1704216.

51. Jen Fitzpatrick, *Protecting People's Privacy on Health Topics*, GOOGLE BLOG (July 1, 2022), https://blog.google/technology/safety-security/protecting-peoples-privacy-on-health-topics/.

52. *See generally* David S. Cohen, Greer Donley & Rachel Rebouché, *Abortion Pills*, 76 STAN. L. REV. (forthcoming 2024), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4335735.

of that State from traveling to another State to obtain an abortion? In my view, the answer is no based on the constitutional right to interstate travel."[53] However, the dissenters in *Dobbs* were far less sanguine as to what might follow:

> After this decision, some States may block women from traveling out of State to obtain abortions, or even from receiving abortion medications from out of State. Some may criminalize efforts, including the provision of information or funding, to help women gain access to other States' abortion services.[54]

As anxiety has ramped up amid the real possibility of, for example, antiabortion vigilantes lurking around interstate bus stations and emergency rooms, attention has also focused on other, non-medical types of sensitive data, particularly location data.[55] Specifically, there are concerns that abortion prosecutions will be based on data showing that a person visited an abortion clinic or sought abortion services or products. In its 2022 guidance, the Department of Health and Human Services (HHS) recommended that users turn off their device's location services.[56] However, the guidance basically admitted that most sensitive information (for example, cell phone location data) is unprotected and could well fall into the hands of data brokers or law enforcement. This is because turning off location services does not stop cellular providers from tracking its customers.[57]

In *Carpenter v. United States*, the Supreme Court held that a warrant is required for access to historical cell-site location information,[58] but seeking a warrant will not be a major hurdle for a zealous prosecutor. Meanwhile, the federal courts have interpreted *Carpenter* narrowly, and therefore have opened

53. Dobbs v. Jackson Women's Health Org., 142 S. Ct. 2228, 2309 (2022).

54. *Id.* at 2318.

55. *See generally* Anya E. R. Prince, *Location as Health*, 21 HOUS. J. HEALTH L. & POL'Y 43 (forthcoming 2021).

56. Protecting the Privacy and Security of Your Health, *supra* note 37.

57. *Id.* In a subsequent Bulletin that was not explicitly targeted at reproductive surveillance, OCR cautioned HIPAA entities and their business associates about tracking technologies, "Regulated entities are not permitted to use tracking technologies in a manner that would result in impermissible disclosures of PHI to tracking technology vendors or any other violations of the HIPAA Rules." *Use of Online Tracking Technologies by HIPAA Covered Entities and Business Associates*, U.S. DEP'T HEALTH & HUM. SERVS. (Dec. 1, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/hipaa-online-tracking/index.html (reference omitted).

58. Carpenter v. United States, 138 S. Ct. 2206 (2018); *see also* United States v. Wilson, 13 F.4th 961 (9th Cir. 2021) (warrant required for search of email attachments).

up access to analogous data.[59] Worse, location data have been routinely provided to law enforcement under what are known as "geofence warrants." A typical Fourth Amendment warrant depends on demonstrating probable cause for the search of a person or place. However, a geofence warrant works in reverse. In such a warrant the provider is ordered to identify all devices in a particular area and provide that information to the police.[60] In a recent case before a District Court in Virginia, Google noted that "geofence warrants comprise more than twenty-five percent of *all* warrants it receives in the United States."[61] In what may prove to be a landmark ruling, the court held that the geofence warrant in issue was invalid because it failed to establish probable cause to search every one of the persons in the geofence area.[62] In addition to geofence warrants, law enforcement also circumvents *Carpenter* protection by purchasing location data from data brokers.[63]

Annually there are almost 20 million Google searches for "abortion," with residents of states that have more restrictive reproductive rights laws making significantly more searches for abortion services.[64] Following the leak of the *Dobbs* opinion in May 2022, internet searches for abortion medications spiked to record highs and, not surprisingly, were higher in states that restrict reproductive rights.[65] Mobile apps contain location data on the device and/or in the cloud while online map services or other search engines may have data showing that a person searched for an abortion clinic or abortion drugs.[66]

59. *See, e.g.*, United States v. Moore-Bush, 963 F.3d 29 (1st Cir.), *reh'g en banc granted*, *vacated*, 982 F.3d 50 (1st Cir. 2020), *and on rehearing en banc*, 36 F.4th 320 (1st Cir. 2022) (pole camera recording); United States v. Contreras, 905 F.3d 853 (5th Cir. 2018) (IP addresses); Commonwealth v. McCarthy, 484 Mass. 493 (2020) (automatic license plate reader data).

60. Matthew Guariglia, *Geofence Warrants and Reverse Keyword Warrants are So Invasive, Even Big Tech Wants to Ban Them*, EFF (May 13, 2022), https://www.eff.org/deeplinks/2022/05/geofence-warrants-and-reverse-keyword-warrants-are-so-invasive-even-big-tech-wants.

61. United States v. Chatrie, 590 F. Supp. 3d 901, 914 (E.D. Va., 2022).

62. *Id.* at 927–33. Ultimately, however, in this case the court applied the "good faith" exception. *Id.* at 936–38. *Cf.* In re Search of Info. that is Stored at Premises Controlled by Google LLC, No. 21-SC-3217, 2021 WL 6196136, at 87–88 (D.D.C. Dec. 30, 2021) (overbreadth of warrant cured by two-step search procedure, requiring further court approval after initial identification).

63. *See supra* note 86 and accompanying text.

64. Sylvia Guendelman, Elena Yon, Elizabeth Pleasants, Alan Hubbard & Ndola Prat, *Shining the Light on Abortion: Drivers of Online Abortion Searches Across the United States in 2018*, 15 PLOS ONE 1, 9 (2020).

65. Adam Poliak, Nora Satybaldiyeva, Steffanie A. Strathdee, Eric C. Leas, Ramesh Rao, Davey Smith & John W. Ayers, *Internet Searches for Abortion Medications Following the Leaked Supreme Court of the United States Draft Ruling*, 182 JAMA INTERNAL MED. 1001(2022).

66. Patience Haggin, *Phones Know Who Went to an Abortion Clinic. Whom Will They Tell?*, WALL ST. J. (Aug. 7, 2022), https://www.wsj.com/articles/phones-know-who-went-to-an-abortion-clinic-whom-will-they-tell-11659873781.

There is already evidence that the major online pharmacies that sell abortion medication share large amounts of data with Google.[67]

Concerns about online and on-device privacy are not new to the abortion wars. In 2015 a Massachusetts digital marketing company was hired to send targeted advertisements to "abortion-minded women" attending clinics. The technique employed geofencing, using mobile geofences near abortion clinics that captured a user's device ID, and then targeting the user's browser with advertisements about abortion alternatives. In 2017, the company entered a settlement agreement with the Massachusetts Attorney General and agreed not to target Massachusetts healthcare facilities.[68]

Finally, medical records created in a safe haven or abortion "island" state relating to a procedure, by default, will travel back to the patient's domicile. Carleen Zubrzycki describes this as an "interoperability trap," one that safe haven states should close by, for example, prohibiting the transfer of abortion-related data across state lines.[69]

Medication abortions using the FDA-approved combination of Mifepristone and Misoprostol accounted for 53 percent of all abortions in the United States as of December 1, 2022.[70] This trajectory likely has been accelerated by the FDA decision to allow mail-order provision following a telemedicine consultation first during the pandemic[71] and now permanently.[72] Requests for telemedicine-intermediated abortions increased substantially

67. Jennifer Gollan, *Websites Selling Abortion Pills Are Sharing Sensitive Data with Google*, PRO PUBLICA (Jan. 18, 2023), https://www.propublica.org/article/websites-selling-abortion-pills-share-sensitive-data-with-google.

68. OFF. OF ATT'Y GEN. MAURA HEALEY, *AG Reaches Settlement with Advertising Company Prohibiting 'Geofencing' Around Massachusetts Healthcare Facilities* (Apr. 4, 2017), https://www.mass.gov/news/ag-reaches-settlement-with-advertising-company-prohibiting-geofencing-around-massachusetts-healthcare-facilities.

69. Carleen M. Zubrzycki, *The Abortion Interoperability Trap*, 132 YALE L.J. FORUM 197, 208–23 (2022).

70. Rachel K. Jones, Elizabeth Nash, Lauren Cross, Jesse Philbin & Marielle Kirstein, *Medication Abortion Now Accounts for More Than Half of All US Abortions*, GUTTMACHER INST. (Dec. 1, 2022), https://www.guttmacher.org/article/2022/02/medication-abortion-now-accounts-more-half-all-us-abortions.

71. Letter from Janet Woodcock, M.D., Acting Commissioner of Food and Drugs to Maureen G. Phipps, MD, MPH, FACOG, Chief Executive Officer, American College of Obstetricians and Gynecologists, and William Grobman, MD, MBA, President, Society for Maternal-Fetal Medicine (Apr. 12, 2021), https://www.aclu.org/sites/default/files/field_document/fda_acting_commissioner_letter_to_acog_april_12_2021.pdf.

72. Questions and Answers on Mifepristone for Medical Termination of Pregnancy through Ten Weeks Gestation, U.S. FOOD & DRUG ADMIN. (Jan. 4, 2023), https://www.fda.gov/drugs/postmarket-drug-safety-information-patients-and-providers/questions-and-answers-mifepristone-medical-termination-pregnancy-through-ten-weeks-gestation.

following the *Dobbs* decision particularly in states that have implemented total bans.[73] Nineteen states already require in-person prescribing or explicitly ban the use of telemedicine for medication abortions.[74] However, antiabortion groups reportedly are unhappy with enforcement of these bans and are exploring strategies such as wastewater surveillance.[75] FDA approval of Mifepristone is also under challenge. Both its original approval and the relaxation of its prescribing requirements were successfully challenged before the District Court for the Northern District of Texas before being partially stayed by the Fifth Circuit Court of Appeals.[76] Thereafter, the Supreme Court issued a broader, emergency stay pending resolution by the Firth Circuit.[77]

To curtail the pharmacological end-run around their abortion bans, states with restrictive laws inevitably will seek out and prosecute those who prescribe, transport, or ingest abortion pills.[78] Inevitably, as lawful supply chains are shut down by state lawmakers, they will be replaced with underground sources[79] and their concomitant health risks.[80] While post-*Dobbs* restrictive abortion measures primarily target abortion clinics and physicians, it is an open question

---

73. Abigail R. A. Aiken, Jennifer E. Starling, James G. Scott & Rebecca Gomperts, *Requests for Self-managed Medication Abortion Provided Using Online Telemedicine in 30 US States Before and After the* Dobbs v Jackson Women's Health Organization *Decision*, 328 J. AM. MED. ASS'N 1768 (2022).

74. *State Requirements for the Provision of Medication Abortion*, KFF (Apr. 2023), https://www.kff.org/womens-health-policy/state-indicator/state-requirements-for-the-provision-of-medication-abortion/; *The Availability and Use of Medication Abortion*, KFF (June 1, 2023), https://www.kff.org/womens-health-policy/fact-sheet/the-availability-and-use-of-medication-abortion/.

75. Caroline Kitchener, *Conservatives Complain Abortion Bans Not Enforced, Want Jail Time for Pill 'Trafficking'*, WASH. POST (Dec. 14, 2022), https://www.washingtonpost.com/politics/2022/12/14/abortion-pills-bans-dobbs-roe/.

76. All. for Hippocratic Med. v. U.S. Food & Drug Admin., No. 2:22-CV-223-Z, 2023 WL 2825871 (N.D. Tex. Apr. 7, 2023), *aff'd in part, vacated in part*, 78 F.4th 210 (5th Cir. 2023).

77. Danco Lab'ys, LLC v. All. for Hippocratic Med., et al. 598 U.S. ____ (2023), https://www.supremecourt.gov/opinions/22pdf/22a901_3d9g.pdf.

78. *See* Kerry Breen, *People in Alabama Can Be Prosecuted for Taking Abortion Pills, State Attorney General Says*, CBS NEWS (Jan. 11, 2023), https://www.cbsnews.com/news/abortion-pills-alabama-prosecution-steve-marshall/; Arwa Mahdawi, *Worried that women will be prosecuted for using abortion pills? It's already happening*, GUARDIAN (Mar. 4, 2023), https://www.theguardian.com/commentisfree/2023/mar/04/abortion-pills-women-prosecution-week-in-patriarchy.

79. Stephania Taladrid, *The Post-Roe Abortion Underground*, NEW YORKER (Oct. 10, 2022), https://www.newyorker.com/magazine/2022/10/17/the-post-roe-abortion-underground.

80. *See, e.g.*, U.S. Food & Drug Admin., Warning Letter to Aidaccess.org, MARCS-CMS 575658 (Mar. 8, 2019), https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/aidaccessorg-575658-03082019 ("Dugs that have circumvented regulatory safeguards may be contaminated; counterfeit, contain varying amounts of active ingredients, or contain different ingredients altogether.").

whether prosecutors will also target abortion seekers or those who abort. This is a political rather than legal question because of reassurances the antiabortion movement has given to women over the years that they are not their targets. However, as medication abortions become dominant it is highly likely that prosecutors will turn their attention to those who take the drugs.[81]

In many cases the information needed by prosecutors will be found on mobile devices. For example, and discussed above,[82] in 2013 Purvi Patel purchased mifepristone and misoprostol online and used the drugs to terminate her pregnancy, which resulted in a live birth followed by the baby's death. She was convicted by an Indiana court of child neglect and felony feticide and sentenced to 30 years of imprisonment. Evidence at trial included texts discovered on her tablet in which she discussed the use of the drugs with a friend as well as a receipt from an online supplier. The Indiana Court of Appeals overturned her feticide conviction, and she was released after time served when resentenced on a lower-level neglect charge.[83] A somewhat similar case was reported in 2022 involving a Nebraska teenager and her mother who allegedly acquired mifepristone and misoprostol to terminate a 28-week pregnancy (Nebraska then having a ban after 20 weeks). The prosecution case includes evidence from Facebook chats on mobile devices and computers recovered through a search warrant.[84]

B. PROCESSING

HIPAA protects personal health information such as hospital records from unauthorized disclosure. As a result, data aggregators (aka brokers), or at least those acting lawfully, will usually not have access to that PHI. However, data aggregators do have access to deidentified health records, data received from public health agencies, and a broad array of what may be described as medically inflected data such as credit card data recording the purchase of health products and services. To these data, aggregators add mobile data such as location data or data derived from apps, search engines, or web trackers.

81. *See, e.g.*, Caroline Kitchener & Ellen Francis, *Talk of Prosecuting Women for Abortion Pills Roils Antiabortion Movement*, WASH. POST (Jan. 11, 2023), https://www.washingtonpost.com/nation/2023/01/11/alabama-abortion-pills-prosecution/(discussing suggestion by Alabama attorney-general that he would prosecute women for taking abortion pills).

82. *See supra* Part II.

83. Patel v. State, 60 N.E.3d 1041 (Ind. Ct. App. 2016); *Purvi Patel is Released After Feticide Conviction Overturned*, ASSOCIATED PRESS (Sept. 1, 2016), https://www.indystar.com/story/news/crime/2016/09/01/purvi-patel-releases-feticide-conviction-overturned/89707582/.

84. Jason Koebler & Anna Merlan, *This Is the Data Facebook Gave Police to Prosecute a Teenager for Abortion*, MOTHERBOARD (Aug. 9, 2022), https://www.vice.com/en/article/n7zevd/this-is-the-data-facebook-gave-police-to-prosecute-a-teenager-for-abortion.

They then sell data sets or predictive data drawn from the data.[85] Increasingly, such data (including location data) is sold to law enforcement, typically without any warrant.[86]

It was not surprising that, soon after the draft *Dobbs* opinion was leaked, a data aggregator was contacted by unnamed companies requesting mobile-device data identifying persons who had visited abortion clinics along the Illinois-Missouri border.[87] It is highly likely that such data already exists in the hands of some aggregator or soon will be built out. Some further clues can be gleaned from the current litigation between the Federal Trade Commission (FTC) and Kochava, an Idaho-based company that describes itself as the "largest independent data marketplace for connected devices."[88] The FTC apparently is arguing that the company's data sets make it possible to track consumers to sensitive locations, such as reproductive health clinics.[89] Importantly, as discussed below, the types of aggregated health or medically-inflected data at issue are only thinly regulated[90] and highly unlikely to be subject to HIPAA.

Because personal health information is held in confidence by healthcare providers, unauthorized dissemination or disclosure is a well-established harm (and an obvious HIPAA violation[91]). Indeed, there are numerous accounts of

85. Nicolas P. Terry, *Big Data Proxies and Health Privacy Exceptionalism*, 24 HEALTH MATRIX 65, 85–87 (2014).

86. *Data Broker Helps Police See Everywhere You've Been with the Click of a Mouse: EFF Investigation*, ELEC. FRONTIER FOUND. (Sept. 1, 2022), https://www.eff.org/press/releases/data-broker-helps-police-see-everywhere-youve-been-click-mouse-eff-investigation. *See generally* Dori H. Rahbar, *Laundering Data: How the Government's Purchase of Commercial Location Data Violates Carpenter and Evades the Fourth Amendment*, 122 COLUM. L. REV. 713. 716–17 (2022) (describing instances in which federal agencies have bought location data from commercial data aggregators).

87. Haggin, *supra* note 66.

88. Ashley Belanger, *FTC Sued by Firm Allegedly Selling Sensitive Data on Abortion Clinic Visits*, ARSTECHNICA (Aug. 18, 2022), https://arstechnica.com/tech-policy/2022/08/ftc-sued-by-firm-allegedly-selling-sensitive-data-on-abortion-clinic-visits/.

89. Compl., Kochava Inc. v. Fed. Trade Comm'n, No. 2:22-cv-00349 (N.D. Idaho Aug. 12, 2022), https://cdn.arstechnica.net/wp-content/uploads/2022/08/Kochava-v-FTC-Complaint.pdf.

90. *See generally* Nicolas P. Terry, *Assessing the Thin Regulation of Consumer-Facing Health Technologies*, 48 J.L. MED. & ETHICS 94 (2020) (arguing that the design and structures of existing data protection and safety regulation in the U.S. have resulted in exceptionally thin protection for the users of consumer-facing devices and product that rely on or that facilitate consumer collection or aggregation of health and wellness data).

91. *See, e.g.*, Health and Human Services, *Dental Practice Pays $10,000 to Settle Social Media Disclosures of Patients' Protected Health Information*, U.S. DEP'T HEALTH & HUM. SERVS. (Dec. 31, 2020), https://public3.pagefreezer.com/browse/HHS.gov/31-12-2020T08:51/https://

persons who work in hospitals or pharmacies accessing the health records of family members or friends.[92] Many of these have led to lawsuits,[93] even reported cases,[94] while a few offenders have faced employment"[95] or even criminal justice sanctions.[96] Moreover, as detailed below,[97] HIPAA contains numerous exceptions that in the face of escalating prosecution and intervention will almost inevitably lead to more and more disclosures.

C. DISSEMINATION

This probable dissemination will upend the tradition of healthcare confidentiality. It is also likely to reopen the debate as to just how much information healthcare providers need to acquire and whether they should retain it, a battle that has generally been lost by privacy advocates as modern medicine has attempted to overcome system fragmentation with broad information sharing and the adoption of electronic health records.[98] The post-*Dobbs* world will upend patient expectations of privacy as states enact whistleblower protections,[99] which will essentially encourage snooping on

---

www.hhs.gov/hipaa/for-professionals/compliance-enforcement/agreements/elite/index.html.

92. *See generally* Charles Ornstein, *Small-Scale Violations of Medical Privacy Often Cause the Most Harm*, PROPUBLIC (Dec. 10, 2015) (providing examples of snooping in the medical redords of friends and family members), https://www.propublica.org/article/small-scale-violations-of-medical-privacy-often-cause-the-most-harm.

93. *See, e.g.*, Susan Vela, HOMETOWN LIFE, *Young woman suesWoman Sues Beaumont, Livonia clinic over medical privacy Clinic Over Medical Privacy*, HOMETOWN LIFE, (Nov. 20, 2019), https://www.hometownlife.com/story/news/local/—.ivonia/2019/11/20/young-woman-sues-hospital-clinic-alleging-privacy-invasion/4191030002/.

94. *See, e.g.*, Yath v. Fairview Clinics, N.P., 767 N.W.2d 34 (Minn. Ct. App. 2009) (describing unsuccessful privacy action against healthcare providers whose employees allegedly posted information from the patient's medical record on the internet); Doe v. Guthrie Clinic, Ltd., 22 N.Y.3d 480, 5 N.E.3d 578 (2014) (holding breach of confidence action against a healthcare provider was not sustainable when the employee responsible for the breach acted outside the scope of his or her employment); Walgreen Co. v. Hinchy, 21 N.E.3d 99, 103 (Ind. Ct. App. 2014), *on reh'g*, 25 N.E.3d 748 (Ind. Ct. App. 2015) (holding evidence supported finding that pharmacist's actions were within the scope of employment when divulged the information she learned from patient records).

95. *See, e.g.*, Fred Donovan, TECHTARGET, *New York Suspends Nurse for HIPAA Violation Affecting 3K Patients*, TECHTARGET (June 11, 2018), https://healthitsecurity.com/news/new-york-suspends-nurse-for-hipaa-violation-affecting-3k-patients.

96. *See, e.g.*, Debra Wood, *Nurse Pleads Guilty to HIPAA Violation*, AMERICANAM. MOBILE (June 25, 2017), https://www.americanmobile.com/nursezone/nursing-news/nurse-pleads-guilty-to-hipaa-violation/.

97. *See infra* Part IV.

98. *See generally* Nicolas P. Terry & Leslie P. Francis, *Ensuring the Privacy and Confidentiality of Electronic Health Records*, 2007 U. ILL. L. REV. 681 (2007).

99. *See, e.g.*, S. 1373, 124th Sess. § 44-41-950(D) (S.C. 2022).

records and disclosing what has heretofore been confidential healthcare information.

Many states increasingly will strangle access to information about abortion and other reproductive services. For example, a proposed South Carolina law would criminalize both (1) providing internet information regarding self-administered abortions and (2) hosting or maintaining a website that provides information on how to obtain an abortion.[100] Leaving First Amendment[101] and Communications Decency Act[102] challenges aside, such state provisions are bound to chill online discourse, cutting off women from needed health information. As abortion foes reduce information such as how to access FDA approved abortion medications[103] or out-of-state abortion services, they are as likely to encourage *misinformation* about medically appropriate services and products.[104] There are already reports of social media sites being flooded with misinformation about "abortion reversal pills."[105] It is likely we will see more disinformation campaigns directed at the vulnerable.[106] Having been successful in raising First Amendment claims against state attempts to regulate misinformation-disseminating "crisis pregnancy centers,"[107] increasing numbers of shadowy or state-promoted organizations will seek to increase the

100. *See, e.g.*, *id.* § 44-41-860(B).

101. Brett Wilkins, *"Aiding and Abetting": SC GOP Pushes "Blatantly Unconstitutional" Bill to Ban Abortion Info Online*, SALON (July 25, 2022), https://www.salon.com/2022/07/25/aiding-and-abetting-sc-pushes-blatantly-unconstitutional-bill-to-ban-abortion-info-online_partner/ (discussing freedom of speech issues related to proposed SC law that would criminalize the online sharing of abortion information).

102. 47 U.S.C. § 230.

103. *See generally The Availability and Use of Medication Abortion*, KFF (June 1, 2023), https://www.kff.org/womens-health-policy/fact-sheet/the-availability-and-use-of-medication-abortion/ (detailing how state use restrictive laws to reduce access to mifepristone to by restricting telemedicine access and mandating unsubstantiated claims about the drug's safety or side effects).

104. This is not solely a post-*Dobbs* phenomenon. *See, e.g.*, *Translating Abortion Disinformation: The Spanish Language Anti-Choice Landscape*, NARAL PRO CHOICE AM., https://www.prochoiceamerica.org/wp-content/uploads/2022/05/Translating-Abortion-Disinformation-The-Spanish-Language-Anti-Choice-Landscape.pdf (last visited July 29, 2023).

105. Rebecca Kern & Ruth Reader, *The Latest Social Media Misinformation: Abortion Reversal Pills*, POLITICO (Aug. 20, 2022), https://www.politico.com/news/2022/08/20/abortion-misinformation-social-media-00052645.

106. *See generally* Jenna Sherman, *How Abortion Misinformation and Disinformation Spread Online*, SCI. AM. (June. 24, 2022), https://www.scientificamerican.com/article/how-abortion-misinformation-and-disinformation-spread-online/ (detailing misinformation and disinformation appearing on social media channels).

107. Nat'l Inst. of Fam. & Life Advocs. v. Becerra, 138 S. Ct. 2361 (2018) (California law requiring crisis pregnancy centers to follow a government-drafted script about the availability of state-sponsored services was a content-based regulation of speech).

friction already suffered by those already dealing with difficult and heretofore private decisions.[108] The growing seriousness of the misinformation issue already can be gauged from Google's notification to Congress that only advertisements from certified abortion providers[109] will be displayed in search results.[110]

D. INVASION

Finally, post-*Dobbs* privacy harms will extend further into intrusions into women's lives and decisional interference.[111] The former suggests a dystopian future where the most personal and private aspects of a woman's life are probed and investigated by zealous prosecutors and vigilantes. The latter brings us full circle to *Dobbs*' rejection of decisional privacy in the face of state interests in prenatal life.

The physical and psychological harms that do and will flow from these invasions are immeasurable. Justifiably, the initial reaction to *Dobbs* has been to examine the impact on pregnant women and related services. For example, will doctors be able to give *legally* safe treatments for miscarriages given that treatment for abortion and miscarriage are the same?[112] Will restrictive abortion laws impact the evidence-based treatment of ectopic pregnancies?[113] Related concerns have been raised regarding continued access to some contraceptive methods and even in vitro fertilization.[114] As the American

108. *Cf.* S.B. 23-190, 74th Gen. Assemb., Reg. Sess. (Colo. 2023) (prohibiting dissemination of advertisement provides abortion or emergency contraception services when they do not).

109. *About Abortion Certification and Disclosures*, *Advertising Policies Help*, GOOGLE, https://support.google.com/adspolicy/answer/9274988 (last visited July 29, 2023).

110. *See* Letter from Google to Senator Warren and Representative Slotkin (Aug. 25, 2022), https://www.warner.senate.gov/public/_cache/files/c/7/c7753efa-3adc-4cd7-9b09-6d12ab88999a/CDC0FFBD434398E0AE66A038707FA10B.response-to-warner-slotkin.pdf.

111. Solove, *supra* note 38, at 552–62.

112. *See* Charlotte Huff, *In Texas, Abortion Laws Inhibit Care for Miscarriages*, NAT'L PUB. RADIO (May 10, 2022), https://www.npr.org/sections/health-shots/2022/05/10/1097734167/in-texas-abortion-laws-inhibit-care-for-miscarriages.

113. *See* Jessica Winter, *The Dobbs Decision Has Unleashed Legal Chaos for Doctors and Patients*, NEW YORKER (July 2, 2022), https://www.newyorker.com/news/news-desk/the-dobbs-decision-has-unleashed-legal-chaos-for-doctors-and-patients.

114. Nicole Karlis, *How Abortion "Trigger Laws" Could Inadvertently Impede Fertility Treatments* (May 10, 2022), SALON, https://www.salon.com/2022/05/10/abortion-trigger-laws-ivf/. Some states may clarify this issue. *See* S. 1373, 124th Sess. § 44-41-840 (S.C. 2022) (noting that bill did not apply to "contraception" or "in vitro fertilization and assisted reproductive technology procedures").

Medical Association and other national bodies representing providers have noted:

> Without access to medications proven to be safe and effective, our patients' health is at risk. As physicians and pharmacists, we view patient wellbeing as paramount and are deeply troubled that continuity of care is being disrupted. We call on state policymakers to ensure through guidance, law, or regulation that patient care is not disrupted and that physicians and pharmacists shall be free to continue to practice medicine and pharmacy without fear of professional sanction or liability.[115]

Restrictive abortion laws must also be viewed through the wider lens of maternal health. Overall, states with restrictive abortion laws have a greater proportion of maternity care "deserts" and fewer maternal care providers. Pregnancy-related death rates and overall maternal death rates are significantly higher there compared to those in abortion-access states.[116]

It is not hard to picture some far broader harms. The Affordable Care Act brought major advances for women's health, including, in particular, preventative care as an essential health benefit.[117] These preventative care services include contraception, counseling for sexually transmitted infections, and screening for HIV, cervical cancer, and domestic violence.[118] Women who faced criminalization pre-*Dobbs* have long weighed the risks of criminal charge(s) from seeking care against its benefits, and have avoided full engagement with care as a result.[119] Post-*Dobbs*, more women of child-bearing age may start to avoid routine interactions with the healthcare system because

115. Press Release, AMA, AphA, ASHP, NCPA Statement on State Laws Impacting Patient Access to Medically Necessary Medications, ASHP NEWS CENTER (Sept. 8, 2022), https://www.ashp.org/news/2022/09/08/statement-on-state-laws-impacting-patient-access-to-medically-necessary-medications.

116. Eugene Declercq, Ruby Barnard-Mayers, Laurie C. Zephyrin & Kay Johnson, *The U.S. Maternal Health Divide: The Limited Maternal Health Services and Worse Outcomes of States Proposing New Abortion Restrictions*, COMMONWEALTH FUND (Dec. 14, 2022), https://doi.org/10.26099/z7dz-8211.

117. *ACA-Covered Preventive Health Services for Women*, AGENCY FOR RSCH. HEALTHCARE & QUALITY, https://www.ahrq.gov/ncepcr/tools/healthier-pregnancy/fact-sheets/preventive-health-services.html (last visited Apr. 20, 2023).

118. *Affordable Care Act Expands Prevention Coverage for Women's Health and Well-Being*, HUMAN RES. & SERVS. ADMIN. AGENCY, https://www.hrsa.gov/womens-guidelines (last visited Dec. 2022).

119. In one particularly chilling example, during a focus group convened by researchers studying the effect of Tennessee's fetal assault law, one woman affected by that law reported that, "when I was pregnant, I was scared to death to have that open relationship with my doctor because the laws in effect prevented . . . it from being a care issue. It became a law, a liability issue. I was freaking terrified." *See* BACH, *supra* note 20, at 130–31.

they are fearful that their health information may in the future be used against them. A comparison to the utilization of healthcare services by undocumented persons (or even documented persons from families that include undocumented persons) during increased Immigration and Customs Enforcement (ICE) is apposite. Research has shown that Hispanic respondents were less likely to use a regular healthcare provider or have an annual checkup when there was increased ICE activity in their state[120] as well as healthcare avoidance, stress, and anxiety.[121]

Finally, as women react to the post-*Dobbs* world and the perils associated with some of their online behaviors, it may not only be period trackers that they delete.[122] Mobile technologies have been deployed to improve health behaviors,[123] empower patients,[124] and increase patients' engagement with their own health.[125] Yet, post-*Dobbs* prosecutions may broadly chill the use of health-related technologies or even technologically mediated care, such as telehealth.[126] In the dystopian future triggered by *Dobbs*, women will find the technologies they rely on for their health turned against them as tools of surveillance.

As is the case in pregnancy prosecution generally, these privacy harms will be borne disproportionately by those who are already subjected to surveillance and criminalization. Scholars have long documented the ways in which privacy is severely compromised and often non-existent for those who are poor, for

120. *See* Abigal S. Friedman & Atheendar S. Venkataramani, *Chilling Effects: US Immigration Enforcement and Health Care Seeking Among Hispanic Adults*, 40 HEALTH AFF. (MILLWOOD) 1056 (2021).

121. *See* Karen Hacker, Jocelyn Chu, Lisa Arsenault & Robert P. Marlin, *Provider's Perspectives on the Impact of Immigration and Customs Enforcement (ICE) Activity on Immigrant Health*, 23 J. HEALTH CARE FOR POOR & UNDERSERVED 651, 655 (2012).

122. Flora Garamvolgyi, *Why US Women Are Deleting Their Period Tracking Apps*, GUARDIAN (June 28, 2022), https://www.theguardian.com/world/2022/jun/28/why-us-woman-are-deleting-their-period-tracking-apps.

123. Myeunghee Han & Eunjoo Lee, *Effectiveness of Mobile Health Application Use to Improve Health Behavior Changes: A Systematic Review of Randomized Controlled Trials*, 24 HEALTHCARE INFORMATICS RSCH. 207 (2018).

124. Emily May, *How Digital Apps Are Empowering Patients*, DELOITTE (Oct. 19, 2021), https://www2.deloitte.com/us/en/blog/health-care-blog/2021/how-digital-health-apps-are-empowering-patients.html.

125. Tim Wood, *Patient Engagement Technology & Its Role in Healthcare*, J2 INTERACTIVE, (Oct. 25, 2021), https://www.j2interactive.com/blog/patient-engagement-technology/.

126. Oliver J. Kim, *Dobbs and Telehealth: What's the Impact?*, BIPARTISAN POL'Y CTR. (Aug. 16, 2022), https://bipartisanpolicy.org/blog/dobbs-and-telehealth/.

those who are Black and Brown, and for those who seek social welfare support.[127]

An analysis of the various informational privacy harms that may follow the fall of *Roe* is a critical step in understanding the future role of the HIPAA Privacy Rule to protect patients' reproductive autonomy. The Privacy Rule only applies to "covered entities," typically most healthcare insurers and healthcare providers[128] and only with regard to "protected health information (PHI)."[129] Developers or providers of fertility and period tracking apps, mapping or search services, text and chat apps, and data brokers typically are not covered entities and HIPAA will not apply except in rare cases where a healthcare provider or its "business associate" (BA)[130] provided the app or service in question. Therefore, HIPAA will not apply even though a developer, service provider, or aggregator is holding personal health information.[131]

It follows that HIPAA's application is limited to cases of disclosure of PHI held in confidence by insurers or healthcare providers or their employees.[132] PHI may not be disclosed by covered entities unless authorized by the patient[133] or as permitted or required under the Privacy Rule.[134]

The impact of state whistleblower protections to, say, a healthcare employee who discloses abortion-related information is an open question; in general, the HIPAA Privacy Rule preempts state law, unless the latter is more protective of PHI.[135] It is unlikely that the Secretary would apply the public health "compelling need"[136] or other exceptions to whistleblowers or other state enforcement processes.[137] Notwithstanding, there are specific exceptions permitting disclosure in judicial or administrative proceedings such as in

127. *See, e.g.*, KHIARA BRIDGES, THE POVERTY OF PRIVACY RIGHTS (2017); Priscilla Ocen, *The New Racially Restrictive Covenant: Race, Welfare and the Policing of Black Women in Subsidized Housing*, 59 UCLA L. REV. 1540 (2012); Wendy A. Bach, *The Hyperregulatory State: Women, Race, Poverty and Support*, 25 YALE J.L. & FEMINISM 317 (2014).

128. 45 C.F.R. §§ 160.102, 160.103 (2013).

129. *Id.* § 160.103. The role of healthcare clearinghouses, an additional group of covered entities, is outside the scope of this Article.

130. *Id.*

131. *See, e.g.*, Nicolas P. Terry, *Big Data Proxies and Health Privacy Exceptionalism*, 24 HEALTH MATRIX 65, 87 (2014); Terry, *supra* note 90, at 95.

132. 45 C.F.R. § 164.502(a) (2013).

133. *Id.* § 164.508.

134. *Id.* § 164.502.

135. *Id.* § 160.202.

136. *Id.* § 160.203.

137. *Id.* § 160.204.

response to subpoena or discovery request[138] or to law enforcement in the case of warrants, subpoenas, and similar demands or requests.[139]

IV. HIPAA GESTALT V. HIPAA REALITY

A mythology of generalized health privacy protection has emerged around HIPAA. Some claims about its scope are simply risible such as when a serving Congressperson was asked about her vaccination status and replied, "Your . . . question is a violation of my HIPAA rights."[140] In fact, there is a long history of the Privacy Rule being cited as a barrier to the most innocuous or incidental discussions of patients and refusals by providers to share information with family members.[141] Providers who have been criticized for failure to share patient information will often cite HIPAA restrictions rather than admit to their own outdated technologies.[142] Often the HIPAA myth is rooted in understandable but nevertheless overly cautious reactions by healthcare workers to HIPAA and its sanctions.[143] On other occasions, the over-citation of HIPAA is more disturbing, such as when reports surfaced that HIPAA sanctions have been used to intimidate whistleblowers.[144] The sobering reality is that HIPAA, the nation's preeminent health privacy law, can address only a small number of post-*Dobbs* privacy issues.

---

138. *Id.* § 164.512(e).

139. *Id.* § 164.512(f)(1)(ii); *see also id.* § 164.103 (defining "[r]equired by law").

140. Philip Bump, *That's Not How Any of This Works, Marjorie Taylor Greene*, WASH. POST, (July 21, 2021), https://www.washingtonpost.com/politics/2021/07/21/thats-not-how-any-this-works-marjorie-taylor-greene/; @Acyn, TWITTER (July 20, 2021, 2:10 PM), https://twitter.com/Acyn/status/1417592852759007236.

141. *See* Paula Span, *Hipaa's Use as Code of Silence Often Misinterprets the Law*, N.Y. TIMES (July 17, 2015), https://www.nytimes.com/2015/07/21/health/hipaas-use-as-code-of-silence-often-misinterprets-the-law.html; *see also When Health Care Providers May Communicate About You with Your Family, Friends, or Others Involved in Your Care*, U.S. DEP'T HEALTH HUM. SERVS., OFF. CIV. RTS. (June 8, 2020), https://www.hhs.gov/sites/default/files/ocr/privacy/hipaa/understanding/consumers/consumer_ffg.pdf.

142. Christina Farr, *Consumer Privacy Laws Are Not to Blame for Health Care's Biggest Mess*, CNBC (Jan. 16, 2018), https://www.cnbc.com/2018/01/16/hipaa-not-reason-for-difficult-medical-record-sharing-commentary.html; *see also 11 Debunked Myths About HIPAA and Medical Records Privacy for Patients*, HIPAA SEC. SUITE (Jan. 15, 2019), https://hipaasecuritysuite.com/11-debunked-myths-about-hipaa-and-medical-records-privacy-for-patients/.

143. *See* Bryan K. Touchet, Stephanie R. Drummond & William R. Yates, *The Impact of Fear of HIPAA Violation on Patient Care*, 55 PSYCHIATRIC SERVS. 575, 575–76 (2004).

144. Joe Davidson, *VA Uses Patient Privacy to Go After Whistleblowers, Critics Say*, WASH. POST (July 17, 2014), https://www.washingtonpost.com/politics/federal_government/va-uses-patient-privacy-to-go-after-whistleblowers-critics-say/2014/07/17/bafa7a02-0dcb-11e4-b8e5-d0de80767fc2_story.html.

A. PRIVACY VERSUS CONFIDENTIALITY

Judged as a data protection law, the HIPAA Privacy Rule is nothing more than a modest endeavor. It employs a downstream data protection model that seeks to contain collected health information within the healthcare system by prohibiting its migration to non-healthcare parties. HIPAA does not in any way control or regulate the collection of patient data as would an upstream, collection-focused "privacy" model.[145] A more accurate description of the Privacy Rule would be "the doctor/hospital/insurer" confidentiality rule."[146] HIPAA regulates a relatively narrow cohort of data custodians, traditional health-care providers, and provides detailed guidance as to the occasions when disclosure may be authorized,[147] permitted, or required.[148] However, it is a mistake to overstate its scope and view it as a law providing broad or unqualified protection of health information.

B. HEALTH INFORMATION CURATED OUTSIDE OF THE HEALTHCARE SYSTEM

The root of HIPAA's greatest limitation is that its scope is limited to a cohort of data custodians rather than to a type of data. Its "original sin" was that it was structured around a group of identified health-care data custodians rather than *anyone* collecting or disclosing health-care data.[149] Because of the limitation to HIPAA-covered entities or their BAs the HIPAA rules seldom will apply to web or app-based consumer-facing health technologies that, for example, enable patient-accessed, -generated, or -curated healthcare information.[150] This limited scope can be illustrated by observing the transfer of an ob-gyn medical record from a provider to the patient's on-device health app, a function that has been encouraged by the federal government.[151] Such data are non-rival and so they can exist in more than one place, yet with distinct legal protections. The records stored on the provider's EHR would be protected by the HIPAA Privacy Rule, but the patient's copy stored on their mobile device would not. The latter would exist in what is sometimes called

145. Nicolas P. Terry, *Big Data Proxies and Health Privacy Exceptionalism*, 24 HEALTH MATRIX 65, 87 (2014).

146. Nicolas P. Terry, *Regulatory Disruption and Arbitrage in Health-Care Data Protection*, 17 YALE J. HEALTH POL'Y, L. & ETHICS 143, 162 (2017).

147. 45 C.F.R. § 164.508 (2013).

148. *Id.* § 164.502 (2013).

149. Terry, *supra* note 146, at 164.

150. Terry, *supra* note 90, at 94.

151. *See, e.g.*, Stephen Barlas, *HHS Proposes Steps Toward Health Data Interoperability CMS and ONC Proposals Would Implement Cures Act*, 44 PHARMACY & THERAPEUTICS 347, 348–49 (2019).

the HIPAA-free zone and would be relatively unprotected,[152] although as already discussed both versions are likely exposable by subpoena or warrant.

C. *DOBBS*, HIPAA EXCEPTIONS, AND REPRODUCTIVE HEALTHCARE PRIVACY

In truth, the HIPAA Privacy Rule's list of permitted disclosures has always tainted the Rule as reading "less like a list of confidentiality protections and more like a catalogue of exceptions and, specifically, process rules for authorizations to avoid confidentiality."[153] Within the Rule, there are exceptions to the general rule of non-disclosure, including authorization, required disclosures, and permitted disclosures.

With very few exceptions the patient themselves can authorize the disclosure of their PHI. Consent has not been an explicit part of the Privacy Rule since 2002,[154] where requirements for initial consent to share health information with a provider were removed.[155] Authorization is a special form of consent with quite specific requirements[156] and is somewhat akin to informed consent.[157] Required disclosures are quite limited, arising when patients request access to their records or in the case of an HHS enforcement procedure.[158]

Permitted (in the sense that the patient's authorization is not required) disclosures apply in a broad range of situations including sharing information for essentially internal use (treatment, payment, and healthcare operations).[159] Most concerning, in the context of *Dobbs,* however, are the myriad of circumstances permitting disclosure. In short, despite the efforts of the Biden administration to reassure patients and providers, the reality is that HIPAA, even if rigorously enforced, contains significant exceptions that can undermine the privacy of patient information in a context in which a state criminalizes or makes relevant to child welfare cases additional aspects of reproductive conduct.

---

152. *See generally* Terry, *supra* note 90 at 95.

153. Terry & Francis, *supra* note 98, at 717.

154. *See* 67 Fed. Reg. 53182, 53255 (Aug. 14, 2002).

155. Standards for Privacy of Individually Identifiable Health Information, 45 C.F.R. § 164.506(a) (2000).

156. *Id.* § 164.508.

157. *See generally What Is the Difference Between "Consent" and "Authorization" Under the HIPAA Privacy Rule?*, U.S. DEP'T HEALTH & HUM. SERVS., (Dec. 28, 2022) https://www.hhs.gov/hipaa/for-professionals/faq/264/what-is-the-difference-between-consent-and-authorization/index.html.

158. *See* 45 C.F.R. § 164.502(a) (2023).

159. *Id.* § 164.506.

First, and most significantly, HIPAA allows disclosure "as required by law."[160] The regulations specify that the covered entity "may use or disclose protected health information to the extent that such use or disclosure is required by law and the use or disclosure complies with and is limited to the relevant requirements of such law."[161] This regulation clearly applies both to federal and state law. It further instructs that the covered entity must "meet the requirements" described in other, more specific subsections of the regulations that cover various situations in which a disclosure might be "required by law." Relevant here are the rules concerning disclosures for "law enforcement purposes"[162] and disclosures for "judicial and administrative proceedings."[163]

Several aspects of the law enforcement exception are important here. First, HIPAA allows disclosure to law enforcement to comply with a specific law requiring disclosure of certain types of wounds or other physical injuries. The paradigmatic example here is the reporting of gunshot victims. But this exception is not limited to those circumstances. If a state legislature required reporting of pregnancy-related conditions like miscarriage, HIPAA would allow those disclosures. As noted above, long before *Dobbs*, individuals have been prosecuted for engaging in self-managed abortions. A state that is concerned that miscarriages might be the result of self-managed abortion could require disclosure of healthcare records that contain evidence of miscarriages or other pregnancy complications, which could open the door to further prosecutions of this nature.

Second, HIPAA allows disclosure to comply with a court order, court-ordered warrant or a subpoena or summons, to comply with a grand jury subpoena, or, in slightly more limited circumstances, to comply with administrative requests for information. Once a prosecution is commenced, courts can authorize the disclosure of significant parts of healthcare records.

The HIPAA crime victim exception is also concerning. Under HIPAA covered entities may disclose information in response to police requests concerning an individual who is suspected to be a victim of a crime.[164] While generally, the crime victim must consent to disclosure, if the crime victim

160. *Id.* § 164.512(a).
161. *Id.*
162. *Id.* § 164.512(f).
163. *Id.* § 164.512(e).
164. *Id.* § 164.512(f)(3).

cannot consent because of "incapacity" the covered entity can disclose without consent.[165]

The concern here involves the growing state law trend defining a fetus as a victim of a crime. By definition, the fetus would likely be "incapacitated" under the HIPAA rules, allowing for disclosure without consent. Currently 38 states have fetal homicide laws.[166] While many of these laws explicitly exempt pregnant women from prosecution under these statutes, this is not universally true. Moreover, nothing after *Dobbs* bars states from revising those statutes and prosecuting women who they believe have attempted to abort their fetuses in violation of state law. In addition, there is a long history of prosecutions of pregnant women for conduct during pregnancy even in the face of laws that purport to exempt prosecution of the woman herself. As noted above, journalists, advocates, and scholars already have documented thousands of prosecutions and forced interventions involving pregnancy.[167] In addition, at least two states—South Carolina and Alabama—have permitted prosecution for pregnancy-related conduct against individuals who were pregnant.[168] Finally, while states may continue to exempt the pregnant person from prosecution, that does not render the crime victim exception irrelevant. Take for example, a patient who discloses to a healthcare provider that she obtained abortion-inducing medication from a particular source. That fetus could be a "crime victim" and information about who provided the medication is still relevant and disclosable under this exception.

In the civil law context, HIPAA also provides some exceptions that raise concerns. For example, HIPAA allows disclosure of protected health information to "a public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect." While standards about what constitutes reportable information as well as who must report vary significantly by state,[169] the federal Child Abuse Prevention and Treatment Act (CAPTA) requires every state, as a condition of federal funding, to have in place "provisions or procedures for an individual to report known and suspected instances of child abuse and neglect, including a State law for

165. *Id.* § 164.512(f)(3)(ii) (noting that in the case of the crime victim not consenting disclosure is subject to the additional requirements at 164.512(f)(3)(ii)(A)–(C)).

166. *Who Do Fetal Homicide Laws Protect? An Analysis for a Post-Roe America*, PREGNANCY JUST., https://www.pregnancyjusticeus.org/wp-content/uploads/2022/12/fetal-homicide-brief-with-appendix-UPDATED.pdf (last visited July 29, 2023).

167. *See supra* notes 11–24 and accompanying text.

168. *See* Whitner v. State, 492 S.E.2d 777 (S.C. 1997); *In re* Ankrom, 152 So. 3d 397 (Ala. 2013).

169. *Mandatory Reporters of Child Abuse and Neglect*, CHILD WELFARE INFOR. GATEWAY, https://www.childwelfare.gov/pubpdfs/manda.pdf (last visited July 29, 2023).

mandatory reporting by individuals required to report such instances."[170] In every state, healthcare providers are included among those who must report.[171]

Again, the concern here is about laws focused on fetal harm. As detailed above, at least twenty-six states require health-care providers to report when they treat infants who show evidence at birth of having been exposed to drugs, alcohol, or other controlled substances," and in twenty-three states and the District of Columbia, "prenatal exposure to controlled substances is included in definitions of child abuse or neglect in civil statutes, regulations, or agency policies."[172] In addition, in Texas at least, state law authorizes the filing of a petition for termination of parental rights before the birth of a child[173] and courts have made clear that such a termination can be based on pregnancy-related conduct.[174] Finally, in the context of substance use and pregnancy, three states (Minnesota, Wisconsin and South Dakota) specifically authorize the civil commitment of pregnant people to protect the fetus they are carrying. One can easily imagine, after *Dobbs,* states going further and defining either abortion or the intention to secure an abortion as child abuse. Such a possibility raises the serious concern that a person who discloses to a healthcare provider that she intends to obtain an abortion could end up reported to the child welfare system.

Also in the civil realm, the privacy rule specifies that a covered entity "may disclose protected health information in the course of any judicial or administrative proceeding . . . in response to an order of a court or administrative tribunal, provided that the covered entity discloses only the protected health information expressly authorized by such order."[175] In addition, a covered entity may also disclose information pursuant to a "subpoena, discovery request or other lawful process" provided that the entity receives assurances regarding notice to the individual and efforts to obtain a qualified protected order in the litigation.[176] Texas has already turned to civil enforcement as a means of preventing abortion. In this context the civil law exceptions raise serious concerns.

Finally, the privacy rule allows for disclosures, in some circumstances, in which the covered entity concludes that they possess information that is

170. 42 U.S.C. § 5106a(b)(2)(B)(i).

171. CHILD WELFARE INFOR. GATEWAY, *supra* note 169.

172. *Id.*

173. TEX. FAM. CODE ANN. § 161.102 (1995).

174. *See, e.g.*, *In re* K.L.B., 2009 WL 3444833 (Tex. App. July 16, 2009) (holding that the Texas statute concerning abuse and neglect can include pregnancy-related conduct).

175. 45 C.F.R. § 164.512I (2023).

176. *Id.* § 164.512(e)(ii).

necessary to prevent a "serious threat to health or safety."[177] Again, in a state in which abortion is largely outlawed, a court could easily conclude that a disclosure that a person intends to obtain an abortion falls under this exception.

Although not applicable to sharing with other treatment providers[178] or when required by law,[179] HIPAA does have an important disclosure-minimizing requirement that otherwise applies. The "minimum necessary" standard[180] requires covered entities to evaluate their practices and enhance safeguards as needed to limit unnecessary or inappropriate access to and disclosure of protected health information."[181]

In summary, while HIPAA provides a reasonably strong confidentiality rule, it is limited in its applicability, has almost zero applicability in the mobile health space, and is subject to a long list of exceptions. The Office for Civil Rights, the HHS enforcement office, is not large and primarily relies on complaints and self-reporting through breach notifications to trigger investigations. The relatively small number of cases brought tend to be high profile ones or exemplars[182] and HHS-OCR has been criticized for failing to enforce smaller or repeat violations.[183]

D. REPRODUCTIVE INFORMATION AND HIPAA NON-COMPLIANCE

In the area of reproductive healthcare criminalization specifically there is significant evidence of HIPAA non-compliance.[184] Returning for a moment to the Tennessee fetal assault prosecutions and the plethora of PHI contained in the criminal court files, it is fair to question whether that PHI was all lawfully disclosed. To be fair, there are plausible legal exceptions to HIPAA that could

177. *Id.* § 164.512(j).

178. *Id.* § 164.502(b)(2)(i).

179. *Id.* § 164.502(b)(2)(v).

180. *Id.* §§ 164.502(b), 164.514(d).

181. *Minimum Necessary Requirement*, U.S. DEP'T HEALTH & HUM. SERVS. (Apr. 4, 2003), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/minimum-necessary-requirement/index.html.

182. *See generally* U.S. DEP'T HEALTH & HUMAN SERVS., ANNUAL REPORT TO CONGRESS ON HIPAA PRIVACY, SECURITY, AND BREACH NOTIFICATION RULE COMPLIANCE FOR CALENDAR YEAR 2021 (Feb. 17, 2023), https://www.hhs.gov/sites/default/files/compliance-report-to-congress-2021.pdf.

183. *See, e.g.*, Charles Ornstein & Annie Waldman, *Few Consequences for Health Privacy Law's Repeat Offenders*, PROPUBLICA (Dec. 29, 2015), https://www.propublica.org/article/few-consequences-for-health-privacy-law-repeat-offenders.

184. Although this Article focuses on healthcare involving pregnancy, scholars have documented extensive evidence of widespread disclosure of presumptively confidential information particularly in the emergency room setting. *See, e.g.*, Ji Seon Song, *Cops in Scrubs*, 48 FLA. ST. U.L. REV. 861, 885–87 (2021).

have resulted in these disclosures. So perhaps all the specific health information contained in the criminal files was disclosed to a child welfare agency who then disclosed it to police or prosecutors. On the other hand, the Tennessee study found that none of the criminal files contained any court orders, subpoenas or other written legal processes. So perhaps these disclosures were all lawful results of disclosures to child welfare agencies, or perhaps compliance with HIPAA in this context was not entirely legal.

The concern regarding the legality of these disclosures was heightened as the team conducted the qualitative interview portion of the study. As one prosecutor explained,

> If we needed to talk to a nurse about a situation, or we needed additional records, we could get those records. If we needed to go down to a facility and meet with people, and talk to them about it, or needed information, they always seemed very . . . I never had any obstacles with the local hospitals at all.[185]

Similarly, in another interview of a prosecutor the team asked whether their office faces any resistance from hospitals or doctors about testifying or sharing information. The prosecutor responded, "no, never a problem, it would be the opposite."[186]

The HIPAA regulations require that, absent narrow emergency circumstances, prosecutors would have to issue a subpoena or obtain another court order to get such information, but it appears quite clear that is not the practice on the ground. So, there is at least some evidence on the ground that in the specific area of reproductive healthcare and criminalization, HIPAA is underenforced. To the extent that the Biden administration is signaling, through its guidance, that it intends to enforce the protections available in the privacy rule, this is good news for patients seeking care. But even rigorously enforced, HIPAA does not offer sufficient protection.

V. EXPANDING LEGAL PROTECTIONS POST-*DOBBS*

The Biden administration has been scrambling to find a federal legal response to the state laws ecstatically embracing an end to federal constitutional scrutiny of reproductive health limitations. Additionally, policymakers must endure a very different judicio-political environment from that of *Roe* and the 1970s. The destruction of *Roe* has become a singular policy for one of our two dominant political parties while abortion became the

185. BACH, *supra* note 20, at 133.
186. *Id.*

predominant litmus test for Senate confirmation of justices nominated to the Supreme Court.[187] In turn, that court seems more respectful of state rights (increasingly and questionably equating democratic liberty with state decision-making) and keen to curtail federal agency powers. For example, both *Chevron* "Zero"[188] analysis and the "major questions" doctrine[189] could sharply curtail federal attempts to use rulemaking to preserve substantive abortion rights or related informational privacy protections. With its options limited it is not surprising that the Biden administration would cast a broad net looking for legal support.

Given that access to abortion services is a subset of access to healthcare services generally, it was natural for the Biden administration to attempt to leverage the Emergency Medical Treatment and Labor Act (EMTALA), a broad federal statute that requires emergency departments to, *inter alia*, screen and stabilize persons including those in labor.[190] In a July 2022 guidance, the Centers for Medicare and Medicaid Services (CMS) noted that screenings for a medical emergency are matters for clinicians and "include, but are not limited to: ectopic pregnancy, complications of pregnancy loss, or emergent hypertensive disorders, such as preeclampsia with severe features."[191] The guidance also noted that "[i]f a physician believes that a pregnant patient presenting at an emergency department is experiencing an emergency medical condition as defined by EMTALA, and that abortion is the stabilizing treatment necessary to resolve that condition, the physician must provide that treatment" and that EMTALA preempts state law.[192] In *Texas v. Becerra*, the District Court placed this guidance under a nationwide injunction.[193] However, the EMTALA argument fared better before a District Court in Idaho. At issue

187. *See, e.g.*, Carl Hulse, *Kavanaugh Gave Private Assurances. Collins Says He 'Misled' Her*, N.Y. TIMES (Jun. 24, 2022), https://www.nytimes.com/2022/06/24/us/roe-kavanaugh-collins-notes.html; Leigh Ann Caldwell & Julie Tsirkin, *Conservatives push anti-abortion rights as litmus test for next nominee*, NBC NEWS (Sept. 21, 2020), https://www.nbcnews.com/politics/congress/conservatives-push-anti-abortion-rights-litmus-test-next-nominee-n1240628.

188. *See, e.g.*, King v. Burwell, 576 U.S. 473, 485 (2015). *See generally* Cass R. Sunstein, "*Chevron Step Zero*," 92 VA. L. REV. 187 (2013) (describing Supreme Court jurisprudence concerning the circumstances under which courts should apply *Chevron* deference and seeking to resolve that doctrine).

189. *See, e.g.*, W. Virginia v. Env't Prot. Agency, 142 S. Ct. 2587, 2595 (2022). *See generally* Mila Sohoni, *The Major Questions Quartet*, 136 HARV. L. REV. 262 (2022).

190. Social Security Act, 42 U.S.C. § 1395dd.

191. CTR. MEDICARE & MEDICAID SERVS., QSO-21-22-HOSPITALS, REINFORCEMENT OF EMTALA OBLIGATIONS SPECIFIC TO PATIENTS WHO ARE PREGNANT OR ARE EXPERIENCING PREGNANCY LOSS (Aug. 25, 2022).

192. *Id.*

193. Texas v. Becerra, No. 5:22-CV-185-H, 2022 WL 3639525 (N.D. Tex. Aug. 23, 2022) at *19–*26 (arguing that the guidance "goes well beyond EMTALA's text.").

was the state's abortion trigger law which bans all abortions,[194] leading the Biden administration to seek to enjoin the law to the extent it conflicted with EMTALA.[195] Judge Winmill reflected on the decisional and informational lacunae *Dobbs* opened up for "the pregnant patient, laying on a gurney in an emergency room facing the terrifying prospect of a pregnancy complication that may claim her life [and the unimaginable] anxiety and fear she will experience if her doctors feel hobbled by an Idaho law that does not allow them to provide the medical care necessary to preserve her health and life."[196]

Whether requesting it or not, the Biden administration clearly is hoping for assistance from states that are less hostile to reproductive services. Before *Dobbs*, researchers increasingly identified "abortion deserts"[197] as the Supreme Court reduced the protections initially provided by *Roe* and states passed stricter restrictions such as TRAP laws[198] aimed at threading *Casey*'s undue burden test.[199] After *Dobbs*, attention has shifted somewhat to identifying "abortion access islands."[200] Some of these "islands," states that increasingly provide abortion services to non-residents, have themselves legislated in the wake of *Dobbs*. For example, Colorado,[201] Nevada,[202] New York,[203]

194. *See* IDAHO CODE § 18-622 (2020).

195. U.S. v. Idaho, 623 F. Supp. 3d 1096, 1105 (D. Idaho 2022).

196. *Id.* at *14. Notwithstanding the argument that the Biden administration overreached with its EMTALA guidance, there are press reports of hospitals being investigated for breaching the statute's screen and stabilize mandate. *See, e.g.*, Harris Meyer, *Hospital Investigated for Allegedly Denying an Emergency Abortion After Patient's Water Broke*, KFF HEALTH NEWS (Nov. 1, 2022), https://khn.org/news/article/emtala-missouri-hospital-investigated-emergency-abortion/.

197. *See, e.g.*, Alice F. Cartwrigh, Mihiri Karunaratne, Jill Barr-Walker, Nicole E. Johns, and Ushma D. Upadhyay, *Identifying National Availability of Abortion Care and Distance from Major US Cities: Systematic Online Search*, 20 J. OF MED. INTERNET RSCH. 186, 192 (2018).

198. *See Targeted Regulation of Abortion Providers (TRAP) Laws*, GUTTMACHER INST. (Jan. 22, 2020), https://www.guttmacher.org/state-policy/explore/targeted-regulation-abortion-providers.

199. *See* Planned Parenthood of Se. Pennsylvania v. Casey, 505 U.S. 833, 874 (1992) ("Only where state regulation imposes an undue burden on a woman's ability to make this decision does the power of the State reach into the heart of the liberty protected by the Due Process Clause").

200. *See, e.g.*, Jessica Lussenhop, *Minnesota Set to Become "Abortion Access Island" in the Midwest, but for Whom?*, PROPUBLICA (Aug. 25, 2022), https://www.propublica.org/article/minnesota-abortion-access-island-barriers.

201. S.B. 23-188, 74th Gen. Assemb., Reg. Sess. (Colo. 2023).

202. *See* Nev. Exec. Order 2022-08, Protecting Access to Reproductive Health Services In Nevada (June 28, 2022), https://gov.nv.gov/layouts/full_page.aspx?id=360658.

203. *See* Harris Meyer, *Hospital Investigated for Allegedly Denying an Emergency Abortion After Patient's Water Broke*, KFF HEALTH NEWS (Nov. 1, 2022), https://kffhealthnews.org/news/article/emtala-missouri-hospital-investigated-emergency-abortion/.

Connecticut,[204] and Washington[205] have passed laws or issued directives protecting their states' providers from actions in other states and prohibits law enforcement and courts from cooperating with out of state civil or criminal actions. Meanwhile, the Governor of New Mexico has announced the building of a new abortion clinic near the Texas border.[206] Of particular relevance to informational privacy is the Governor of California's Executive Order that, *inter alia*, prohibits state agencies or employees from "providing any information, including patient medical records, patient-level data, or related billing information . . . [regarding] . . . reproductive healthcare services legally performed or provided in California."[207] The Governor also used some of his reelection funds to buy advertisements on billboards in several states with restrictive abortion laws stating, "[Y]ou do not need to be a California resident to receive abortion services."[208]

VI. REFORMING INFORMATIONAL PRIVACY

There is an inverse relationship between healthcare access and health privacy. As healthcare access increases and patients are protected against discrimination based on health (for example, by prohibiting insurers from medical underwriting[209]), the need for health privacy should decrease.[210] *Dobbs* suggests a cycle moving in the opposite direction; because of decreasing of healthcare access (here, access to reproductive healthcare services) there is an urgent need to increase privacy protection for women of reproductive age.

Section 4 of President Biden's July 2022 Executive Order on "Protecting Access to Reproductive Healthcare Services" directs the Attorney-General, the Secretary of Homeland Security, the Chair of the FTC, and the Secretary of the HHS to address the protection of privacy, safety, and security regarding

204. *See* N.Y. CRIM. PROC. LAW § 570.17 (2022); Substitute H.B. 5414, Public Act No. 22-19., Reg. Sess. (Conn. 2022).

205. *See* Off. Governor. Jay Inslee, Directive of the Governor 22-12 (June 30, 2022), https://www.governor.wa.gov/sites/default/files/directive/22-12%20-%20Prohibiting%20assistance%20with%20interstate%20abortion%20investigations%20(tmp).pdf?.

206. *See* N.M. Exec. Order 2022-123, Expanding Access to Reproductive Health Care Services (Aug. 31, 2022), https://www.governor.state.nm.us/wp-content/uploads/2022/08/Executive-Order-2022-123.pdf.

207. Cal. Exec. Order N-12-22 (June 27, 2022), https://www.gov.ca.gov/wp-content/uploads/2022/06/6.27.22-EO-N-12-22-Reproductive-Freedom.pdf.

208. David Weigel, *Calif. Governor Rents Billboards in Red States to Tout Abortion Access*, WASH. POST (Sept. 15, 2022), https://www.washingtonpost.com/politics/2022/09/15/gavin-newsome-abortion/.

209. *See, e.g.*, 45 C.F.R. § 147.108 (2015).

210. Nicolas P. Terry & Christine Coughlin, *A Virtuous Circle: How Health Solidarity Could Prompt Recalibration of Privacy and Improve Data and Research*, 74 OKLA. L. REV. 51, 52 (2021).

reproductive services.[211] HHS and FTC were directed to consider actions respectively under HIPAA and the FTC Act, respectively.

A. EXPANDING HIPAA

The question is, does HHS have the power to better regulate the reproductive services informational space, sub-regulatory guidance aside?[212] Given the voluminous provisions that HHS promulgated in the two decades after HIPAA became law, the HIPAA enabling statute was extraordinarily bareboned. The explanation is relatively obvious: Congress was essentially addressing its later self, establishing the scaffolding for its future legislation. However, and pursuant to the initial statute,[213] when that option expired, the Secretary's recommendations were turned into a final rule.

Among the rudimentary provisions of the original HIPAA statute are three that made for serious limitations going forward and will reduce HHS's options post-*Dobbs*. First, the statute clearly regulates by reference to certain limited cohorts of healthcare persons (health plans, healthcare clearinghouses, and most healthcare providers) holding personal health information rather than *any* persons holding health data.[214] Second, the enabling statute has a broad carve out for public health activities "under any law providing for the reporting of disease or injury, child abuse, birth, or death, public health surveillance, or public health investigation or intervention."[215] Overall, and as noted by the Fourth Circuit, the legislation provided "a clear mandate from Congress directing HHS to act in accordance with the intelligible principles set forth in HIPAA [with] clear limits upon the scope of that authority and the type of entities whose actions are to be regulated."[216] However, neither HIPAA nor later legislation suggest any broader legislative mandate that could right many of the informational privacy wrongs that initially flowed from evolving personal technologies and now from *Dobbs*.

---

211. Exec. Order 14076, Protecting Access to Reproductive Healthcare Services, 87 Fed. Reg. 42053 (July 8, 2022), https://www.whitehouse.gov/briefing-room/presidential-actions/2022/07/08/executive-order-on-protecting-access-to-reproductive-healthcare-services/.

212. *See Guidance on HIPAA Privacy Rule and Disclosures of Information Relating to Reproductive Health Care*, U.S. DEP'T HEALTH & HUMAN SERVS. (June 29, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/phi-reproductive-health/index.html; *Guidance on Protecting the Privacy and Security of Your Health Information When Using Your Personal Cell Phone or Tablet*, U.S. DEP'T HEALTH & HUMAN SERVS. (June 29, 2022), https://www.hhs.gov/hipaa/for-professionals/privacy/guidance/cell-phone-hipaa/index.html.

213. Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, Sec. 264(c)(1), 110 Stat. 1936 (1996).

214. 42 U.S.C. § 1320d(1); *see also* 42 U.S.C. § 300jj(3).

215. 42 U.S.C. § 1320d(7)(b).

216. South Carolina Medical Ass'n v. Thompson, 327 F.3d 346, 352 (4th Cir. 2003).

The 1999 proposed rule,[217] the initial final rule,[218] and, after the Secretary reopened the public comment period,[219] the 2002 final rule with modifications addressing topics such as consent and marketing[220] were all enacted pursuant to the original HIPAA statute and seemed clearly within the enabling statute's scope. In 2009, Congress passed the HITECH Act authorizing, *inter alia*, the extension of certain Privacy Rule provisions directly to the business associates of covered entities,[221] new notification of breach provisions,[222] further limitations on disclosures of PHI for marketing purposes,[223] limitations on the sale of EHR data,[224] expansions of patient rights of access,[225] and improved enforcement.[226]

Other than an Interim final rule on enforcement[227] authorized by HITECH,[228] the only major regulatory action following the passage of HITECH was the so-called Omnibus Rule that HHS promulgated under HIPAA, HITECH, and GINA.[229] The Omnibus Rule made some

217. Standards for Privacy of Individually Identifiable Health Information, 64 Fed. Reg. 59918 (proposed Nov. 3, 1999) (to be codified at 45 C.F.R. pts. 160, 164).

218. Standards for Privacy of Individually Identifiable Health Information, 65 Fed. Reg. 82462 (Dec. 28, 2000) (to be codified at 45 C.F.R. pts. 160, 164).

219. Request for Comments, Standards for Privacy of Individually Identifiable Health Information, 66 Fed. Reg. 12738 (Feb. 28, 2001).

220. Standards for Privacy of Individually Identifiable Health Information, 67 Fed. Reg. 53183 (Aug. 14, 2002) (to be codified at 45 C.F.R. pts. 160, 164).

221. Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, 123 Stat. 226 (Feb. 17, 2009), § 13401, § 13404.

222. *Id.* at § 13402.

223. *Id.* at § 13406.

224. *Id.* at § 13405(d), further discussed below, text at n. 232.

225. *Id.* at § 13405(e).

226. *Id.* at § 13410.

227. *HIPAA Administrative Simplification: Enforcement, Interim final rule 67 FR 53182*, HEALTH & HUM. SERVS. (Oct. 30, 2009), https://www.govinfo.gov/content/pkg/FR-2002-08-14/pdf/02-20554.pdf.

228. Health Information Technology for Economic and Clinical Health (HITECH) Act, Title XIII of Division A and Title IV of Division B of the American Recovery and Reinvestment Act of 2009 (ARRA), Pub. L. No. 111-5, 123 Stat. 226 (Feb. 17, 2009), § 13410(d).

229. Modifications to the HIPAA Privacy, Security, Enforcement, and Breach Notification Rules Under the Health Information Technology for Economic and Clinical Health Act and the Genetic Information Nondiscrimination Act; Other Modifications to the HIPAA Rules, 78 Fed. Reg. 5566, 5702 (Jan. 25, 2013) (to be codified at 45 C.F.R. pt. 160–164), https://www.govinfo.gov/content/pkg/FR-2013-01-25/pdf/2013-01073.pdf. In the years that followed the Omnibus Rule there have been a series of relatively minor amendments to the Privacy Rule, e.g., Technical Corrections to the HIPAA Privacy, Security, and Enforcement Rules, 78 FR 34264 06/07/2013; 79 FR 7289 (February 6, 2014), https://

fundamental changes to the HIPAA model,[230] but HHS's reliance on specific language in HITECH arguably confirms that the original HIPAA statute lacked sufficient authority to make such changes.

For example, while it is likely that HHS always wanted to directly regulate "business associates," the original HIPAA Rule had to do so indirectly through BA contracts[231] because BAs were not included in the original HIPAA statute's list of regulated persons. The popularity of mobile health—and now the concerns raised in the wake of Dobbs—require extending health privacy beyond traditional healthcare stakeholders. However, the omnibus rule's extension of HIPAA beyond those stakeholders to their business associates was based on specific and limited statutory language, which suggests that HITECH had not meaningfully extended the regulatory scope. This was also the case with the regulation of non-traditional healthcare providers who supplied "personal health records" in the case of security breaches. Again, the statutory language ("vendor of personal health records"), albeit here directed at FTC rulemaking, was both precise and limited.[232]

Post-*Dobbs*, attention also has been paid to HIPAA's treatment of what are called "psychotherapy notes" keying on what appears to be exceptional status applied to a particular subset of health information. These are notes taken by a mental health professional "documenting or analyzing the contents of conversation during a private counseling session" and do not, for example, include typical medical records information such as medications or treatment plans.[233] HIPAA provides additional protection for these notes by requiring

www.govinfo.gov/content/pkg/FR-2014-02-06/html/2014-02280.htm; Health Insurance Portability and Accountability Act (HIPAA) Privacy Rule and the National Instant Criminal Background Check System (NICS), 81 Fed. Reg. 382, 396 (Jan. 6, 2016) (to be codified at 45 C.F.R. pt. 1), https://www.govinfo.gov/content/pkg/FR-2016-01-06/pdf/2015-33181.pdf. A more substantial NPRM, Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement, has been published but is limited to fragmentation and other matters internal to the healthcare system. Proposed Modifications to the HIPAA Privacy Rule to Support, and Remove Barriers to, Coordinated Care and Individual Engagement, 86 Fed. Reg. 6446, 6538 (Jan. 21, 2021) (to be codified at 45 C.F.R. pts. 160 and 164), https://www.govinfo.gov/content/pkg/FR-2021-01-21/pdf/2020-27157.pdf.

230. For a summary, see generally Melissa M. Goldstein & William F. Pewen, *The HIPAA Omnibus Rule: Implications for Public Health Policy and Practice*, 128 PUB. HEALTH REP. 554 (2013).

231. *Business Associate Contracts*, HEALTH & HUM. SERVS. (Jan. 25, 2013), https://www.hhs.gov/hipaa/for-professionals/covered-entities/sample-business-associate-agreement-provisions/index.html.

232. HITECH Act, § 13407; *see also* 16 C.F.R. § 318 (2009).

233. 45 C.F.R. § 164.501 (2013).

authorization for many uses[234] and limiting the patient's right of access.[235] Although this is a carve-out of a subset of information, psychotherapy notes do not provide a particularly persuasive analogy to reproductive information. These psychotherapy notes, sometimes called process notes,[236] are not health records in the sense that reproductive health documentation would be.

HITECH also provided new authority for HHS to require market inalienability for PHI.[237] This led to the Omnibus Rule's requirement that "a covered entity must obtain an authorization for any disclosure of protected health information which is a sale of protected health information . . . [s]uch authorization must state that the disclosure will result in remuneration to the covered entity."[238] Inalienability provisions are effective privacy tools. Could HITECH authorize some type of "criminal inalienability" rule prohibiting even warrant- or subpoena-authorized use of a person's health record in proceedings focused on reproductive health? Leaving aside the merit or workability of such a provision, the HITECH language is too limited to support such a rule.[239]

Notwithstanding these limitations, HIPAA's leaky faucet is overdue for reform. HHS should aim to reduce the use of healthcare information in prosecution and re-examine some of 'the broader exceptions to patient confidentiality, particularly those that bow too generously to state law, state agencies, state courts, and law enforcement.

These limited but nontrivial goals are partially reflected in the Notice of Proposed Rulemaking (NPRM) published by HHS in April 2023.[240] The agency had decided:

> "[To] provide heightened protections for another especially sensitive category of health information—PHI sought for the purposes of conducting a criminal, civil, or administrative investigation into or proceeding against any person in connection with seeking, obtaining,

234. *Id.* § 164.508(a)(2).

235. *Id.* § 164.524(a)(1)(i).

236. *See* Rebecca A. Clay, *Keeping Track, American Psychological Association*, AM. PSYCHOLOGICAL ASS'N (Jan. 2007), https://www.apa.org/gradpsych/2007/01/track (last visited Apr. 20, 2023) (discussing difference between "progress notes" and "process notes").

237. Health Information Technology for Economic and Clinical Health (HITECH) Act, Pub. L. No. 111-5, § 13405(d), 123 Stat. 226 (2009).

238. 45 C.F.R. § 164.508(a)(4) (2013).

239. *See* HITECH § 13405(d)(1) ("[A] covered entity or business associate shall not directly or indirectly receive remuneration in exchange for any protected health information of an individual.").

240. HIPAA Privacy Rule to Support Reproductive Health Care Privacy, 88 Fed. Reg. 23506 (Apr. 17, 2023) (to be codified at 45 C.F.R. pts. 160, 164) [hereinafter NPRM].

> providing, or facilitating reproductive health care that is lawful under the circumstances in which it is provided."[241]

In the proposed rule, disclosure for investigation or proceeding is prohibited only when the reproductive healthcare is "lawful."[242] The NPRM lists three situations: first, if the care is lawful in the state where performed;[243] second, if required or authorized by a federal law (such as EMTALA[244]);[245] or third, if the healthcare was lawful (including, for example, if a rape or incent exception applied[246]) but still under investigation.[247] The prohibition on disclosure will be operationalized by requiring the covered entity to condition some disclosures on the receipt of a signed attestation that the use for which the PHI is sought was not a prohibited use.[248]

While useful in some circumstances, the scope of these "heightened protections" fails to address many of the fundamental healthcare record privacy issues identified in this Article. First, the provisions themselves are quite narrow. Perhaps as a result, the proposed rule fails to address central preexisting dangers to healthcare privacy and fails to cut off a key source of disclosures that have been and are likely to be central to prosecutions.

The scope of these "heightened protections" is quite narrow. Most importantly, increasingly reproductive healthcare is *not* lawful. Fifteen states have enacted either total or effectively total (such as six week) bans[249] and this number is likely to increase. As such the NPRM's greatest impact is likely to be on information about abortions performed in abortion destination states when the state of residence asserts extraterritoriality for its investigations or proceedings and seeks to punish patients and those that assisted them.[250] The practical impact of the federal law authorization provision is less clear. As already discussed, the CMS guidance[251] asserting EMPTALA preemption has already met legal pushback from abortion restrictive states,[252] and it is unclear

241. *See* NPRM at 23509–10.
242. *Id.* at 23552 (proposed 45 C.F.R. § 164.502(a)(5)).
243. *Id.* (proposed 45 C.F.R. § 164.502(a)(5)(iii)(C)(1)).
244. *Id.* at 23531.
245. *Id.* at 23552 (proposed 45 C.F.R. § 164.502(a)(5)(iii)(C)(2)).
246. *See id.* at 23531.
247. *Id.* at 23552 (proposed 45 C.F.R. § 164.502(a)(5)(iii)(C)(3)).
248. *Id.* at 23553 (proposed 45 C.F.R. § 164.509).
249. *Tracking the States Where Abortion Is Now Banned*, N.Y. TIMES (July 24, 2023), https://www.nytimes.com/interactive/2022/us/abortion-laws-roe-v-wade.html.
250. *See supra* notes 30–32.
251. CTR. MEDICARE & MEDICAID SERVS., QSO-21-22-HOSPITALS, REINFORCEMENT OF EMTALA OBLIGATIONS SPECIFIC TO PATIENTS WHO ARE PREGNANT OR ARE EXPERIENCING PREGNANCY LOSS (Aug. 25, 2022).
252. *See supra* notes 190–196.

how healthcare providers faced with the legal indeterminacy around following federal over state law or *vice versa* will decided when presented with, say, a woman facing a miscarriage or ectopic pregnancy who needs pregnancy loss management. Finally, the "lawful" healthcare provision is sufficiently narrow such that it is likely to have minimal effects.

Second, the proposed changes fail to address the use of healthcare data in the circumstances that have historically been central to the prosecutions involving pregnancy: allegations that conduct during pregnancy—primarily but not exclusively drug use—harmed and/or resulted in the demise of the fetus. As detailed above, the proposed regulation focuses on "circumstances in which the PHI is sought for the purpose of investigation or imposing liability on any person for the mere act of seeking, obtaining, providing or facilitating reproductive healthcare." The problem here is that in the majority of previous cases, the allegation was that during the pregnancy the pregnant person did something that resulted in fetal harm.[253] The allegations in these cases had nothing to do with "seeking, obtaining, providing or facilitating reproductive healthcare." Therefore, the proposed rule likely not effect disclosures regarding cases that have historically been central to pregnancy-related prosecutions.

Third, the attestation requirement fails to address what has historically been a central method of criminalizing pregnancy: the disclosure of PHI pursuant to 45 C.F.R 164.512(b)(ii), permitting disclosures to a "public health authority or other appropriate government authority authorized by law to receive reports of child abuse or neglect."[254] Given the growing trend of defining the fetus as a person, the number of states that define pregnancy-related conduct as child abuse, and the very real possibility that states expand these efforts, the attestation requirement, which simply requires those requesting information to attest that the use or disclosure is not for a prohibited purpose,[255] does nothing to address disclosures pursuant to these provisions.

Finally, the question arises whether the NPRM will withstand legal challenge. Indeed, it is clear from the NPRM's extensive background discussion, the careful mapping of the proposed rule changes to the HIPAA's statutory and regulatory history,[256] and its detailed focus on the physician-

253. *See supra* note 11–22 and accompanying text.

254. 45 C.F.R. § 164.512(b)(ii) (2013).

255. NPRM at 23553.

256. *See, e.g.*, NPRM at 23525 (noting that the "widely recognized distinction between public health activities, which primarily focus on improving the health of populations, and criminal investigations").

patient relationship's grounding in trust[257] that HHS is anticipating such a challenge. HHS's core argument is that the original balance between protecting PHI and disclosing it for law enforcement purposes has been disrupted by state abortion restrictions that include investigations and prosecutions and that new prohibitions on disclosure are required to "preserve that balance."[258] Although we disagree with the premise that the prior balance was appropriately struck, litigation will largely turn on this analysis.

B. PRIVACY PROTECTIONS OUTSIDE HIPAA

In general, confidentiality laws regulate disclosure of personal information. The HIPAA privacy model, modified by HITECH, combines confidentiality with breach notification. However, those are not the only protective models available to policymakers. Others include Anonymization (mandating the removal of certain identifiers prior to correction), Inalienability (prohibiting the transfer of certain data), and Privacy (prohibiting or limiting the collection of information).[259] These are all models that could be useful in dealing with the fallout from *Dobbs*.

As discussed previously, the only types of *Dobbs*-escalated informational privacy harms that HIPAA is equipped to deal with are those involving collection and dissemination. Further, the HIPAA Privacy Rule only applies to a subset of such cases: those where a covered entity or BA is responsible for the disclosure. Neither HIPAA nor HITECH seems to authorize more expansive regulation aimed at, for example, mobile health developers or data aggregators.

In contrast, some federal laws already go beyond HIPAA confidentiality and provide additional protection of health information. For example, the Genetic Information Nondiscrimination Act of 2008 (GINA) was based on the recognition of "the potential misuse of genetic information to discriminate in health insurance and employment."[260] In part, GINA prohibits employment discrimination based on genetic information. It prohibits employers from requesting, requiring, or purchasing genetic information about a person or

257. NPRM at 23509 (noting that "individuals do not forgo lawful healthcare when needed—or withhold important information from their healthcare providers that may affect the quality of healthcare they receive—out of a fear that their sensitive information would be revealed outside of their relationships with their healthcare providers").

258. NPRM at 23516.

259. Terry, *supra* note 146, at 151–55.

260. Genetic Information Non-discrimination Act of 2008. 42 U.S.C. § 2000ff(2).

their family members (Title II).[261] As such, it adopts aspects of both Inalienability and Privacy.

After HIPAA, the federal laws with the strongest informational privacy footprint are those administered by the FTC. The Commission's primary tool is § 5 of the Federal Trade Commission Act which prohibits "unfair or deceptive acts or practices in or affecting commerce."[262] Section 5 frequently is used in proceedings against businesses that misrepresent their products or fail to comply with their own privacy policies. For example, in the health app space, the former would include making a representation that an app was as accurate as a traditional blood pressure cuff without competent and reliable scientific evidence substantiating such a claim.[263] The latter is well-illustrated by the case of the developer of a period tracking app sharing health information of its users with outside data analytics providers notwithstanding a promise that such information would be kept private.[264]

Overall, the FTC's jurisdiction and enforcement authority are best understood as broad[265] but "thin,"[266] as evidenced by the agency's apparent frustration with having only a few privacy protecting powers that it can use in policing data aggregators.[267] Notwithstanding, and of particular relevance for health privacy harms that occur in the HIPAA-free zone, the FTC seems acutely aware of the dangers and is increasingly asserting its presence in the space. For example, in 2016 the Commission published guidance for mobile app developers which emphasized data minimization (limiting data collection to what is necessary to accomplish a specified purpose[268]) and the

261. *Genetic Information Discrimination*, U.S. EQUAL EMP. OPPORTUNITY COMM'N, https://www.eeoc.gov/genetic-information-discrimination (last visited Apr. 20, 2023).

262. 15 U.S.C. § 45.

263. *See* Fed. Trade Comm'n v. Aura Labs, Inc., No. 8:16-cv-02147-DOC-KES, 2016 WL 7055120 (C.D. Cal. Dec. 2, 2016).

264. *See In re* Flo Health, Inc., Case No. C-4747 (Fed. Trade Comm'n June 17, 2021), https://www.ftc.gov/system/files/documents/cases/192_3133_flo_health_decision_and_order.pdf.

265. *See generally A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, FED. TRADE COMM'N (May 2021), https://www.ftc.gov/about-ftc/mission/enforcement-authority (describing the commissions investigative, law enforcement and rulemaking authority).

266. *See generally* Terry, *supra* note 90, at 95 (observing that FTC prohibitions on "unfair or deceptive acts or practices" are limited when compared to more robust privacy regimes).

267. *See Data Brokers, A Call for Transparency and Accountability*, FED. TRADE COMM'N (May 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf.

268. *Glossary: D*, EUR. DATA PROT. SUPERVISOR, https://edps.europa.eu/data-protection/data-protection/glossary/d_en#data_minimization (last visited Nov. 25, 2023).

implementation of security by design.[269] In 2021, the FTC doubled down on its Health Breach Notification Rule[270] issued pursuant to the HITECH Act[271] with an eyebrow-raising interpretative guidance that "[w]hen a health app . . . discloses sensitive health information without users' authorization, this is a 'breach of security' under the Rule."[272]

However, the FTC initiative most relevant to the post-*Dobbs* world is the Commission's announced interest in engaging in future rulemaking to restrict commercial surveillance or lax data security practices.[273] Such regulation would increase pressure on businesses to reduce the privacy harms associated with collection, processing, and dissemination of reproduction-related information. The extant example of such privacy harms is the ongoing Kochava litigation.[274] The FTC argued that the data aggregator's sale of its geolocation data sourced from mobile devices could be used to trace the movements of persons to and from sensitive locations, such as reproductive health clinics, places of worship, homeless and domestic violence shelters, and addiction recovery facilities.[275] The Commission argued that the release of such data "is likely to injure consumers through exposure to stigma, discrimination, physical violence, emotional distress, and other harms.[276]

Another federal privacy regime applies to those types of harms although its current legal status is in flux. The Confidentiality of Alcohol and Drug Abuse Patient Records rule,[277] often referred to as "Part 2," introduced a special layer of confidentiality applicable to the identity and records of patients with substance use disorders (SUD). Promulgated prior to the passage of HIPAA, Part 2 remained in force after HIPAA Privacy was enacted, serving

269. *Mobile Health App Developers: FTC Best Practices*, FED. TRADE COMM'N (Dec. 2022), https://www.ftc.gov/business-guidance/resources/mobile-health-app-developers-ftc-best-practices.

270. 16 C.F.R. pt. 318 (2009).

271. *See* HITECH, *supra* note 228.

272. Fed. Trade Comm'n, Statement of the Commission on Breaches by Health Apps and Other Connected Devices (Sept. 15, 2021), https://www.ftc.gov/system/files/documents/public_statements/1596364/statement_of_the_commission_on_breaches_by_health_apps_and_other_connected_devices.pdf.

273. Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273–74 (Aug. 22, 2022) (to be codified at 16 C.F.R. ch. 1), https://www.govinfo.gov/content/pkg/FR-2022-08-22/pdf/2022-17752.pdf.

274. *See* Complaint, *supra* note 89.

275. *Id.* at 6.

276. *Id.* at ¶ 29.

277. Confidentiality of Substance Use Disorder Patient Records, 85 Fed. Reg. 42986–3096 (July 15, 2020) (to be codified at 42 C.F.R. pt. 2), https://www.govinfo.gov/content/pkg/FR-2020-07-15/pdf/2020-14675.pdf.

as an additional and arguably more robust protection of exceptionally sensitive health information. Part 2, like GINA and, to an extent, psychotherapy notes, applied exceptional protections to specific cohorts of health information and so serves as an important analogy for the protection of reproduction information.

Briefly, Part 2 requires a detailed consent in writing from the patient for any use of their health information that includes the purpose of the disclosure and its recipient identified with considerable specificity. A notice informs the recipient that in most cases redisclosure is prohibited and specifies other use restrictions.[278] Because people who use drugs may become involved in the criminal justice system with a subset being involved in judicial diversion programs, Part 2 contains specific protective provisions addressing those issues.[279]

On its face, Part 2 thereby seems like an attractive model for informational privacy after *Dobbs*; it identifies a particularly sensitive subset of health information that has serious implications for stigma, distress, and involvement with the criminal justice system, and it makes it far harder for healthcare providers—let alone those outside of the healthcare system—to access the information. However, in something of a surprise, Congress included a provision in the otherwise pandemic-specific CARES Act of 2020 that will fundamentally change Part 2's enabling legislation.[280] The legislation clearly intended to align the protection of substance use records with the more broadly applicable HIPAA model.[281] This change was driven in part by the concerns of providers who treat individuals with both SUD and other, non-behavioral conditions who have struggled to keep two separate sets of records, particularly when they are stored in an electronic health record. Providers also worried about the impact of segregating the records on emergency department assessment and overall coordinated care.[282]

278. 42 C.F.R. §§ 2.31–33 (2020).

279. *See id.* § 2.35 (2018); *Id.* §§ 2.61–67 (2020).

280. Coronavirus Aid, Relief, and Economic Security Act or the CARES Act, Pub. L. No. 116-136, 134 Stat. 281 (Mar. 2020).

281. On November 28, 2022, OCR and SAMHSA issued a Notice of Proposed Rulemaking to revise Part 2 that carries out the CARES Act mandate by closely aligning HIPAA and Part 2. Confidentiality of Substance Use Disorder (SUD) Patient Records, 87 Fed. Reg. 74216–87 (Dec. 2, 2022) (to be codified at 42 C.F.R. pt. 2; 45 C.F.R. pt. 164). Although the revision does further restrict the use and disclosure of Part 2 records in civil and criminal proceedings, a court order will overrule any restriction. *See* 87 Fed. Reg. 74216–87, 74245–46.

282. Nicolas Terry, Melissa Goldstein & Kirk Nahra, *COVID-19: Substance Use Disorder, Privacy, and the CARES Act*, HEALTH AFFS. BLOG (June 8, 2020), https://www.healthaffairs.org/do/10.1377/hblog20200605.571907/full/.

Although much of Part 2 will later be aligned with the HIPAA Privacy Rule, it still retains some particularly strong protections designed to minimize the use of substance use records in court proceedings. A party seeking disclosure of a patient's substance use record must show "good cause" requiring the court to "weigh the public interest and the need for disclosure against the injury to the patient, to the physician-patient relationship, and to the treatment services."[283] In the absence of that specific order, a substance use record "may not be disclosed or used in any civil, criminal, administrative, or legislative proceedings conducted by any Federal, State, or local authority, against a patient,"[284] barring the record from, for example, use as evidence in a criminal prosecution,[285] law enforcement investigation,[286] or an application for a warrant.[287] If reproductive health records were similarly protected by federal law, it would come close to some kind of presumptive "criminal inalienability" protective model.

Of course, beyond the FTC or Part 2 there are countless other examples of alternatives or additions to mainstream confidentiality rules like HIPAA. For example, Illinois' Biometric Information Privacy Act provides robust protection against the retention or disclosure of biometric information, albeit subject to exceptions for subpoenas and admissibility in legal proceedings.[288] Texas[289] and Washington[290] have similar laws. Many states have taken similar steps to protect the results of HIV-related information,[291] and many states include the option to allow for anonymous testing.[292] However, state laws in reproductive autonomy-friendly states will be of little utility, and in autonomy-rejecting states such privacy protections likely will be interpreted or legislated away.

C. REFORMATIVE FEDERAL PRIVACY LEGISLATION

Predictably, an analysis of the limitations of our federal health information privacy models in the face of *Dobbs* leads to a proposal for a stronger federal law dealing with the issue. It is conceded that the passage of enhanced federal privacy legislation would be addressing a symptom of *Dobbs* rather than curing

283. 42 U.S.C. § 290dd-2(b)(2)(C).
284. 42 U.S.C. § 290dd-2(c).
285. *Id.*
286. 42 U.S.C. § 290dd-2(c)(3).
287. 42 U.S.C. § 290dd-2(c)(4).
288. 740 ILL. COMP. STAT. 14 (2010).
289. TEX. BUS. & COM. CODE ANN. § 503.001 (2017).
290. WASH. REV. CODE § 19.375.020 (2017).
291. 35 PA. CONS. STAT. § 7601 (1999).
292. ARIZ. ADMIN. CODE § 9-6-1005 (2018); CAL. HEALTH AND SAFETY CODE § 120895 (Deering 2006).

the fundamental problem, which will require federal reproductive autonomy legislation. It must also be conceded that if the current Administration or a future one finds itself with a filibuster-proof Senate majority, reproductive autonomy, not privacy, will likely be the legislative priority.

Notwithstanding, pursuing a far stronger federal privacy law, even if it is not the *Dobbs* "silver bullet," is a worthy end because it could remove or reduce some of the health privacy harms that adversely impact reproductive autonomy and establish a beachhead in the continuing fight for increased recognition of liberty interests.

We have already discussed the mythology of generalized health privacy protection that has grown up around HIPAA.[293] In practical terms, that myth accomplishes little. Very few understand the level of exposure for health information found in the HIPAA-free zone ameliorated by only the occasional assist from the FTC. However, the HIPAA mythology—or more accurately, the *expectations* of privacy that it fuels—may have political force. HIPAA is a touchstone for health privacy expectations just as *Roe* was for reproductive autonomy. Used correctly and understood as cultural touchpoints, both could help create popular pressure for legislative change. Opinion polls clearly fail to impress lawmakers in conservative-leaning states, but nationally a strong majority favors abortion rights,[294] a position apparently endorsed by the success of pro-abortion ballot initiatives[295] and evidenced by the larger role of abortion preferences[296] displayed in the November 2022 midterm elections. Most Americans believe it is difficult to control access their online

293. *See supra* Part IV.

294. *See* Steven Shepard, *Abortion Was a 50/50 issue. Now, It's Republican Quicksand*, POLITICO (Apr. 8, 2023), https://www.politico.com/news/2023/04/08/republican-party-abortion-trap-00091088; Alison Durkee, *How Americans Really Feel About Abortion: The Sometimes Surprising Poll Results As Court Ruling Threatens Mifepristone Access*, FORBES (Apr. 11, 2023), https://www.forbes.com/sites/alisondurkee/2023/04/11/how-americans-really-feel-about-abortion-the-sometimes-surprising-poll-results-as-court-ruling-threatens-mifepristone-access/?sh=4c1165d07933.

295. *See* Rachel M. Cohen, *How Abortion Rights Advocates Won Every Ballot Measure This Year*, VOX (Nov. 11, 2022), https://www.vox.com/policy-and-politics/23451074/abortion-ballot-measure-midterms-kentucky-montana-michigan.

296. Alice Miranda Ollstein & Megan Messerly, *A Predicted 'Red Wave' Crashed into Wall of Abortion Rights Support on Tuesday*, POLITICO (Nov. 11, 2022), https://www.politico.com/news/2022/11/09/abortion-votes-2022-election-results-00065983.

information[297] and an even larger number favor increased protection for their health information.[298]

There also appears to be substantial political traction for increased privacy protection at the federal level. Privacy and particularly health privacy enjoy a long history of bipartisanship. Although bipartisanship is highly unlikely to outweigh the GOP's commitment to abortion restrictions, federal privacy legislation that reduces some of the post-*Dobbs* privacy harms might still have traction.

Beyond the beltway, a growing appreciation of the interrelationships between reproductive access and informational privacy could create a powerful narrative that would encourage fundamental legislative reforms in Washington. For example, a recent survey of a sample of registered voters nationwide found 63 percent in favor of Congress acting to ban the sale or sharing of app or search engine reproductive data.[299] Some politicians already have embraced these interrelationships. For example, Senator Ron Wyden's reaction to *Dobbs* included the following:

> "Congress must pass legislation protecting people's data so their web searches, text messages and location tracking aren't weaponized against them. Technology companies must take immediate steps to limit the collection and retention of customer data so that they don't become tools of persecution."[300]

Representative Sara Jacobs, when she announced her "My Body, My Data Act," stated, "It's unconscionable that information could be turned over to the government or sold to the highest bidder and weaponized against us, and

297. Brooke Auxie, Lee Rainie, Monica Anderson, Andrew Perrin, Madhu Kumar & Erica Turner, *Americans and Privacy: Concerned, Confused and Feeling Lack of Control Over Their Personal Information*, PEW RSCH. CTR. (Nov. 15, 2019), https://www.pewresearch.org/internet/2019/11/15/americans-and-privacy-concerned-confused-and-feeling-lack-of-control-over-their-personal-information/; Neil Lloyd & Chris Jackson, *Most Americans Say It Is Increasingly Difficult to Control Who Can Access Their Online Data*, IPSOS (Jan. 7, 2022), https://www.ipsos.com/en-us/news-polls/data-privacy-2022.

298. *Patient Survey Shows Unresolved Tension Over Health Data Privacy*, AM. MED. ASS'N (July 25, 2022), https://www.ama-assn.org/press-center/press-releases/patient-survey-shows-unresolved-tension-over-health-data-privacy; Sydney Murphy, *9 in 10 Americans Want Their Health Info Kept Private*, HEALTHDAY NEWS (Aug. 2, 2022), https://www.webmd.com/health-insurance/news/20220802/9-in-10-americans-want-their-health-info-kept-private.

299. *Abortion Rights and Democracy: A Guide for Advocates*, NAVIGATOR RSCH. (Sept. 22, 2022), https://navigatorresearch.org/wp-content/uploads/2022/09/Navigator-Update-09.22.2022.pdf.

300. Press Release, Wyden Statement on the Overturning of Roe v. Wade (June 24, 2022), https://www.wyden.senate.gov/news/press-releases/wyden-statement-on-the-overturning-of-roe-v-wade.

especially against low-income people and people of color . . ."[301] Subsequently, Representative Jacobs and Representative Anna Eshoo introduced their proposed "Secure Access for Essential Reproductive (SAFER) Health Act," that, among other things, would require patient authorization (HIPAA-speak for consent) for disclosure of information about pregnancy termination or loss in civil, criminal, administrative, or legislative proceedings.[302]

It is not only patients' interests that have been unraveled. Doctors have also been negatively affected as the healthcare they provide is demonized and criminalized. [303] As the AMA Privacy Principles argue, "Health care information is one of the most personal types of information an individual can possess and generate . . . and individuals accessing, processing, selling, and using it without the individual's best interest at heart can cause irreparable harm.[304]

A potential vehicle for expanding privacy protections for health information is the bipartisan and bicameral American Data Privacy and Protection Act (ADPPA).[305] ADPPA fundamentally differs from the current approach to the regulation of private persons in the United States. Rather than being domain- or entity-specific, the statute would apply to most data and most data custodians. At its heart are Fair Information Practices (FIPPS) principles, [306] such as data proportionality, transparency, and consent. Additional obligations would apply to data aggregators.[307] "Sensitive Covered Data," which includes a "healthcare condition or treatment,"[308] are subject to

301. Press Release, Congresswoman Jacobs Announces My Body, My Data Act to Protect Reproductive Health Data (June 2, 2022), https://sarajacobs.house.gov/news/documentsingle.aspx?documentid=542 (last accessed Apr. 20, 2023).

302. Press Release, On 50th Anniversary of Roe, Eshoo and Jacobs Introduce Legislation to Protect Reproductive Healthcare (Jan. 25, 2023), https://eshoo.house.gov/media/press-releases/50th-anniversary-roe-eshoo-and-jacobs-introduce-legislation-protect.

303. Selena Simmons-Duffin, *Doctors Weren't Considered in Dobbs, But Now They're on Abortion's Legal Front Lines*, NPR (July 3, 2022), https://www.npr.org/sections/health-shots/2022/07/03/1109483662/doctors-werent-considered-in-dobbs-but-now-theyre-on-abortions-legal-front-lines.

304. AMA PRIVACY PRINCIPLES 2, AM. MED. ASS'N (2020), https://www.ama-assn.org/system/files/2020-05/privacy-principles.pdf.

305. American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2021–2022).

306. Pam Dixon, *A Brief Introduction to Fair Information Practices*, WORLD PRIVACY FORUM, (Jan. 4, 2008), https://www.worldprivacyforum.org/2008/01/report-a-brief-introduction-to-fair-information-practices/.

307. *Overview of the American Data Privacy and Protection Act, H.R. 8152*, CONG. RSCH. SERV. (Aug. 31, 2022), https://crsreports.congress.gov/product/pdf/LSB/LSB10776.

308. American Data Privacy and Protection Act, H.R. 8152, 117th Cong. § 2(28)(A)(ii) (2021–2022).

additional levels of protection.[309] The Act would be enforced by a newly established "Bureau of Privacy" within the FTC[310] and by state attorneys general.[311] Compliance with HIPAA by a HIPAA-covered entity would satisfy most provisions of the ADPPA.[312]

By addressing many, if not all, of the privacy gaps and harms wrought by private persons identified above, the ADPPA would improve reproductive informational privacy. Specifically, sensitive reproduction-inflected data held by app developers, search engines, and data aggregators in the HIPAA-free zone would be far better protected. However, ADPPA would be less effective in dealing with the harms triggered by public persons. Prosecutors would still be able to pursue reproductive information using subpoena or warrant powers. As a result, to minimize and possibly eliminate the informational fallout from *Dobbs*, two additional reforms are required.

First, Congress must borrow from Part 2 and require that any records concerning of reproductive healthcare "may not be disclosed or used in any civil, criminal, administrative, or legislative proceedings conducted by any Federal, State, or local authority, against a patient,"[313] absent a court hearing weighing "the public interest and the need for disclosure against the injury to the patient, to the physician-patient relationship, and to the treatment services" and a clear finding authorizing disclosure.[314]

Second, and certainly contrary to the trend toward data maximization in healthcare generally, this Article has made clear the enormous harms that flow from the presence of healthcare when wielded by those who seek to criminalize reproductive conduct. As a result, there must be an increased emphasis on data minimization. There is no question that data minimization in this particular domain will be a sea change for healthcare, but absent legislation we are going to have to look to healthcare providers to be far more circumspect as to what reproductive information they collect and how long they retain it.

VII. CONCLUSION

The repercussions of *Dobbs* are still being understood. The state statutes triggered by the decision or the new, repressive laws being crafted across the country extend the deep fissures about equitable access to healthcare services and, potentially, state attitudes to federal health privacy policies. Some of the

309. *See, e.g.*, *id.* at § 102(2)(3).
310. *Id.* at § 401.
311. *Id.* at § 402.
312. *Id.* at § 404 (a)(3).
313. 42 U.S.C. § 290dd2(c).
314. 42 U.S.C. § 290dd2(b)(2)(C).

repercussions are not new but are just now brutally highlighted. *Dobbs* will encourage states to double down on fetal personhood and the criminalization of the pregnant poor or persons of color. And, because confidential health information will be a key to successful prosecutions, health information about women or designed to help them increasingly will be targeted.

This Article has not identified a "silver bullet" to address the health information issues raised by *Dobbs*. Indeed, most of the deficiencies in our privacy models and specifically in HIPAA have long been recognized. HIPAA and the soon to be reformulated Part 2 do not proffer "off-the-shelf" solutions for the health informational privacy crisis that is unfolding. Notwithstanding, HIPAA's heightened consent rule ("authorization"), its "minimum necessary" standard, and Part 2's requirement of a strict judicial order, all indicate that there are models available to better protect highly sensitive health information.

What our Article makes clear is that, as well-meaning as no doubt it was, the Biden administration guidance reassuring doctors and patients about HIPAA protections does not withstand analysis. The criminalization of reproductive services will increase dramatically, and medical records *will* end up in the hands of law enforcement and other government entities that can forcibly interfere in families' lives. While it is obvious that *Dobbs* itself must be reset by federal legislation, it is equally the case that federal privacy legislation must be recast to truly protect reproductive information.

UNENJOINED INFRINGEMENT AND COMPULSORY LICENSING

Jorge L. Contreras[†] *& Jessica Maupin*[††]

ABSTRACT

After the U.S. Supreme Court's 2006 decision in eBay v. MercExchange, federal courts have denied a substantial number of requests for permanent injunctions following a finding of patent infringement. Without an injunction, an infringing party may continue to practice the infringed patent, typically subject to the payment of a court-approved ongoing royalty. Courts and scholars have debated whether unenjoined infringement and the payment of an ongoing royalty therewith constitutes a judicial compulsory license or something else. To assess how courts view unenjoined infringement, we identified seventy-seven post-eBay cases in which patent infringement was found, but a permanent injunction was denied. In each case, we analyzed the language used by the court in establishing the right of the infringer to continue to operate under the infringed patent(s) and its obligation to compensate the patent holder. This language, as well as the surrounding transactional and litigation context, indicates that at least some federal district courts have been granting compulsory patent licenses upon the denial of permanent injunctions, both tacitly and expressly. Moreover, the Federal Circuit has agreed with this characterization in at least some cases.

To remove any lingering uncertainty, we recommend that the Federal Circuit acknowledge that a district court that declines to enjoin the infringement of a valid and enforceable patent, and concurrently orders the infringer to compensate the patent holder for acts of future unenjoined infringement, has authorized a compulsory license of the patent. Such an acknowledgment would better align the realities of unenjoined infringement with existing doctrines of patent exhaustion and transfer and encourage courts to focus greater attention on the non-royalty aspects of such licenses, which are currently missing key terms such as license scope, field of use, duration, and termination. It would also inform U.S. foreign policy regarding compulsory licensing by other countries.

DOI: https://doi.org/10.15779/Z38GQ6R356

 The authors thank Bernard Chao, Thomas Cotter, Tomas Gómez-Arostegui, Fabian Gonell, Mark Lemley, Matthew Sag, Pamela Samuelson and Norman Siebrasse for their thoughtful comments on earlier drafts of this Article. This Article has benefitted from presentation and discussion at the 2021 Intellectual Property Scholars Conference (IPSC) and the 2022 Works in Progress in Intellectual Property (WIPIP) conference.

† James T. Jensen Endowed Professor for Transactional Law and Director of the Program on Intellectual Property and Technology Law, University of Utah S.J. Quinney College of Law.

†† Associate, McGuireWoods LLP.

TABLE OF CONTENTS

I. INTRODUCTION

Compulsory patent licensing occurs when a governmental entity requires a patent holder, against its will, to permit others to practice a patent.[1] Several countries have granted compulsory patent licenses over the past few decades, typically to provide local populations with low-cost access to medicines.[2] Yet, proposals to enact a general compulsory licensing power in the United States have been unsuccessful for more than a century.[3] What's more, the U.S. government has frequently applied diplomatic and trade pressure to countries that have sought to issue compulsory licenses of drugs patented by U.S. firms.[4] The Office of the U.S. Trade Representative, in its annual *Special 301 Report*, has regularly criticized compulsory licensing by other countries as undermining intellectual property rights, reducing incentives to invest in research and development, and impeding new biomedical discoveries.[5] While the principal international agreement pertaining to patent rights expressly permits compulsory licensing,[6] the U.S. government has urged other nations to issue

1. *See infra* Section II.A.

2. *See* Sapna Kumar, *Compulsory Licensing of Patents During Pandemics*, 54 Conn. L. Rev. 59, 73–75 (2022); David Shore, *Divergence and Convergence of Royalty Determinations Between Compulsory Licensing under the TRIPS Agreement and Ongoing Royalties as an Equitable Remedy*, 46 Am. J. L. & Med. 55, 66–72 (2020); John R. Thomas, Cong. Rsch. Serv., R43266, Compulsory Licensing of Patented Inventions 9–13 (2014) (cataloging and summarizing non-U.S. compulsory licenses).

3. Hartford-Empire Co. v. United States, 323 U.S. 386, 417 (1945) ("Congress was asked as early as 1877, and frequently since, to adopt a system of compulsory licensing of patents. It has failed to enact these proposals into law."). *See also* Dawson Chem. Co. v. Rohm & Haas Co., 448 U.S. 176, 215 n. 21 (1980) ("Compulsory licensing of patents often has been proposed, but it has never been enacted on a broad scale.").

4. *See* Kumar, *supra* note 2, at 73–75.

5. Off. of the U.S. Trade Rep., Exec. Off. of the President, 2020 Special 301 Report (2020), at 14 [hereinafter Special 301 Report].

6. Agreement on Trade-Related Aspects of Intellectual Property Rights, art. 31, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299, 33 I.L.M. 1197 (1994) [hereinafter TRIPS Agreement]. *See also* Ministerial Declaration of 14 November 2001, WTO Doc. WT/MIN(01)/DEC/1, 41 I.L.M 746.

compulsory licenses only in extremely limited circumstances and only after making every effort to obtain authorization from the patent owner.[7]

Against this backdrop, following the U.S. Supreme Court's landmark 2006 decision in *eBay v. MercExchange*,[8] federal courts have denied a substantial number of requests for permanent injunctive relief after finding patent infringement. Without an injunction, an infringing party may continue to practice a patent, typically subject to the payment of a court-approved royalty.

7. Special 301 Report, *supra* note 5, at 14. *See also* MAKAN DELRAHIM, DEPT. OF JUSTICE, FORCING FIRMS TO SHARE THE SANDBOX: COMPULSORY LICENSING OF INTELLECTUAL PROPERTY RIGHTS AND ANTITRUST 17 (2004), https://www.justice.gov/atr/speech/forcing-firms-share-sandbox-compulsory-licensing-intellectual-property-rights-and ("[C]ompulsory licensing presents many policy and practical issues. I believe, however, that the remedy is appropriate so long as antitrust authorities carefully consider the potential harm to innovation, and draft the license as narrowly as they reasonably can."). This position appears to have softened somewhat during the COVID-19 pandemic, given the U.S. Trade Representative's support for a proposed waiver of trade sanctions at the World Trade Organization with respect to countries that permit the use of COVID-19 technologies without authorization of the holders of relevant intellectual property. Press Release, Off. U.S. Trade Rep., Statement from Ambassador Katherine Tai on the COVID-19 Trips Waiver (May 5, 2021), https://ustr.gov/about-us/policy-offices/press-office/press-releases/2021/may/statement-ambassador-katherine-tai-covid-19-trips-waiver#:~:text=WASHINGTON%20–%20United%20States%20Trade%20Representative,protections%20for%20COVID%2D19%20vaccines.

8. eBay Inc. v. MercExchange, L.L.C., 547 U.S. 388 (2006).

Numerous advocates,[9] scholars,[10] and even some judges[11] have assumed that this court-sanctioned ability to practice a patent after a finding of infringement—what has been termed "unenjoined" infringement—is, in effect, a court-imposed compulsory license with court-determined compensation.

The characterization of unenjoined infringement as compulsory licensing is entirely consistent with other doctrines of patent law, including patent exhaustion and transfer. In fact, treating unenjoined infringement as anything *other* than a compulsory patent license would lead to anomalous and unintended results, such as a patent holder being able to collect twice for the practice of the same patent[12] or to collect ongoing royalties even after the patent has been transferred to another party.[13]

---

9. *See Compulsory licensing in the context of U.S. injunction cases involving medical technologies*, KNOWLEDGE ECOLOGY INTL., (Mar. 21, 2019), https://www.keionline.org/us-injunction-medical.

10. *See* John M. Golden, *United States*, *in* INJUNCTIONS IN PATENT LAW: TRANS-ATLANTIC DIALOGUES ON FLEXIBILITY AND TAILORING 291, 306–07 (Jorge L. Contreras & Martin Husovec eds., 2022) ("[A] district court may provide a remedy that can operate as a sort of case-specific compulsory license: specifically, the court may order the payment of 'ongoing royalties' for continuing activity that would otherwise constitute infringement"); Shore, *supra* note 2, at 58 ("Typically referred to as 'ongoing royalties,' these court-mandated compulsory licenses are a modern alternative to injunctions against adjudged infringers."); H. Tomás Gómez-Arostegui, *Prospective Compensation in Lieu of a Final Injunction in Patent and Copyright Cases*, 78 FORDHAM L. REV. 1661, 1663 (2010) ("[L]ower courts . . . are now struggling with what relief, if any, to give prevailing plaintiffs in lieu of an injunction . . . [M]ost award prospective compensation . . . commonly a continuing royalty . . . for future, postjudgment infringements . . . thereby effectively creating a compulsory license."); Daniel A. Crane, *Intellectual Liability*, 88 TEX. L. REV. 253, 263 (2009) ("In effect, the combination of declining to issue a permanent injunction and awarding the patentee a reasonable royalty is a compulsory license"); Christopher A. Cotropia, *Compulsory Licensing Under TRIPS and the Supreme Court of the United States' Decision in eBay v. MercExchange*, *in* PATENT LAW AND THEORY: A HANDBOOK OF CONTEMPORARY RESEARCH 557, 574 (Toshiko Takenaka & Rainer Moufang eds., 2009) ("[T]he *de facto* effect of an injunction denial is, by definition, a government-allowed compulsory license."); Bernard H. Chao, *After eBay, Inc. v. MercExchange: The Changing Landscape for Patent Remedies*, 9 MINN. J. L. SCI. & TECH. 543, 572 (2008) ("Some courts have replaced the permanent injunction with an ongoing royalty, a compulsory license that is only available to the losing defendant."); DANIEL GERVAIS, THE TRIPS AGREEMENT: DRAFTING HISTORY AND ANALYSIS 450 (3rd ed. 2008) ("[T]he systematic impossibility to obtain an injunction and to obtain only actual damages could amount to a compulsory license.").

11. Paice LLC v. Toyota Motor Corp., 504 F.3d 1293, 1316 (Fed. Cir. 2007) (Rader, J., concurring). *See infra* Sections III.B.3–4.

12. *See infra* Section IV.A (discussing patent exhaustion).

13. *See infra* Section IV.B (discussing patent transfers).

The traditional test for granting permanent injunctive relief under the common law requires a finding that the plaintiff would be irreparably harmed if such relief were not granted.[14] Some injuries, such as encroachments on property, depletion of natural resources, and violations of civil rights, have traditionally given rise to a presumption of irreparable harm.[15] The same presumption existed under patent law for many years. The presumption of irreparable harm in patent cases was largely based on the property-like character of patents. A patent confers on its owner "the right to exclude others from making, using, offering for sale, or selling the invention,"[16] a set of rights that evokes the traditional right to exclude by property owners. Likewise, Section 261 of the Patent Act states that "patents shall have the attributes of personal property."[17] These considerations led courts, particularly the Court of Appeals for the Federal Circuit, to treat patents as unique assets, like real estate, that should automatically be entitled to protection from unauthorized exploitation by permanent injunctions.[18] Accordingly, the Federal Circuit adopted a general presumption that a permanent injunction will automatically issue once a patent has been adjudged infringed and valid, absent exceptional circumstances.[19] As a result, injunctions were more likely to issue in patent cases than most other types of litigation.[20]

---

14. *See* 1 DAN B. DOBBS, DOBBS LAW OF REMEDIES 58 (2nd ed. 1993).

15. *See* Mark P. Gergen, John M. Golden & Henry E. Smith, *The Supreme Court's Accidental Revolution? The Test for Permanent Injunctions*, 112 COLUM. L. REV. 203, 220–24, 231–32 (2012). More recently, Congress reinstated the presumption of irreparable harm in trademark cases. *See* Trademark Modernization Act of 2020 as incorporated in Consolidated Appropriations Act. Trademark Modernization Act of 2020, Pub. L. No. 116-260, § 226, 134 Stat. 1182 (2020).

16. 35 U.S.C. § 154(a)(1).

17. 35 U.S.C. § 261.

18. *See, e.g.*, H.H. Robertson, Co. v. United Steel Deck, Inc., 820 F.2d 384, 390 (Fed. Cir. 1987), *abrogated by* Markman v. Westview Instruments, Inc., 52 F.3d 967 (Fed. Cir. 1995) ("In matters involving patent rights, irreparable harm has been presumed when a clear showing has been made of patent validity and infringement. This presumption derives in part from the finite term of the patent grant, for patent expiration is not suspended during litigation, and the passage of time can work irremediable harm . . . The nature of the patent grant thus weighs against holding that monetary damages will always suffice to make the patentee whole, for the principal value of a patent is its statutory right to exclude.")(citation omitted); Richardson v. Suzuki Motor Co., 868 F.2d 1226, 1246–47 (Fed. Cir. 1989) ("Infringement having been established, it is contrary to the laws of property, of which the patent law partakes, to deny the patentee's right to exclude others from use of his property.").

19. *See* MercExchange LLC v. eBay, Inc., 401 F.3d 1323, 1339 (Fed. Cir. 2005), vacated and remanded sub nom. eBay Inc. v. MercExchange, L.L.C., 547 U.S. 388 (2006).

20. Though strong, the presumption of irreparable harm in patent cases was not absolute. The presumption could be rebutted under various circumstances, including the defendant's showing that future infringement was unlikely (due, for example, to advancement of technology), the patentee was willing to license the patent for monetary consideration, the patentee unduly delayed in bringing suit, or the patentee's market share was large in

The U.S. Supreme Court revisited the availability of injunctive relief in patent cases in *eBay, Inc. v. MercExchange LLC*.[21] Justice Thomas, writing for the Court, held that the decision to grant or deny an injunction is an act of judicial discretion that must be exercised in accordance with "well-established principles of equity."[22] He articulated a four-factor equitable test to be applied by courts considering the grant of injunctive relief in patent cases. This test requires that the plaintiff must satisfy the following four factors for a permanent injunction to be granted:

1. that it has suffered an irreparable injury;
2. that remedies available at law [i.e., monetary damages] are inadequate to compensate it for that injury;
3. that considering the balance of hardships between the plaintiff and defendant, a remedy in equity is warranted; and
4. that the public interest would not be disserved by the award of an injunction.

Numerous scholars have studied the impact of *eBay* on the availability of injunctive relief in U.S. patent cases. These studies have uniformly found that, following *eBay*, district courts have issued fewer permanent injunctions in patent cases, with significantly fewer injunctions issued when the patent holder is a non-practicing entity (NPE).[23] Researchers have also observed that

comparison to the infringer's. *See, e.g.*, Reebok Int'l, Ltd. v. J. Baker, Inc., 32 F.3d 1552, 1557–59 (Fed. Cir. 1994) (denying injunction on the basis of no reputational harm and monetarily compensable actual damages); High Tech Med. Instrumentation, Inc. v. New Image Indus., Inc., 49 F.3d 1551, 1557–58 (Fed. Cir. 1995) (denying injunction on the basis of patentee's willingness to license its patents).

21. eBay v. MercExchange, 547 U.S. 388, 391–94 (2006).

22. eBay, 547 U.S. at 391. *But see* Gergen et al., *supra* note 15, at 205 (suggesting that the eBay four-factor test did not actually reflect well-established principles of equity).

23. *See* Colleen V. Chien & Mark A. Lemley, *Patent Holdup, the ITC, and the Public Interest*, 98 CORNELL L. REV. 1, 9–10 (2012) ("Based on our review of district court decisions since eBay, courts have granted about 75% of requests for injunctions, down from an estimated 95% pre-eBay."); THOMAS F. COTTER, COMPARATIVE PATENT REMEDIES 103 (2013) (finding empirical evidence that from 2007 to 2011, courts have granted permanent injunctions in approximately 75% of all patent cases, with a substantially lower success rate for cases brought by non-practicing entities); Christopher B. Seaman, *Permanent Injunctions in Patent Litigation After eBay: An Empirical Study*, 101 IOWA L. REV. 1949, 1983, 1987–88 (2016) (finding that in the eight years before and after *eBay* was decided, permanent injunctions were issued in 72.125% of infringement cases, and in only 16% of cases in which the patentee was a non-practicing entity); Christopher J. Clugston & Wonjoon Kim, *The Unintended Consequences of the Injunction Law after eBay v. MercExchange*, 99 J. PAT. & TRADEMARK OFF. SOC'Y 249, 260 (2017) ("Since *eBay*, injunction denials have increased to more than one-quarter (29.8%) of all patent cases."). *See also* Ryan T. Holte & Christopher B. Seaman, *Patent Injunctions on Appeal: An Empirical Study of the Federal Circuit's Application of* eBay, 92 WASH. L. REV. 145, 187–88 (2017) (finding that

plaintiffs sought fewer injunctions after *eBay* despite an overall increase in the number of patent suits,[24] suggesting that patent holders, aware of the higher burdens required to obtain injunctive relief, find it less economically attractive to seek injunctions.

These studies confirm that U.S. district courts, applying the four-factor *eBay* test, permit unenjoined infringement of patents in a meaningful number of cases. The implications of this trend for innovation, markets, and the patent system have been vigorously debated in the literature.[25] This Article does not wade into that long-running debate. Rather, it acknowledges that, for better or worse, unenjoined infringement has been permitted throughout the United States for the past sixteen years, and it now seeks to elucidate the legal character of such unenjoined infringement. The question is whether unenjoined infringement is continued patent infringement that remains subject to further remedial action by the patent holder, or whether it is effectively a compulsory patent license imposed by the court. This Article explores the

---

between 2006 and 2013, the Federal Circuit affirmed district court grants of permanent injunctions 88%, 22 of 25 cases, of the time and denials of permanent injunctions 53%, 9 of 17 cases, of the time); Ryan Davis, *Patent Injunctions Drop Sharply In 2018*, LAW 360 (Jan. 3, 2019), https://www.law360.com/articles/1121976/patent-injunctions-drop-sharply-in-2018 (reporting results of a study conducted by LexMachina).

24. Kirti Gupta & Jay P. Kesan, *Studying the Impact of eBay on Injunctive Relief in Patent Cases* (Hoover Inst. Working Group on Intell. Prop., Innovation and Prosperity, Working Paper No. 17004, Jan. 10, 2017), https://www.hoover.org/research/studying-impact-ebay-injunctive-relief-patent-cases (finding that in the six years prior to *eBay*, 459 motions for permanent injunctions resulted in the issuance of 381 permanent injunctions, while in the six years following *eBay*, 384 motions for permanent injunctions resulted in the issuance of 308 permanent injunctions).

25. *Compare* Filippo Mezzanotti & Timothy Simcoe, *Patent Policy and American Innovation After eBay: An empirical examination*, 48 RSCH POL. 1271, 1272 (2019) ("In general, we find no evidence of a decline in American innovation—whether measured as patents, R&D, venture capital or productivity growth—relative to the pre-*eBay* baseline."), Filippo Mezzanotti, *Roadblock to Innovation: The Role of Patent Litigation in Corporate R&D*, 67 MANAGEMENT SCI. 7362, 7383 (2021) (finding *eBay* "had a positive effect on innovation"), *and* Chien & Lemley, *supra* note 23, at 2 ("*eBay* solved much of the patent system's holdup problem"), *with* Adam Mossoff, *The Injunction Function: How and Why Courts Secure Property Rights in Patents*, 96 NOTRE DAME L. REV. 1581, 1584 (2021) (explaining the reduction in injunctions under *eBay* "undermines the function of [patent] property rights in spurring economic activities in the U.S. innovation economy."), Paul R. Michel & John T. Battaglia, *eBay, the Right to Exclude, and the Two Classes of Patent Owners*, 2020 PATENTLY-O PATENT L. J. 1, 9 (2020) ("The probabilities on injunctive relief for NPEs should increase . . . [a]nd that itself is critical if courts are serious about properly valuing U.S. patents and restoring the U.S patent system to its innovation- and economic-driving goals"), *and* Tim Carlton, *Note: The Ongoing Royalty: What Remedy Should a Patent Holder Receive When a Permanent Injunction is Denied?*, 43 GA. L. REV. 543, 564 (2009) ("The emerging practice of the district courts of imposing an ongoing royalty rate on patent holders is not the best solution and is unfair to the patent holder.").

latter possibility, including the terms and conditions of that compulsory license, how it comports with U.S. treaty obligations, and its implications for U.S. attitudes toward compulsory licenses granted by other countries.

The remainder of this Article proceeds as follows: Section II.A describes the different legal interpretations given to unenjoined infringement, and whether unenjoined infringement should be viewed as a continuing wrong that subjects the infringer to successive suits for damages, or as infringement as to which a court has determined damages in advance, either through a lump sum payment or ongoing royalties. Section II.B then turns to the question of whether unenjoined infringement accompanied by court-determined compensation is effectively a compulsory license and concludes that it is. Part III describes a novel empirical assessment of judicial decisions in which injunctions were denied in patent cases. Section III.A describes the methodology used to collect and code these decisions. Sections III.B and III.C then respectively report the aggregate trends identified as well as specific uses of language relating to ongoing royalties and compulsory licensing. Section III.D discusses the conclusions that the Article draws from these findings, namely that several courts and judges have characterized unenjoined infringement as compulsory licensing. Part IV addresses the implications that flow from considering unenjoined infringement as compulsory licensing, including its possible effect on patent exhaustion, the transfer of patents, and international treaty obligations. The Article then addresses the need to specify additional terms of the compulsory license grant. The Article concludes by recommending that courts, and the Federal Circuit in particular, acknowledge that unenjoined infringement accompanied by court-determined compensation is in fact compulsory licensing.

II. THE DEBATE OVER UNENJOINED INFRINGEMENT

While the Supreme Court's decision in eBay opened the door to unenjoined infringement, it says nothing about the status and obligations of the infringer after the denial of an injunction. Moreover, the case settled before the lower court on remand could fully adjudicate these issues.[26] This vacuum

26. After the Supreme Court rendered its decision in *eBay*, the case was remanded to the district court for further proceedings in accordance with the Supreme Court's ruling. On remand, the district court, applying the Supreme Court's four-factor test, upheld its prior denial of injunctive relief, allowing the defendants to continue to infringe the asserted patent. MercExchange, L.L.C. v. eBay, Inc., 500 F. Supp. 2d 556, 569–91 (E.D. Va. 2007) [hereinafter *eBay IV*]. The district court also confirmed an earlier jury award of $25 million in "reasonable royalty" damages with respect to infringement of the relevant patent. *Id.* at 563. However, the case settled in February 2008, before further issues regarding the compensation payable by eBay to MercExchange could be adjudicated. Paul M. Janicke, *Implementing the "Adequate Remedy*

left lower courts and commentators without guidance regarding the conditions, if any, under which an infringer could continue to infringe patents after the denial of an injunction. As one patent holder observed a few months after the *eBay* decision, "[t]he landscape of the remedy that should follow the denial of a patentee's request for permanent injunction post-*eBay* is uncharted territory."[27]

In the wake of *eBay,* significant debate emerged around two interrelated questions concerning unenjoined infringement. First, should a court's decision to deny a permanent injunction be viewed as conferring on the infringer an ongoing right to practice the infringed patent, or should the unenjoined infringer be viewed as committing continuing infringement of the asserted patent? Second, if unenjoined infringement is somehow permitted, what, if anything, should the infringer pay the patent holder to continue to infringe the patent?

A. COMPENSATION FOR UNENJOINED INFRINGEMENT

Once it is determined that no injunction will be issued to prevent an infringer from continuing to practice a valid and enforceable patent, one must ask where that leaves the infringer. There are two competing schools of thought in this regard. One holds that an infringer that continues to infringe a patent following the denial of an injunction remains an infringer, and that infringer is subject to subsequent suits by the patent holder for money damages and even further attempts to obtain an injunction (the "ongoing infringement" school). As Professor Bernard Chao succinctly puts it, "[a]fter losing a first lawsuit, a defendant continues to infringe at its own peril."[28] The competing school of thought holds that the court denying an injunction thereby authorizes the infringer to continue to practice the infringed patent, thus necessitating the infringer's compensation of the patent holder (the "compensation" school).[29] Section II.A considers the dueling theoretical

at Law" *for Ongoing Patent Infringement After eBay v. MercExchange*, 51 IDEA: INTELL. PROP. L. REV. 163, 174 (2011).

27. Corrected Brief of Plaintiff-Cross Appellant Paice LLC at 63, Paice LLC v. Toyota Motor Corp., 504 F.3d 1293 (Fed. Cir. 2007) (No. 06-1610, -1631, Fed. Cir. Dec. 18, 2006), 2006 U.S. Fed. Cir. Briefs LEXIS 393, at *75 [hereinafter *Paice* CAFC Brief].

28. Chao, *supra* note 10, at 571. *See also* Janicke, *supra* note 26, at 165 ("Ongoing unenjoined infringement remains unlawful, and it cannot be made otherwise by the waving of a judicial magic wand.").

29. *See* Paice LLC v. Toyota Motors Corp., 609 F. Supp. 2d 620, 630 (E.D. Tex. 2009), *dismissed*, 455 F. App'x 955 (Fed. Cir. 2010) ("[T]he law must ensure that an adjudged infringer who voluntarily chooses to continue his infringing behavior must adequately compensate the patent holder for using the patent holder's property. Anything less would be manifestly unjust and violate the spirit, if not the letter, of the U.S. Constitution and the Patent Act.").

perspectives that motivate the ongoing infringement and compensation schools.

1. Ongoing Infringement and Successive Damages Suits

Standing alone, the denial of an injunction does not necessarily exonerate an infringer from liability for continuing to infringe the asserted patent. Even if the patent holder is unlikely to obtain an injunction in a future action against the infringer, it is certainly entitled to monetary damages to compensate it for the infringement and could bring successive actions to recover those damages.

The need to initiate successive suits to recover damages against an unenjoined, ongoing tortfeasor arises in various areas of law. In nuisance cases, for example, when the harm continues, the injured party's remedy absent an injunction is "to bring from time to time separate suits for the recurring injuries sustained."[30]

The district court in *eBay* appears to have contemplated the possibility of successive damages suits for unenjoined infringement when it initially denied MercExchange's request for an injunction. Specifically, the court noted that if it denied the injunction and "if the defendants continue to infringe the plaintiff's patents, the court will be more inclined to award enhanced damages for any post-verdict infringement."[31] Likewise, in *z4 Techs., Inc. v. Microsoft Corp.*,[32] a patent infringement case decided one month after the Supreme Court's decision in *eBay*, the district court denied z4's request for an injunction against Microsoft under the *eBay* framework.[33] Then, to provide z4 with "an efficient method for . . . recovery of future monetary damages post-verdict," the court issued an order "severing z4's continuing causes of action for

30. Burleyson v. W. & Atl. R. Co., 87 S.E.2d 166, 171 (Ga. App. 1955). *See also* St. Louis, I.M. & S.R. Co. v. Biggs, 12 S.W. 331, 331 (Ark. 1889) ("[T]he injury to be compensated in a suit is only the damage which has happened, and there may be as many successive recoveries as there are successive injuries."); Naylor v. Eagle, 303 S.W.2d 239, 241 (Ark. 1957) ("If it is known merely that damage is probable, or, that even though some damage is certain, the nature and extent of that damage cannot be reasonably known and fairly estimated, but would be only speculative and conjectural, then the statute of limitations is not set in motion until the injury occurs, and there may be as many successive recoveries as there are injuries.").

31. MercExchange, L.L.C. v. eBay, Inc., 275 F. Supp. 2d 695, 714–15 (E.D. Va. 2003), *aff'd in part*, *rev'd in part sub nom.* MercExchange, LLC v. eBay, Inc., 401 F.3d 1323 (Fed. Cir. 2005), *vacated and remanded sub nom.* eBay Inc. v. MercExchange, L.L.C., 547 U.S. 388 (2006), and *judgment entered*, 660 F. Supp. 2d 653 (E.D. Va. 2007).

32. z4 Techs., Inc. v. Microsoft Corp., 434 F. Supp. 2d 437, 444 (E.D. Tex. 2006).

33. *Id.* at 439–44.

monetary damages due to Microsoft's continuing post-verdict infringement of z4's patents."[34]

Other courts, however, have rejected the successive suit theory. In *Paice LLC v. Toyota Motor Corp.*,[35] a patent infringement case considered by the Federal Circuit shortly after *eBay*, Toyota's hybrid vehicle drivetrain was found to infringe patents held by Paice. The district court, applying the four *eBay* factors, denied the permanent injunction that Paice sought.[36] It then ordered Toyota to pay Paice an ongoing royalty of $25 per vehicle to continue to practice the infringed patent.[37] On appeal, Paice argued that the lack of an injunction against Toyota's continuing infringement should not be viewed as granting Toyota an affirmative right to practice Paice's patent, which it referred to as a "compulsory license."[38] Rather, Toyota's continuing practice of the patent should be viewed as continuing infringement—possibly willful—as to which Paice "may elect to come back to court periodically to seek past damages."[39] The Federal Circuit rejected Paice's argument and instead affirmed the district court's ongoing royalty as the method to compensate Paice for Toyota's unenjoined infringement (see Section II.A.3, *infra*).[40]

One advantage of the successive action approach is that it gives the patent holder a potential claim for enhanced damages for "willful infringement"

34. *Id.* at 444. *Cf.* Saffran v. Bos. Sci. Corp., No. 2-05-CV-547 (TJW), 2008 U.S. Dist. LEXIS 106711, at *2 (E.D. Tex. Feb. 14, 2008) (finding that in case in which plaintiff did not seek an injunction, the "court sua sponte severs plaintiff's continuing causes of action for future royalties.").

35. Paice LLC v. Toyota Motor Corp., 504 F.3d 1293, 1316 (Fed. Cir. 2007).

36. Paice LLC v. Toyota Motor Corp., No. 2:04-CV-211-DF, 2006 WL 2385139, at *4–6 (E.D. Tex. Aug. 16, 2006) (*Paice I*), aff'd in part, vacated in part, remanded, 504 F.3d 1293 (Fed. Cir. 2007).

37. *See* Paice LLC v. Toyota Motors Corp., 609 F. Supp. 2d 620, 622 (E.D. Tex. 2009) (summarizing the holding in *Paice I* as follows: "The Court awarded damages for past infringement in the amount found by the jury and established, dividing the jury's lump-sum damages award for past infringement by the number infringing vehicles sold, an ongoing royalty rate of $25 per infringing vehicle for the remaining life of the '970 Patent.").

38. Paice CAFC Brief, *supra* note 27, at *75–81.

39. *Id.* at *81.

40. *Paice LLC*, 504 F.3d at 1314 (citing, e.g., Shatterproof Glass Corp. v. Libbey-Owens Ford Co., 758 F.2d 613, 628 (Fed. Cir. 1985) in which the Federal Circuit upheld a 5% court-ordered royalty, based on sales, "for continuing operations."). Other plaintiffs have also argued in favor of the successive suit theory. *See* Voda v. Cordis Corp., No. CIV-03-1512-L, 2006 U.S. Dist. LEXIS 63623, at *20–21 (W.D. Okla. Sep. 5, 2006) ("Plaintiff suggests severing his action for monetary damages for post-verdict infringement . . . The court sees no reason for severance of a cause of action for the post-verdict damages . . . The court therefore denies plaintiff's motion for severance.").

under § 284 of the Patent Act.[41] That is, whatever uncertainty may have existed prior to an adjudication, once a court rules in a final and unappealable decision that a patent is valid, enforceable and infringed, there is little doubt that continuing to practice the patent without the owner's consent constitutes infringement.[42] Accordingly, in many cases a fact finder could find unenjoined infringement in a subsequent proceeding to constitute "willful" infringement, thereby authorizing the court to award the patent holder enhanced damages.[43]

From a historical standpoint, Professor Tomás Gómez-Arostegui argues that successive suits are the only legally permissible way to compensate a patent holder for unenjoined infringement.[44] Specifically, he points out that the historical English courts sitting in equity did not grant prospective financial rewards, and current federal courts issuing remedies in equity may not exceed those historically available.[45] Professor Paul Janicke likewise argues that, under the Patent Act, a plaintiff may "elect to wait to recover damages for future wrongs after they occur by bringing successive actions" but that "compelling an unwilling plaintiff to accept judicially preset periodic payments for future infringements is not a remedy within the power of a federal court."[46]

Despite these considerations, as discussed in Part III below, most courts that have denied injunctions against continuing tortious conduct, whether

41. Once infringement has been established, a district court may "increase the damages up to three times the amount found or assessed." 35 U.S.C. § 284. Courts have interpreted this provision as giving rise to the possibility of enhanced damages when infringement has been "willful." *See* Halo Elecs., Inc. v. Pulse Elecs., Inc., 579 U.S. 93, 106 (2016).

42. *See* Janicke, *supra* note 26, at 186–87 (finding that infringements after judgment are "almost certainly willful").

43. *Id.*; Gómez-Arostegui, *supra* note 10, at 1663 ("A subsequent suit might strengthen the possibility of a willful-damages award"); Chao, *supra* note 10, at 569 ("If the defendant continues to infringe after losing a first lawsuit, a subsequent lawsuit carries the very real risk of a finding of willful infringement that would result in enhanced damages and attorneys fees.").

44. Gómez-Arostegui, *supra* note 10, at 1665 ("[A] plaintiff who succeeds on the merits of her case but who fails to obtain a final injunction must be allowed to periodically sue for any subsequent infringements, if she so chooses."). But *see* Mark A. Lemley, *The Ongoing Confusion Over Ongoing Royalties*, 76 MO. L. REV. 695, 697–99 (2011) (challenging Janicke's and Gómez-Arostegui's interpretations).

45. Tomás Gómez-Arostegui & Sean Bottomley, *The Traditional Burdens for Final Injunctions in Patent Cases c.1789 and Some Modern Implications*, 71 CASE W. RES. L. REV. 403, 442 (2020) ("[F]ederal courts lack the authority to award ongoing royalties for post-judgment infringements. Apart from the absence of statutory authorization, the English Court of Chancery did not recognize a remedy like this in 1789, which is the time and place the Supreme Court looks to for the default, equitable remedies of the federal courts."); Gómez-Arostegui, *supra* note 10, at 1666 ("[T]he compulsory licenses awarded by federal courts today are ultra vires because they were unknown in the Court of Chancery in 1789.").

46. Janicke, *supra* note 26, at 165.

patent infringement or nuisance, have *not* required injured parties to bring successive claims to recover for future harm. Doing so can be viewed as unduly burdensome to the injured parties, who must engage in, and pay for, protracted litigation, and inefficient for courts that must hear such repeated cases. As noted by one district court, the likely result is "an endless succession of lawsuits presenting the same issue."[47] As a result, most courts have determined the compensation to be paid to the injured party for future harm in the same set of proceedings in which the injunction was denied rather than forcing the parties to return to court for future proceedings at a later date.[48] Sections II.A.2 and II.A.3 below discuss the forms that such compensation takes.

2. Unenjoined Infringement Authorized by a Lump Sum Payment

If a court does not enjoin tortious conduct, such as patent infringement, then the court may award compensation for future harm to the injured party at the time the injunction is denied. This compensation may take one of two forms: a lump sum payment or an ongoing payment. This Section briefly discusses compensation for unenjoined infringement in the form of a lump sum payment while Section II.A.3, infra, turns to the more common remedy of ongoing royalties.

---

47. Ord. Granting in Part and Denying in Part Motion for Ongoing Royalties at 15, Apple, Inc. v. Samsung Elecs. Co., No. 12-CV-00630-LHK, (N.D. Cal. Feb. 15, 2018), ECF No. 2217) (quoting Lemley, *supra* note 44, at 697). *See also* Janicke, *supra* note 26, at 181 ("Few patent owners, having been put through the rigors, delays, and costs of patent litigation, will want to choose the successive suits option."); Norman V. Siebrasse, Rafal Sikorski, Jorge L. Contreras, Thomas F. Cotter, John Golden, Sang Jo Jong, Brian J. Love & David O. Taylor, *Injunctive Relief*, *in* PATENT REMEDIES AND COMPLEX PRODUCTS: TOWARD A GLOBAL CONSENSUS 115, 158 (C. Bradford Biddle et al. eds., 2019) ("forcing a patentee to relitigate a continuing course of infringement from scratch would threaten to unduly dilute the incentives that the patent system means to provide."); Lemley, *supra* note 44, at 697 ("[I]t seems odd to say that the only possible solution is to doom the parties, Zeno-like, to an endless succession of lawsuits presenting the same issue and leading (hopefully, at least) to the same outcome."). Indeed, the prospect of imposing on plaintiffs the burden of bringing successive lawsuits to recover for ongoing injuries is often raised as an argument for issuing injunctions in the first place. *See, e.g.*, Paice CAFC Brief, *supra* note 27, at *81; Michigan Law Review, *Equity and the Eco-System: Can Injunctions Clear the Air*?, 68 MICH. L. REV. 1254, 1280 (1970) ("[I]f the injury is continuous, any remedy other than an injunction may lead to the undesirable result of necessitating periodic suits by the plaintiff."). *But see* Janicke, *supra* note 26, at 181 ("In all events, successive actions may not be as burdensome to the courts as might at first appear. The issues of validity, enforceability, and scope will have already been adjudicated and hence will be precluded by the first judgment. Infringement may be a new issue if the product configuration has changed in some significant way, but all the other major issues in a typical patent case will be foreclosed.").

48. *See infra* Section III.B.

One well-known tort case in which a court awarded the plaintiffs a lump sum for a continuing nuisance that the court did not enjoin is *Boomer v. Atlantic Cement Co.*[49] In *Boomer*, a cement plant was permitted to continue to emit dirt, smoke, and vibrations that constituted a nuisance to neighboring landowners provided that it paid those landowners "permanent damages" to compensate them for the ongoing "servitude" that the nuisance imposed on their land.[50] The *Boomer* court relied on a long line of earlier nuisance cases awarding permanent damages when the abatement of a nuisance was not practical or possible.[51]

Lump sum payments are also routinely awarded to compensate patent holders for past infringement.[52] Likewise, lump sum awards may be made to compensate patent holders for *future* infringement, including in cases of unenjoined infringement.[53] As one district court explained,

> A second way to calculate a royalty is to determine a one-time lump sum payment that the infringer would have paid at the time of the hypothetical negotiation for a license covering all sales of the licensed product both past and future. This differs from payment of an ongoing royalty because, with an ongoing royalty, the licensee pays based on the revenue of actual licensed products it sells. When a one-time lump sum is paid, the infringer pays a single price for a license covering both past and future infringing sales.[54]

---

49. *See* Boomer v. Atl. Cement Co., 257 N.E.2d 870, 875 (N.Y. App. 1970).

50. *Id.*

51. *Id.* at 874.

52. Thomas F. Cotter, John M. Golden, Oskar Liivak, Brian J. Love, Norman V. Siebrasse, Masabumi Suzuki & David O. Taylor, *Reasonable Royalties*, *in* PATENT REMEDIES AND COMPLEX PRODUCTS: TOWARD A GLOBAL CONSENSUS 6, 31 (C. Bradford Biddle et al. eds., 2019).

53. *See* BASF Plant Sci., LP v. Commonwealth Sci. & Indus. Rsch. Org., No. 2:17-CV-503-HCM, 2019 WL 8108116, at *16 (E.D. Va. Dec. 23, 2019), *aff'd in part*, *rev'd in part, and remanded*, 28 F.4th 1247 (Fed. Cir. 2022). *See also* Christopher B. Seaman, *Ongoing Royalties in Patent Cases After eBay: An Empirical Assessment and Proposed Framework*, 23 TEX. INTELL. PROP. L.J. 203, 222 (2017) ("[A] jury may decide prospective compensation as part of a paid-in-full, 'lump sum' award for the life of the patent, which covers both past and future uses of the patented technology . . . If a jury awards a lump sum without specifying whether it was limited solely to past infringement, the district court may treat the lump sum as also encompassing all future uses.") (citing Regents of Univ. of Cal. v. Monsanto Co., No. C 04–0634 PJH, 2005 WL 3454107, at *26–28 (N.D. Cal. Dec. 16, 2005) and Personal Audio, LLC v. Apple, Inc., No. 9:09-CV-111, 2011 WL 3269330, at *13 (E.D. Tex. July 29, 2011)). *But see* Gómez-Arostegui & Bottomley, *supra* note 45, at 438 ("[S]ection 284 [of the Patent Act] compensates patentees for past, not future, infringements.").

54. Final Annotated Jury Instructions at 52, Apple, Inc. v. Samsung Elecs. Co., No. 12-CV-00630-LHK, 2014 WL 1883327, (N.D. Cal. Apr. 28, 2014), ECF No. 1848; Jury

Lump sum payments have several advantages over ongoing royalties, including simplicity, avoidance of future disputes, and immediate compensation of the patent holder.[55] Nevertheless, calculating the lump sum requires that important assumptions be made about the scope and extent of future infringement—assumptions that, if not borne out, could result in a lump sum that is higher or lower than needed to compensate the patent holder appropriately.[56]

Professor Paul Janicke points out that, in the context of unenjoined patent infringement, Section 284 of the Patent Act requires a court to award a successful patent holder "damages adequate to compensate for the infringement."[57] And because damages awarded by federal courts must generally be rendered in the form of lump-sum payments, absent statutory provisions to the contrary,[58] Janicke contends that a patent holder subjected to unenjoined infringement should be given the option to receive compensation in the form of a lump sum payment for future infringement and not be forced to accept "judicially preset periodic payments for future infringements."[59] Professor Mark Lemley disagrees with Janicke's interpretation of Section 284, arguing that "damages adequate to compensate for the infringement" may include ongoing royalties.[60] Moreover, as discussed in Part III below, most courts that compensate patent holders for unenjoined infringement have chosen to award ongoing royalties.

3. Unenjoined Infringement Authorized by an Ongoing Royalty

As an alternative to awarding a lump sum payment, district courts that have denied injunctions in patent infringement cases often establish ongoing royalty obligations to compensate patent holders for unenjoined infringement.[61] Though patent damages are usually decided by a jury, the level of ongoing royalties for unenjoined infringement is generally determined by a district court

Instructions at 33, Apple Inc. v. Samsung Elecs. Co., Ltd., No. 5:11-cv-01846-LHK, 2013 WL 11233253 (N.D. Cal. Nov. 18, 2013), ECF No. 2784.

55. *See* Seaman, *supra* note 53, at 224.

56. *See id.* at 225; Lemley, *supra* note 44, at 701; Gómez-Arostegui, *supra* note 10, at 1675.

57. Janicke, *supra* note 26, at 174–75.

58. *Id.* at 166 (citing cases outside of patent law), 174–75 (citing Federal Circuit cases), and 177–81 (drawing analogies to the Restatement (Second) of Torts).

59. *Id.* at 165.

60. *See* Lemley, *supra* note 44, at 697–98.

61. *See* infra Section III.B. *See also* Lisa M. Tittemore, The Controversy Over "Ongoing Royalty" Awards in the Evolving Landscape of Remedies for Patent Infringement, Fed. Lawyer, Nov.–Dec. 2009, at 29–30 ("[S]ince eBay, ongoing royalties have become far more prevalent").

as a matter of equity.[62] This being said, some courts have charged juries to determine such royalty rates in an advisory capacity.[63]

The amount of ongoing royalties can be either a per-unit fixed amount or a percentage of the infringer's net sales revenue from infringing products during the remaining life of the infringed patent(s).[64] Ongoing royalties are often based on, if not identical to, the jury-determined royalty for past infringement of the same patents, though numerous courts have varied these rates.[65] Significant scholarly and judicial attention has been devoted to the appropriate analytical framework for determining ongoing royalties for unenjoined infringement,[66] including whether such ongoing royalties should be higher than royalties awarded for past infringement due to the infringer's post-action willfulness.[67] Although important, these issues are beyond the scope of this Article.

B. IS UNENJOINED INFRINGEMENT COMPULSORY LICENSING?

As noted in the Introduction, some commentators have characterized a court's authorization of unenjoined infringement conditioned on the infringer's payment of compensation to the patent holder as the judicial issuance of a compulsory license.[68] Yet the Federal Circuit, in its first decision to consider the issue, generated considerable confusion by expressly denying that unenjoined infringement accompanied by an "ongoing royalty" is a compulsory license.[69] This Section considers the arguments that have been made with respect to the characterization of unenjoined infringement as judicially-ordered compulsory licensing.

---

62. Paice LLC v. Toyota Motor Corp., 504 F.3d 1293, 1316 (Fed. Cir. 2007) ("[T]he fact that monetary relief is at issue in this case does not, standing alone, warrant a jury trial"). *See* Seaman, *supra* note 53, at 220–21; Lemley, *supra* note 44, at 700. But see Gómez-Arostegui & Bottomley, *supra* note 45, at 442 ("[A] party should not be forced to face an equitable remedy assessed by a judge when an adequate remedy, and a right to a jury trial, would be available at law."); Ronald J. Schutz & Patrick M. Arenz, *Uncharted Waters: Determining Ongoing Royalties for Victorious Patent Holders Denied an Injunction*, 11 SEDONA CONF. J. 75, 78–80 (2010) (arguing that an ongoing royalty should be determined by a jury).

63. Seaman, *supra* note 53, at 221–22. *See also* Lemley, *supra* note 44, at 700.

64. *See* Seaman, *supra* note 53, at 225–27; Lemley, *supra* note 44, at 701.

65. *See* Seaman, *supra* note 53, at 227–28; Lemley, *supra* note 44, at 702.

66. *See* Siebrasse et al., *supra* note 47, at 157–59; Seaman, *supra* note 53, at 227–28; Lemley, *supra* note 44, at 700–7; Schutz & Arenz, *supra* note 62, at 82–83.

67. *See* generally Jonathan M. Barnett & David J. Kappos, Restoring Deterrence: *The Case for Enhanced Damages in a No-Injunction Patent System*, USC LAW LEGAL STUDIES PAPER NO. 22-2 (Feb. 14, 2022), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4034791; Siebrasse et al., *supra* note 47, at 158; Seaman, *supra* note 53, at 229; Lemley, *supra* note 44, at 702–3.

68. *See supra* notes 9–10, and accompanying discussion.

69. Paice LLC v. Toyota Motor Corp., 504 F.3d 1293, 1316 (Fed. Cir. 2007) (*Paice II*).

1. Defining Compulsory Licensing

To analyze whether unenjoined infringement is, in fact, compulsory licensing, it is useful first to understand precisely what constitutes compulsory licensing.

a) What is a License?

As provided by the Patent Act, "whoever *without authority* makes, uses, offers to sell, or sells any patented invention, within the United States or imports into the United States any patented invention during the term of the patent therefor, infringes the patent."[70] The "authority" referenced in the Act is typically referred to as a "license" to practice the patent.[71] A license "[i]n its simplest form . . . means only leave to do a thing which the licensor would otherwise have a right to prevent."[72] As described by the Federal Circuit, "[a] patent license agreement is in essence nothing more than a promise by the licensor not to sue the licensee."[73]

Agreements conferring patent licenses may take a variety of forms and, like other contracts, may be written, oral, or electronic. Likewise, patent licenses may be granted by implication, without the formal contractual mechanisms of offer and acceptance. As the Supreme Court observed nearly a century ago,

> No formal granting of a license is necessary in order to give it effect. Any language used by the owner of the patent or any conduct on his part exhibited to another, from which that other may properly infer that the owner consents to his use of the patent in making or using it, or selling it, upon which the other acts, constitutes a license . . . .[74]

The term "license" is thus fairly broad, encompassing a range of modalities. This Article discusses some of these in the following Sections.

b) What is a Compulsory License?

If a license is a promise by a patent holder not to assert its rights against the licensee's practice of a patent, then a *compulsory* license is such a promise when it is required of the patent holder by a governmental entity. As explained

70. 35 U.S.C. § 271(a) (emphasis added).

71. JORGE L. CONTRERAS, INTELLECTUAL PROPERTY LICENSING AND TRANSACTIONS: THEORY AND PRACTICE 47 (2022) [hereinafter CONTRERAS, IP TRANSACTIONS].

72. W. Elec. Co., Inc. v. Pacent Reproducer Corp., 42 F.2d 116, 117 (2d Cir. 1930).

73. Spindelfabrik Suessen-Schurr, Stahlecker & Grill GmbH v. Schubert & Salzer Maschinenfabrik Aktiengesellschaft, 829 F.2d 1075, 1081 (Fed. Cir. 1987). *See also* Jim Arnold Corp. v. Hydrotech Sys., 109 F.3d 1567, 1577 (Fed. Cir. 1997); Raymond C. Nordhaus, *Patent License Agreements*, 21 BUS. L. 643, 644 (1966) ("A nonexclusive license constitutes merely a waiver of infringement suit or covenant not to sue under the licensed patent.").

74. De Forest Radio Tel. & Tel. Co. v. United States, 273 U.S. 236, 241 (1927).

by the World Trade Organization (WTO), "[c]ompulsory licensing is when a government allows someone else to produce a patented product or process without the consent of the patent owner . . . "[75] Similarly, a recent report by the Congressional Research Service explains,

> The term "compulsory license" refers to the grant of permission for an enterprise seeking to use another's intellectual property to do so without the consent of its proprietor. The grant of a compulsory patent license typically requires the sanction of a governmental entity and provides for compensation to the patent owner.[76]

The involuntary compensatory nature of a compulsory license is highlighted by Dr. Rosa Castro Bernieri, who notes that "[u]nder a compulsory license, the IP right, which is traditionally conceived as a right to exclude, is transformed into a right to receive compensation."[77] As these definitions demonstrate, a compulsory license is simply a license that a patent holder is compelled, usually by a governmental body, to grant to another, generally with compensation.

Compulsory intellectual property licenses are authorized under two prominent multilateral international agreements. The Paris Convention for the Protection of Industrial Property,[78] originally adopted in 1883, has been adopted by 179 member states including the United States.[79] Provisions introduced to the Convention in 1925 provide that its members "have the right to take legislative measures providing for the grant of compulsory licenses to prevent the abuses which might result from the exercise of the exclusive rights conferred by the patent, for example, failure to work."[80]

---

75. *FAQ: Compulsory Licensing of Pharmaceuticals and TRIPS,* WORLD TRADE ORG., https://www.wto.org/english/tratop_e/trips_e/public_health_faq_e.htm (last accessed Apr. 6, 2023).

76. Thomas, *supra* note 2, at 1. *See also* Kumar, *supra* note 2, at 6 ("A compulsory license allows the government or a government-authorized third party to use or manufacture a patented good, or practice a patented process, without the patent owner's consent."); Cotropia, *supra* note 10, at 559 ("Compulsory licenses are an abrogation of a patentee's right, where the government allows itself or a third party to practice the patented invention without the patentee's consent.").

77. ROSA CASTRO BERNIERI, EX-POST LIABILITY RULES IN MODERN PATENT LAW 37 (2010).

78. *See* generally Paris Convention for the Protection of Industrial Property, July 14, 1967, 828 U.N.T.S 305 [hereinafter Paris Convention].

79. *See WIPO-Administered Treaties*, WORLD INTELL. PROP. ORG., https://www.wipo.int/wipolex/en/treaties/ShowResults?search_what=C&treaty_id=2 (last visited Oct. 25, 2023).

80. Paris Convention, *supra* note 78, art. 5(A)(2) (Hague Revision of 1925).

The Agreement on Trade-Related Aspects of Intellectual Property Rights (the "TRIPS Agreement")[81] was negotiated as part of the WTO Uruguay Round. Article 31 of the TRIPS Agreement permits WTO members to enact national laws that authorize the issuance of compulsory patent licenses to promote the public interest, counter anticompetitive conduct, or engage in noncommercial governmental use.[82] Since its adoption, more than a dozen countries have reportedly invoked the compulsory licensing provisions of the TRIPS Agreement, primarily in the areas of pharmaceutical products,[83] and as of 2014, 87 countries, including the United States, have enacted national legislation authorizing compulsory patent licensing in some form.[84]

As noted in the Introduction,[85] the issuance of compulsory patent licenses, particularly in the area of pharmaceutical products, has given rise to international sanction from countries including the United States. For example, when in 2012 the Indian Patent Office issued a compulsory license to local drug manufacturer Natco Pharma Ltd. to produce Bayer's patented anticancer therapy Nexavar,[86] U.S. government officials and legislators strenuously objected.[87] The non-profit group *Médicins sans Frontières* has cataloged numerous official and unofficial U.S. objections to compulsory patent licensing, particularly in India.[88]

c) Compulsory Patent Licensing in the U.S.

Despite U.S. opposition to compulsory licenses granted by foreign governments, numerous statutory provisions exist in the United States under which patent holders may legally be compelled to grant licenses to others.[89]

---

81. *See generally* TRIPS Agreement, *supra* note 6.

82. *Id.* art. 31. *See also* Cotropia, *supra* note 10, at 563–64.

83. *See* THOMAS F. COTTER, PATENT WARS: HOW PATENTS IMPACT OUR DAILY LIVES 200–1 (2018); Thomas, *supra* note 2, at 9–10.

84. WORLD INTELL. PROP. ORG., EXCEPTIONS AND LIMITATIONS TO PATENT RIGHTS: COMPULSORY LICENSES AND/OR GOVERNMENT USE (PART I) 2 (2014), https://www.wipo.int/edocs/mdocs/scp/en/scp_21/scp_21_4_rev.pdf.

85. *See supra* notes 2–4 and accompanying text.

86. *See* Jorge L. Contreras, Rohini Lakshané & Paxton M. Lewis, *Patent Working Requirements and Complex Products*, 7 NYU J. INTELL. PROP. & ENT. L. 1, 14–15 (2017).

87. *See* James Love, *USPTO and Congress Bash India over the Nexavar Compulsory License*, KNOWLEDGE ECOLOGY INT'L. (June 30, 2012), https://www.keionline.org/21883.

88. *A Timeline of U.S. Attacks on India's Patent Law & Generic Competition*, MEDICINS SANS FRONTIERES (Jan. 2015), https://msfaccess.org/sites/default/files/2018-10/IP_Timeline_US%20pressure%20on%20India_Sep%202014_0.pdf.

89. For a comprehensive catalog of these statutory provisions, see Jonathan M. Barnett, *The Great Patent Grab*, *in* THE BATTLE OVER PATENTS: HISTORY AND THE POLITICS OF INNOVATION 208, 276–77, Appx 6.B Compulsory patent licensing statutes, 1946–1975 (Stephen H. Haber & Naomi R. Lamoreaux eds., 2021).

For example, the U.S. federal government has the right itself, and through any government contractor, to practice any U.S. patent for government purposes, subject only to the payment of "reasonable and entire" compensation as determined by the U.S. Court of Federal Claims.[90] Under the Bayh-Dole Act of 1980, federal agencies may "march in" and require the holders of patents claiming inventions developed with federal funding to license those patents to others when necessary to achieve practical application of the invention, to satisfy health and safety needs, or to meet requirements for public use specified by federal regulation.[91] Likewise, the Atomic Energy Act authorizes the Atomic Energy Commission to grant patent licenses to parties in the nuclear power and fuel industries "if the invention or discovery covered by the patent is of primary importance in the production or utilization of special nuclear material or atomic energy."[92]

The authority to impose compulsory patent licenses in the United States is not limited to actions by federal agencies. Under the Clean Air Act, a district court, upon application of the Attorney General, may require a patent holder "to license [a patent] on such reasonable terms and conditions as the court, after hearing, may determine" when necessary to enable others to comply with federal requirements relating to stationary sources of air pollutants or motor vehicle emissions.[93]

While it is not clear how many, if any, compulsory licenses have been granted by courts under the Clean Air Act,[94] there are abundant examples of federal courts that have ordered the compulsory licensing of patents to remedy anticompetitive conduct. More than one hundred such judicial orders were issued in antitrust cases from the 1940s to the 1970s.[95] As noted by the Supreme Court in *United States v. National Lead Co.*, "assurance against

90. 28 U.S.C. § 1498(a). *See also* Kumar, *supra* note 2, at 9.

91. *See* 35 U.S.C. § 203(a).

92. *See* 42 U.S.C. §§ 2183(c)–(e).

93. *See* 42 U.S.C. § 7608.

94. *See* Thomas, *supra* note 2, at 7 n. 43 (indicating the author's unawareness of any invocation of such compulsory licensing regulations).

95. *See, e.g.*, Barnett, *supra* note 89, at 259–75, Appx. A (listing orders from the 1940s to the 1970s); Jorge L. Contreras, *A Brief History of FRAND: Analyzing Current Debates in Standard-Setting and Antitrust Through a Historical Lens*, 80 ANTITRUST L.J. 39, 74 (2015) (identifying and discussing such orders); F.M. Scherer, *The Political Economy of Patent Policy Reform in the United States*, 7 J. TELECOM. & HIGH TECH. L. 167, 170 (2009) ("Between 1941 and the late 1950s, compulsory licensing decrees had been issued in settlement of more than 100 antitrust complaints"); Delrahim, *supra* note 7, at 1 ("From the U.S. Supreme Court's decision in Besser Manufacturing, to the district court's decision fifty years later in *United States v. Microsoft Corporation*, courts have recognized that compulsory licensing can be a necessary remedy in some [antitrust] cases.").

continued illegal restraints upon interstate and foreign commerce through misuse of these patent rights is provided through the compulsory granting to any applicant therefor of licenses at uniform, reasonable royalties under any or all patents defined in the decree."[96]

Even in patent infringement cases prior to *eBay*, several courts, including the Federal Circuit, recognized that the combination of the denial of an injunction with an ongoing royalty payment effectively gives rise to a compulsory license. For example, in *Shatterproof Glass Corp. v. Libbey-Owens Ford Co.*, the Federal Circuit upheld a district court's order that "denied Shatterproof's request for injunction and granted Libbey-Owens Ford a compulsory license to permit future practice under the . . . patents at a royalty rate of 5%."[97] In the same year, the Federal Circuit in *Atlas Powder Co. v. Ireco Chemicals* expressed concern that "[i]f monetary relief were the sole relief afforded by the patent statute then injunctions would be unnecessary and infringers could become compulsory licensees . . . ."[98] Likewise, in *Monsanto Co. v. Ralph*, the Federal Circuit held that "the imposition on a patent owner who would not have licensed his invention for [a given] royalty is a form of compulsory license, against the will and interest of the person wronged, in favor of the wrongdoer."[99] And in *Foster v. American Machine & Foundry Co.*, a pre-Federal Circuit case, the Second Circuit affirmed a district court's denial of permanent injunction where, after balancing the equities between the parties, the court concluded that the patentee would benefit from a "compulsory royalty."[100] All of these cases indicate that federal courts viewed themselves as having the authority to grant compulsory patent licenses through the denial of permanent injunctions.

d) A Compulsory License Need Not Be a Public License

A *public* license is an intellectual property license that is made available to the public at large, often without charge.[101] Public licenses exist in numerous contexts and are probably best known in the areas of open source code

96. United States v. Nat'l Lead Co., 332 U.S. 319, 348 (1947).

97. Shatterproof Glass Corp. v. Libbey-Owens Ford Co., 758 F.2d 613, 616 (Fed. Cir. 1985).

98. Atlas Powder Co. v. Ireco Chems., 773 F.2d 1230, 1233 (Fed. Cir. 1985).

99. Monsanto Co. v. Ralph, 382 F.3d 1374, 1384 (Fed. Cir. 2004) (quoting Del Mar Avionics, Inc. v. Quinton Instrument Co., 836 F.2d 1320, 1328 (Fed. Cir. 1987) (internal quotation marks omitted)).

100. Foster v. Am. Mach. & Foundry Co., 492 F.2d 1317, 1324 (2d Cir. 1974).

101. *See* CONTRERAS, IP TRANSACTIONS, *supra* note 71, at 592; Christina Mulligan, *A Numerus Clausus Principle for Intellectual Property*, 80 TENN. L. REV. 235, 271 (2013) ("With a public license, a copyright owner creates or chooses a blanket license for a work, allowing anyone to use the work according to the terms.").

software[102] and online content licensed under the Creative Commons suite of licenses.[103] While both of these licensing regimes largely concern copyrights, public licenses also exist with respect to patents, as illustrated by the large number of patents licensed to all takers under the Open COVID Pledge.[104] In each of these cases, the intellectual property holder offers a standardized set of licensing terms that may be accepted by any party that wishes to utilize the licensed rights on the terms offered.

Though license holders, like the ones noted above, offer most public licenses willingly, public licenses may also be compulsory. For example, the U.S. Copyright Act requires copyright holders to grant licenses of their copyrights in certain musical compositions to any party that pays a statutorily determined licensing fee (better known as the right to "cover" a previously recorded song).[105] This provision of the Copyright Act establishes a compulsory licensing regime requiring the granting of public licenses. Likewise, as discussed in Section II.B.1.c, *supra*, when patent holders were found to have violated the antitrust laws in several historical cases, courts ordered them to make licenses available to "all applicants," either on a royalty-bearing or royalty-free basis.[106]

However, the fact that some compulsory licenses, such as those authorized under the Copyright Act and in antitrust cases, are public licenses does not mean that *all* compulsory licenses must be public licenses.[107] In fact, many of

102. *See*, e.g., Jacobsen v. Katzer, 535 F.3d 1373, 1376 (discussing a licensor making software source code "available for public download from a website without a financial fee pursuant to the Artistic License, an 'open source' or public license."); Mulligan, *supra* note 101, at 271–72 (discussing many program creators contribute to open source projects under public licenses).

103. *See* CONTRERAS, IP TRANSACTIONS, *supra* note 71, at 594–95 ("The CC licenses are 'public' licenses. That is, they are not specifically negotiated between copyright owners and users, but are publicly posted and can be 'accepted' by anyone who wishes to use the licensed content."); Mulligan, *supra* note 101, at 271–72.

104. *See* Jorge L. Contreras, *The Open COVID Pledge: Design, Implementation and Preliminary Assessment of an Intellectual Property Commons*, UTAH L. REV. 833, 842 (2021).

105. *See* 17 U.S.C. § 115. For other compulsory licensing regimes established under the Copyright Act, see 17 U.S.C. §§ 111(c) (cable retransmission of broadcast television programming), 116(a) (performance of musical works by coin-operated jukeboxes), 118(d) (performance of copyrighted works by public broadcasters).

106. *See*, e.g., United States v. Nat'l Lead Co., 332 U.S. 319, 348 (1947) ("Further assurance against continued illegal restraints upon interstate and foreign commerce through misuse of these patent rights is provided through the compulsory granting to any applicant therefor of licenses at uniform, reasonable royalties under any or all patents defined in the decree.") (italics added). *See also supra* note 95, and sources cited therein.

107. BERNIERI, *supra* note 77, at 40 (distinguishing compulsory licenses based on whether they are authorized "ex ante" and thus apply uniformly in all cases, or ex post, applying "on a case-by-case basis.").

the most prominent compulsory licenses in the world—those granted with respect to patented pharmaceutical products—have typically been granted to a single local manufacturer.[108] Similarly, as described in Section II.B.1.c, *supra*, most statutory regimes authorizing compulsory licensing in the United States are directed toward the granting of a license to one or more selected licensees, not to the public at large. Thus, there is no general requirement that a compulsory license must be structured as a public license.[109]

2. *The Federal Circuit's Mistaken Distinction Between Ongoing Royalty and Compulsory License in Paice*

As noted in Section II.A.1, *supra*, the Federal Circuit in *Paice v. Toyota* (*Paice II*) affirmed the district court's award of an ongoing royalty to compensate the patent holder for future infringement following the denial of an injunction. Judge Prost, writing for the majority, confirmed the district court's authority to "step in to assess a reasonable royalty in light of the ongoing infringement" when the parties themselves are unable to "negotiate a license amongst themselves regarding future use of a patented invention."[110] Yet Judge Prost is careful not to refer to Toyota's continuing ability to practice Paice's patent as a "compulsory license."[111] Rather, she introduces a key distinction to avoid this term, explaining that "[w]e use the term *ongoing royalty* to distinguish this equitable remedy from a compulsory license."[112]

---

108. *See* Thomas, *supra* note 2, at 10–12 (discussing compulsory patent licenses granted in Brazil, India, South Africa, and Thailand).

109. *But see* Brief Amici Curiae of 52 Intellectual Property Professors in Support of Petitioners at 9, eBay Inc. v. MercExchange LLC, 547 U.S. 388 (05-130) (2006) [hereinafter Amicus Brief of Professors] ("A compulsory license is a blanket rule that permits all others to use a patent upon payment of a specified royalty, giving certainty to those who would infringe the patent that they can do so upon payment of a royalty."). Amici cite no authority for this proposition. Interestingly, the counsel of record (and presumably the principal author) of this brief, Professor Lemley, does not repeat this argument in his 2011 article addressing the issue of unenjoined infringement. *See* Lemley, *supra* note 44, at 11.

110. Paice LLC v. Toyota Motor Corp., 504 F.3d 1293, 1315 (Fed. Cir. 2007) (*Paice II*). Though the Federal Circuit in *Paice* affirmed the district court's authority to set an ongoing royalty for unenjoined infringement, it criticized the district court's failure to explain adequately its rationale for setting the ongoing royalty at $25 per vehicle and remanded the case for reconsideration of the royalty rate.

111. Paice, in its briefing to the Federal Circuit, unequivocally referred to the unenjoined infringement authorized by the district court as a "compulsory license." *See* Paice CAFC Brief, *supra* note 27, at *41 ("The district court erred in setting, sua sponte, a prospective royalty for the remaining life of the '970 patent. In setting this prospective royalty based on the jury's past damages calculation, the district court imposed a compulsory license on the parties. This action was without statutory or precedential basis.").

112. *Paice II*, 504 F.2d at 1313 n.13 (emphasis added). Though the Federal Circuit in Paice II affirmed the district court's authority to set an ongoing royalty for unenjoined infringement,

Unfortunately, Judge Prost's distinction in *Paice II* between an "ongoing royalty" and a "compulsory license" is both incoherent and mistaken. From a purely technical standpoint, the distinction is based on a category error. A *royalty* is a form of compensation, typically distinguished, in patent cases, from an up-front or lump sum payment.[113] A *license* is a grant of legal rights.[114] A payment is not a grant of rights and does not connote any permission or authority for the ongoing infringer to continue to practice the patented invention. Judge Prost acknowledges that some ongoing authorization for unenjoined infringement is granted when she suggests that the parties first be given an opportunity to negotiate a *license* amongst themselves.[115] If they cannot, then the court may step in to determine the applicable ongoing *royalty*. Yet if payment of that ongoing royalty insulates the ongoing infringer from future damage suits, merely calling the payment an ongoing royalty does not make it less of a permission.[116]

More importantly, Judge Prost's justification for distinguishing between a compulsory license and an ongoing royalty is based on a misunderstanding of the term "compulsory license." She writes: "The term 'compulsory license' implies that *anyone* who meets certain criteria has congressional authority to use that which is licensed." To support this assertion, she cites Section 115 of the Copyright Act,[117] which pertains to "cover" recordings of musical compositions (see Section II.B.1.c, *supra*).[118] She then concludes that because the ongoing patent royalty awarded by the district court in *Paice I* applies only to Toyota, "there is no implied authority in the court's order for any other auto manufacturer to follow in Toyota's footsteps and use the patented invention

it criticized the district court's failure to explain adequately its rationale for setting the ongoing royalty at $25 per vehicle and remanded the case for reconsideration of the royalty rate. *Id.*

113. *See* CONTRERAS, IP TRANSACTIONS, *supra* note 71, at 14.

114. *See* Christopher M. Newman, *A License is Not a "Contract Not to Sue": Disentangling Property and Contract in the Law of Copyright Licenses*, 98 IOWA L. REV. 1101 (2013).

115. *See Paice II*, 504 F.3d at 1315; *see also* Soverain Software LLC v. Newegg Inc., 836 F. Supp. 2d 462, 483 (E.D. Tex. 2010) ("[T]he Federal Circuit has encouraged parties to negotiate a license amongst themselves regarding the future use of a patented technology before imposing an ongoing royalty." (citing *Paice II* and Paice LLC v. Toyota Motors Corp., 609 F. Supp. 2d 620 (E.D. Tex. 2009)); Orion IP, LLC v. Mercedes-Benz USA, LLC, No. 6:05 CV 322, 2008 U.S. Dist. LEXIS 108683, at *12 (E.D. Tex. Mar. 28, 2008) (articulating the same standard).

116. Moreover, the term "ongoing royalty" does not encompass judicially authorized unenjoined infringement that is coupled with a lump sum payment (see Section II.A.2 above). Thus, in addition to being grammatically unsound, the term "ongoing royalty" is overly narrow.

117. 17 U.S.C. § 115

118. *Paice II*, 504 F.3d at 1313 n.13.

with the court's imprimatur."[119] In short, Judge Prost reasons that because Toyota is the *only* infringer authorized by the court to continue to practice Paice's patent, this authorization cannot be a compulsory license. Rather, it is something else: an ongoing royalty.

This conclusion is incorrect. As explained in Section II.B.1.c, a *compulsory* license need not be a *public* license. While some compulsory licensing schemes, such as those established under the Copyright Act, do give rise to public licenses, public use is not a requirement for a license to be compulsory. In fact, many compulsory licenses are not public licenses. Rather, such licenses authorize a single company—often a generic drug manufacturer—to produce a patented product that the patent holder cannot or will not distribute in the issuing country. Even in the U.S., most statutory compulsory licensing regimes, and all such regimes pertaining to patents, allow the authorization of one or a selected group of entities to practice a patented invention and do not open the patented technology to all comers.[120] Judge Prost's conflation of a compulsory license with a public license, and the resulting removal of unenjoined infringement from the ambit of compulsory licensing, is thus based on a faulty premise without support under U.S. law.

Judge Rader points out this error in reasoning in his concurring opinion in *Paice II*. He recognizes the sleight of hand performed by the court, observing that "calling a compulsory license an 'ongoing royalty' does not make it any less a compulsory license."[121] For this reason, Judge Rader encourages district courts to permit the parties to negotiate the terms of a license for unenjoined infringement. If the parties do so, he reasons, then the ongoing royalty they negotiate would be just that, and not a compulsory license.[122] Yet if the court steps in and determines the ongoing royalty, then it has established the compensation for unenjoined infringement, removed any further ability of the patent holder to sue the infringer for damages (e.g., in successive suits), and effectively granted a compulsory license.

Academic commentators have recognized that an ongoing royalty coupled with unenjoined infringement is effectively a compulsory license. Professor Bernard Chao notes that the Federal Circuit has approved "granting a compulsory license to the losing defendant which the courts now call an

119. *Id.*

120. *See supra* Section B.1.d.

121. *Paice II*, 504 F.3d at 1316 (Rader, J., concurring). *See also* Hynix Semiconductor Inc. v. Rambus Inc., 609 F. Supp. 2d 951, 983 (N.D. Cal. 2009) (it is a "faulty assumption [to assume] that because one infringer received a compulsory license, others would be free to infringe and entitled to a similar compulsory license.").

122. *See Paice II*, 504 F.3d at 1316 (Rader, J., concurring).

'ongoing royalty.'"[123] Professor Daniel Crane acknowledges then embraces this move toward compulsory licensing as a desirable systemic shift toward a liability-based regime for intellectual property.[124]

Nevertheless, some courts have followed Judge Prost's reasoning in *Paice II* and denied that their establishment of ongoing royalties for unenjoined infringement is tantamount to a compulsory license.[125] Commentators, too, have echoed this argument. Professor Janicke, for example, argues that an ongoing royalty coupled with unenjoined infringement "is neither compulsory nor a license."[126] Yet he fails to follow through on this assertion, arguing instead that courts are simply not authorized to exonerate unenjoined infringement from successive lawsuits for damages.[127] He then seeks to distinguish the rationales underlying existing forms of compulsory licensing (i.e., compulsory licenses granted as remedies in antitrust cases) from the justifications for unenjoined infringement.[128] However, he does not advance any argument to refute the notion that a court that has established an ongoing royalty for unenjoined infringement has in fact granted a compulsory license. Thus, while Professor Janicke does not think that courts *should* grant such compulsory licenses (a conclusion as to which we remain neutral), he does not actually deny that courts are, in fact, doing so.

Professor Christopher Seaman likewise rejects the proposition that courts awarding ongoing royalties following the denial of an injunction are effectively granting compulsory patent licenses. He offers three reasons in support of this position. First, he repeats Judge Prost's assertion that a compulsory license must be a public license.[129] Second, he argues that a patentee that is denied an

123. Chao, *supra* note 10, at 545.

124. Crane, *supra* note 10, at 254 ("Intellectual property is incrementally moving away from the conventional right of the landowner to fence out trespassers and toward a right to collect royalties from constructive licensees. As a categorical matter, this trend away from a right to exclude toward a right to collect royalties represents a shift from a property regime to a liability regime.").

125. *See*, e.g., Creative Internet Adver. Corp. v. Yahoo! Inc., 674 F. Supp. 2d 847, 852 n.6 (E.D. Tex. 2009) ("As discussed by the Federal Circuit in *Paice II*, the Court rejects any suggestion that it is imposing a 'compulsory license' under 17 U.S.C. § 115. The term 'compulsory license' implies that anyone who meets certain criteria has congressional authority to use that which is licensed. The ongoing royalty contemplated in this case is limited to the Defendant Yahoo that was found to infringe the '432 patent.") (citations omitted). The court adjudicating this case is clearly confused, given its reference to 17 U.S.C. § 115, the compulsory licensing provision for cover recordings under the Copyright Act, which has no bearing on the case.

126. Janicke, *supra* note 26, at 165.

127. *See id.* at 174–75.

128. *See id.* at 175–77.

129. *See* Seaman, *Ongoing Royalties*, *supra* note 53, at 216.

injunction need not seek an ongoing royalty and may instead bring successive actions for monetary damages for unenjoined infringement.[130] As such, he reasons, an ongoing royalty is not "compulsory." Nevertheless, various courts, including the Federal Circuit in *Paice II*, have held that courts *do* have the authority, upon request of the infringer (and over the objection of the patent holder), to establish an ongoing royalty for unenjoined infringement.[131] It is thus compulsory. Finally, Professor Seaman asserts that a court-imposed ongoing royalty differs from a "traditional" licensing agreement in that the remedy for breach of the royalty obligation would arise through the court's contempt power rather than an action in breach of contract.[132] While this observation may be correct, the nature of the remedy available for breach does not make a judicially authorized compulsory license any less a compulsory license. Certainly, many well-known compulsory licenses established by judicial order, and even by statute,[133] would be redressed through remedies other than private claims for breach of contract, yet this does not disqualify them as compulsory licenses.

As the above discussion demonstrates, there is considerable uncertainty and disagreement regarding the nature of the legal authority of an unenjoined infringer to practice an infringed patent. To shed further light on the way courts themselves are interpreting this authority, we conducted an empirical assessment of judicial opinions described in the following Part.

III. JUDICIAL CHARACTERIZATION OF UNENJOINED INFRINGEMENT AS COMPULSORY LICENSING IN POST-*EBAY* CASES

To gain a better understanding of how U.S. courts view the legal nature of unenjoined infringement, we reviewed all post-*eBay* district court decisions (and Federal Circuit appeals) in patent infringement cases in which a permanent injunction was denied. We describe the methodology that we used to collect and code these decisions in Section III.A below. We then report the aggregate trends identified as well as specific uses of language relating to ongoing royalties and compulsory licensing in Sections III.B and III.C, respectively. We discuss the conclusions that we draw from these findings in Section III.D.

130. *See id.*
131. *See* Paice LLC v. Toyota Motor Corp., 504 F.3d 1293, 1315 (Fed. Cir. 2007) (*Paice II*).
132. *See* Seaman, *Ongoing Royalties*, *supra* note 53, at 216.
133. *See supra* Section II.B.1.

A. METHODOLOGY

We identified all U.S. district court cases decided between May 15, 2006 (the date of the Supreme Court's decision in *eBay*) and July 5, 2021 (the date of our first search) in which (1) a finding of patent infringement was made and (2) a permanent injunction was denied.[134] To do so, we queried the LexMachina database for patent infringement cases decided during that date range in which an injunctive remedy was sought. We excluded cases in which allegations of patent infringement were combined with other causes of action, such as trademark, copyright, trade secret, contract, and antitrust claims, as we wished to analyze judicial language relating exclusively to the treatment of unenjoined *patent* infringement and to avoid entanglement with other causes of action. We also excluded cases involving claims of patent infringement based on 35 U.S.C. § 271(e)(2) with respect to the filing of an Abbreviated New Drug Application (ANDA), as these cases appeared, as a category, to raise different issues than other patent infringement suits.[135] Finally, because we wished to assess judicial reasoning in the context of denied injunctions, we excluded cases in which a court awarded an ongoing royalty for unenjoined infringement but the patent holder did not seek a permanent injunction.[136]

After these exclusions, our search yielded 263 cases, in 68 of which a permanent injunction was denied and in 195 of which a permanent injunction was granted (including by default judgment). We supplemented these results with additional cases meeting these criteria that we identified through a Lexis search[137] or that were mentioned in the literature and online sources (8 cases), and one case in which a district court's grant of an injunction was reversed by

134. We did not consider decisions regarding preliminary injunctions, as the standards for obtaining preliminary injunctive relief differ materially from those applicable to permanent injunctive relief, and the remedy is grounded in the rules of civil procedure rather than traditional equitable remedy law. *See* John C. Jarosz, Jorge L. Contreras & Robert L. Vigil, *Preliminary Injunctive Relief in Patent Cases: Repairing Irreparable Harm,* 31 TEX. INTELL. PROP. L.J. 63 (2023).

135. Under 35 U.S.C. § 271(e)(2), the filing of an ANDA for a generic drug infringing the patent on an already marketed drug is deemed to constitute patent infringement, as to which an injunction ordinarily issues.

136. *See, e.g.*, Optis Wireless Tech. v. Apple Inc., No. 2:19-CV-00066-JRG, 2021 U.S. Dist. LEXIS 110317 (E.D. Tex. Apr. 14, 2021); SRI Int'l, Inc. v. Cisco Sys., Inc., 254 F. Supp. 3d 680, 724 (D. Del. 2017); Arctic Cat Inc. v. Bombardier Rec. Prods., No. 14-cv-62369-BLOOM/Valle, 2016 U.S. Dist. LEXIS 107654 (S.D. Fla. Aug. 12, 2016); Prism Techs., LLC v. Sprint Spectrum L.P., No. 8:12CV123, 2015 U.S. Dist. LEXIS 169398 (D. Neb. Dec. 18, 2015); Saffran v. Bos. Sci. Corp., No. 2-05-CV-547 (TJW), 2008 U.S. Dist. LEXIS 106711 (E.D. Tex. Feb. 14, 2008).

137. The search query used was: "ebay" and ("ongoing" or "running" or "future royalt*" or "compulsory license") and "patent."

the Federal Circuit, yielding a total of 77 cases involving unenjoined infringement ("Reviewed Cases").[138]

We manually reviewed relevant documents from the dockets in each Reviewed Case, including judicial orders, written opinions, jury instructions, and party pleadings, as well as the case's subsequent history and decisions on appeal. In each case, we determined the type of past and future damages awarded (e.g., lump-sum or ongoing royalty payments), if any. We then reviewed the text of each judicial decision and identified the language used by the district court, as well as any appellate court reviewing the decision below, relating to unenjoined infringement. Our findings and descriptive statistics are presented in Section III.B, below.

B. FINDINGS

1. Injunction Grants Versus Denials

As noted in Section III.A, above, we identified a total of 272 post-*eBay* patent infringement cases in which a permanent injunction was sought. An injunction was issued in 195 of these cases (72%) and denied in 77 of these cases (28%).[139]

Because we wished to determine whether particular judges or courts adopted distinct interpretations of the legal nature of unenjoined infringement, we analyzed our results by federal judicial district. *Figure 1* below illustrates the distribution of these cases among U.S. district courts in each judicial district that denied at least one permanent injunction (a total of 212 cases).[140]

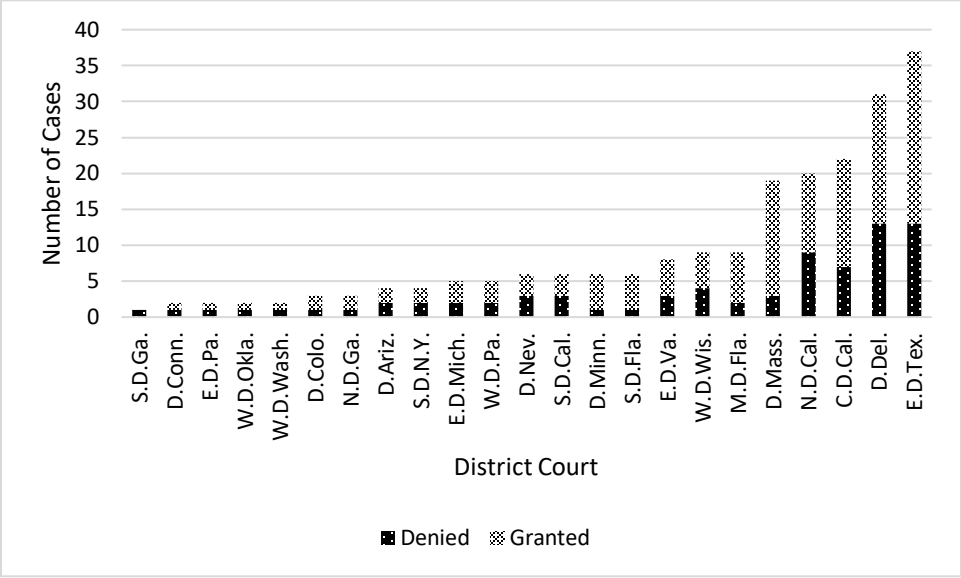
---

138. Our goal was not to identify every district court patent infringement case in which an injunction was denied, but only a meaningful sample of such cases. In an earlier study, Professor Seaman analyzed 218 patent infringement cases between 2006 and 2014 in which an injunction was sought and found that injunctions were denied in 27.5% of those cases (59 cases). Seaman, *Permanent Injunctions*, *supra* note 23, at 1976, 1982. In subsequent work, Professor Seaman identified 57 cases from the same data set in which both a permanent injunction was denied and an ongoing royalty was awarded. Seaman, *Ongoing Royalties, supra* note 53, at 231. Because these studies have different aims, Seaman's exclusion criteria are less restrictive than ours, perhaps explaining the greater number of cases that he identified (e.g., several cases included in *Ongoing Royalties* include trade secret claims, which we excluded from our data set).

139. These results are consistent with post-*eBay* injunction grant rates found in prior empirical studies. *See supra* note 23, and accompanying text.

140. Includes all 77 patent cases in which a permanent injunction was denied, and 135 of the 195 patent cases in which a permanent injunction was issued. It is interesting to note that some judicial districts with relatively high numbers of patent cases, such as the Northern District of Illinois (9 cases), the District of New Jersey (4 cases), the District of Utah (4 cases) and the Northern District of Texas (4 cases), denied no injunctions during the period studied.

Figure 1: All Districts (>1) Injunctions Granted/Denied (2006–20) (n=212)



As shown in Figure 1, during the period studied, the Eastern District of Texas denied permanent injunctions in 13 out of 37 cases (35%). It is followed in total case volume by the District of Delaware (13 out of 31 cases, 42%), the Central District of California (7 out of 22 cases, 32%), and the Northern District of California (9 out of 20 cases, 45%). Among the fourteen district courts that decided five or more patent injunction cases during the period studied, the rate of denial ranged from 50% (Southern District of California) to 16% (District of Massachusetts), with an average denial rate of 35%. These findings suggest that there is not a strong bias for or against the issuance of patent injunctions in any particular judicial district.

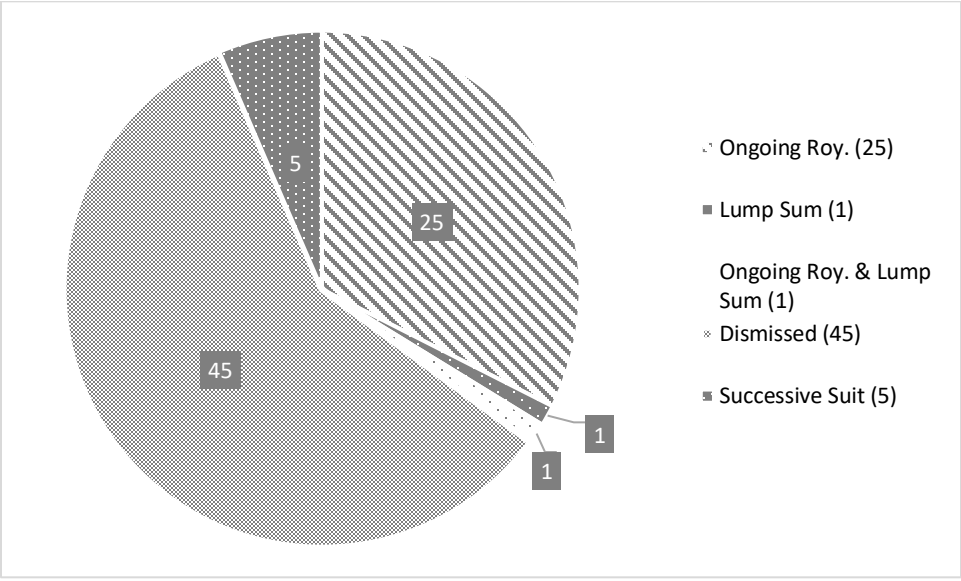
2. Compensation for Unenjoined Infringement

For each of the seventy-seven Reviewed Cases, we determined whether the court: (1) awarded an ongoing royalty ("OR") for future infringement (25 cases, 32%),[141] (2) awarded a lump sum payment for future infringement (1 case, 1%), (3) awarded both an ongoing royalty and a lump sum payment for future infringement (1 case, 1%), (4) expressly acknowledged the patent

141. In addition to the term "ongoing royalty" when referring to compensation for unenjoined infringement, some courts have used the terms "running royalty" and "future damages." *See, e.g.*, Centripetal Networks, Inc. v. Cisco Sys., 492 F. Supp. 3d 495 (E.D. Va. 2020); Tex. Advanced Optoelectronic Sols., Inc. v. Intersil Corp., No. 4:08-CV-451, 2016 U.S. Dist. LEXIS 53948 at 17 (E.D. Tex. Apr. 22, 2016). We have included these terms in the category for ongoing royalties ("OR").

holder's ability to bring successive suits for damages with respect to unenjoined infringement (5 cases, 10%), or (5) specified no compensation as a result of the termination of the litigation via settlement, dismissal or default or the mooting of the question through patent expiration, invalidity or noninfringement (45 cases, 58%). Figure 2 below illustrates the breakdown of different remedies awarded by these courts following the denial of an injunction.

Figure 2: Compensation for Unenjoined Infringement (n=77)



3. District Court Characterization of Unenjoined Infringement as Compulsory Licensing

District courts awarded ongoing royalties for unenjoined infringement in twenty-six of the Reviewed Cases (one of which also included a lump sum payment as partial compensation for future unenjoined infringement). We analyzed the language used by each court when discussing these ongoing royalties.

a) District Court Descriptions of Ongoing Royalties

Most district courts awarding ongoing royalties for unenjoined infringement instructed juries on the meaning of the term "royalty." This instruction read, in nearly identical language in ten different cases, "[a] royalty is a payment made to a patent holder in exchange for the *right* to make, use, or

sell the claimed invention."[142] These courts thus link the payment of an ongoing royalty with the granting of a "right" to practice the infringed patent—a license.

Several other district courts make clear the connection between the ongoing royalty awarded by the court and the unenjoined infringer's right to "use" the patented invention—again describing what amounts to a license. For example, the district court in *BASF Plant Science, LP v. Commonwealth Scientific & Industrial Research Organisation* explained that a court may "impose an ongoing royalty for the adjudged infringer to pay *in order to use* the infringing products."[143] And in *Apple, Inc. v. Samsung Electronics Co.*, the district court stated that "[a]n ongoing royalty permits an adjudged infringer to *continue using* a patented invention for a price."[144]

b) District Court References to Compulsory Licensing

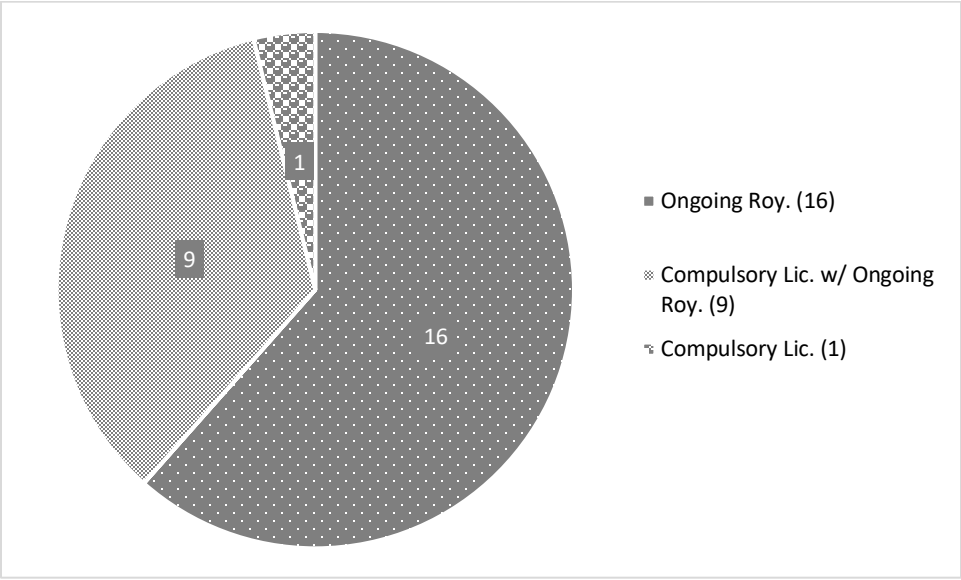
In several cases in which an ongoing royalty was established, the district court expressly referred to the granting of a compulsory license. Figure 3 below breaks down the twenty-six ongoing royalty cases according to whether the court (1) referred only to an ongoing royalty without reference to compulsory licensing (or expressly disavowed compulsory licensing, as in *Paice*) (16 cases, 62%, "OR"), (2) referred both to an ongoing royalty and compulsory licensing (9 cases, 35%, "CL with OR"), or (3) referred only to compulsory licensing without mentioning an ongoing royalty (1 case, 4%, "CL").

142. Jury Instructions at 34, Tex. Advanced Optoelectronic Sols., Inc. v. Intersil Corp., No. 4:08-cv-00451-RAS, 2015 WL 5244713 (E.D. Tex. Mar. 4, 2015) (No. 506) (emphasis added).

143. No. 2:17-CV-503-HCM, 2019 U.S. Dist. LEXIS 228305, at *63 (E.D. Va. Dec. 20, 2019).

144. No. 12-CV-00630-LHK, 2014 U.S. Dist. LEXIS 165975, at *83 (N.D. Cal. Nov. 25, 2014). *See also* Humanscale Corp. v. CompX Int'l Inc., No. 3:09-CV-86, 2010 U.S. Dist. LEXIS 42083, at *12–13 (E.D. Va. Apr. 29, 2010) ("CompX sought and was awarded by the jury future royalties to compensate it for Humanscale's *use* of the McConnell patents until they expire.") (emphasis added); Tex. Advanced Optoelectronic Sols., Inc. v. Intersil Corp., No. 4:08-CV-451, 2016 U.S. Dist. LEXIS 53948, at *17 (E.D. Tex. Apr. 22, 2016) ("Since the Defendant has admitted to the *ongoing sale* of at least one Infringing Product, a running royalty is appropriate.") (emphasis added).

Figure 3: Judicial Use of Compulsory License (CL) Terminology with Ongoing Royalty (OR) Following Unenjoined Infringement (n=26)



When discussing compulsory licenses, the language used by courts was unambiguous. For example, the district court in *Bard Peripheral Vascular, Inc. v. W.L. Gore & Associates* stated that:

> [T]o compensate Plaintiffs for future harm, the Court can impose a *compulsory license* on the continued sales of [Defendant's] infringing products for the remainder of the life of the [Plaintiff's] patent. The Court is satisfied that a fair and full amount of compensatory money damages, when combined with a progressive *compulsory license*, will adequately compensate Plaintiffs' injuries, such that the harsh and extraordinary remedy of injunction—with its potentially devastating public health consequences—can be avoided.[145]

In some instances, courts referred both to an ongoing royalty and a compulsory license, essentially equating the two terms. For example, in *BASF Plant Science, LP v. Commonwealth Scientific & Industrial Research Organisation*, the court held that "[a]n ongoing royalty is essentially a compulsory license for

145. Bard Peripheral Vascular, Inc. v. W.L. Gore & Assocs., No. CV-03-0597-PHX-MHM, 2009 U.S. Dist. LEXIS 31328, at *19–20 (D. Ariz. Mar. 31, 2009). *See also* Finisar Corp. v. DirecTV Grp., Inc., Civil Action No. 1:05-CV-264, 2006 U.S. Dist. LEXIS 101529, at *5 (E.D. Tex. Sep. 26, 2006) ("[T]he court granted future damages to Finisar by means of a compulsory license.").

future use of the patented technology during the life of the patents."[146] In *Hynix Semiconductor Inc. v. Rambus Inc.*, the court, echoing Judge Rader's concurrence in *Paice II*, confirmed that, "'ongoing royalty' is merely a nice way of saying 'compulsory license.'"[147]

In at least six cases, the district court expressly ordered the parties to negotiate a license for continued unenjoined infringement. For example, the court in *Carnegie Mellon University v. Marvell Technology Group, Ltd.* ordered the parties to "meet and confer to prepare a draft joint licensing agreement for ongoing royalties" following the denial of an injunction.[148] These orders are likely the result of the recommendation articulated by the Federal Circuit in *Paice II*:

> In most cases, where the district court determines that a permanent injunction is not warranted, the district court may wish to allow the parties to negotiate a license amongst themselves regarding future use of a patented invention before imposing an ongoing royalty.[149]

---

146. BASF Plant Sci., LP v. Commonwealth Sci. & Indus. Research Organisation, No. 2:17-CV-503-HCM, 2019 U.S. Dist. LEXIS 228305, at *64 (E.D. Va. Dec. 20, 2019); *see also* Centripetal Networks, Inc. v. Cisco Sys., 492 F. Supp. 3d 495, 606 (E.D. Va. 2020) (repeating same language); ResQNet.com, Inc. v. Lansa, Inc., 828 F. Supp. 2d 688, 692 (S.D.N.Y. 2011) ("The court . . . imposed a license at the same rate for future activity covered by the . . . patent.").

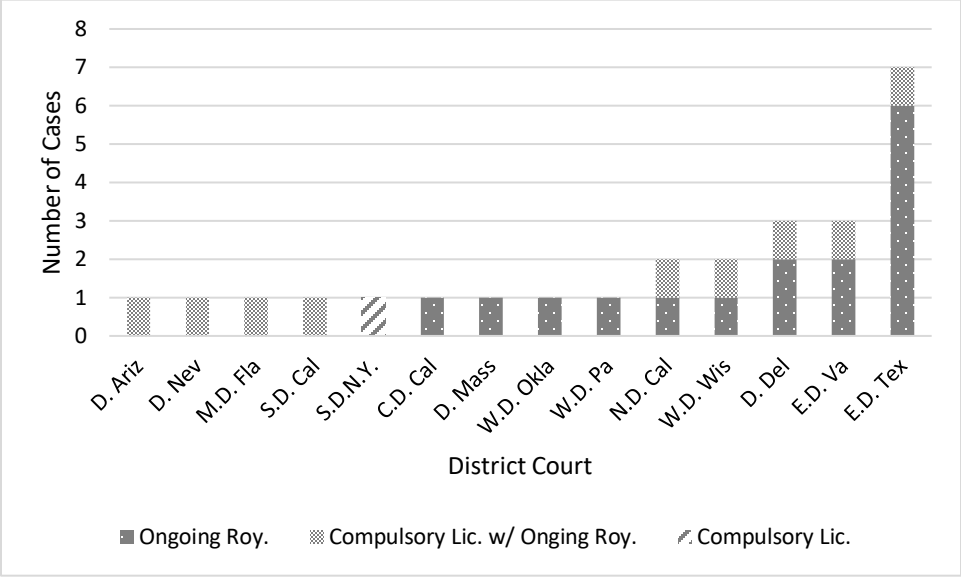
147. Hynix Semiconductor Inc. v. Rambus Inc., 609 F. Supp. 2d 951, 986–87 (N.D. Cal. 2009) (citing Paice LLC v. Toyota Motor Corp., 504 F.3d 1293, 1316 (Fed. Cir. 2007)).

148. Order at 1, Carnegie Mellon Univ. v. Marvell Tech. Grp., Ltd., Civil Action No. 09-290, 2013 U.S. Dist. LEXIS 58331 (W.D. Pa. Apr. 24, 2013); *see also* Server Tech., Inc. v. Am. Power Conversion Corp., No. 3:06-CV-00698-LRH-VPC, 2015 U.S. Dist. LEXIS 41987, at *43–44 (D. Nev. Mar. 31, 2015) ("The parties shall have thirty (30) days from entry of this order to prepare an appropriate compulsory license with an ongoing 15% royalty rate on sales of the AP7900 and AP8900 products from the date of judgment and submit the same for approval and signature of the court."); Fractus, S.A. v. Samsung Elecs. Co., No. 6:09-CV-203 PATENT, 2013 U.S. Dist. LEXIS 37275, at *13 (E.D. Tex. Mar. 15, 2013) ("The Court denied Fractus' request for a permanent injunction; however, the Court gave the parties an opportunity to negotiate a license before setting an ongoing royalty rate."); Douglas Dynamics, LLC v. Buyers Prods. Co., No. 09-cv-261-wmc, 2011 U.S. Dist. LEXIS 157349, at *17 (W.D. Wis. Feb. 25, 2011) ("The parties have until March 28, 2011, in which to reach a licensing agreement for defendant Buyers Products' use of plaintiff's U.S. Patents Nos. 5,353,530 and 6,944,978 or to file their separate positions for the court to use in assessing the appropriate reasonable ongoing royalty."); Order at 1, Hynix Semiconductor Inc. v. Rambus Inc., 609 F. Supp. 2d 951 (N.D. Cal. 2009) (No. 3901) ("[T]he court held a conference call with Rambus and Hynix to set guidelines with respect to negotiating a compulsory license for the use of Rambus's patents . . . The parties intend to meet on March 4 in Seoul, Korea to negotiate the terms of the compulsory license.").

149. *See* Paice LLC v. Toyota Motor Corp., 504 F.3d 1293, 1315 (Fed. Cir. 2007) (*Paice II*); *see also* Soverain Software LLC v. Newegg Inc., 836 F. Supp. 2d 462, 483 (E.D. Tex. 2010) ("[T]he Federal Circuit has encouraged parties to negotiate a license amongst themselves

Figure 4 below breaks down judicial characterizations of compensation for unenjoined infringement by judicial district.

Figure 4: Judicial Characterization by District Court (n=26)



As shown in Figure 4, among the five district courts that have denied two or more patent injunctions during the period studied, all five have referred, in different cases, to the authorization of a compulsory license in connection with the award of ongoing royalties for unenjoined infringement. This finding suggests that there is not a consistent view, even within federal judicial districts, of whether a compulsory license is granted when an ongoing royalty is awarded for unenjoined infringement.

4. Federal Circuit Statements Regarding Compulsory Licensing

Of seventy-seven Reviewed Cases, fifty-three (69%) were appealed to the Federal Circuit.[150] In twenty of those appealed cases, the Federal Circuit ruled

regarding the future use of a patented technology before imposing an ongoing royalty." (citing *Paice II* and Paice LLC v. Toyota Motors Corp., 609 F. Supp. 2d 620 (E.D. Tex. 2009)); Orion IP, LLC v. Mercedes-Benz USA, LLC, No. 6:05 CV 322, 2008 U.S. Dist. LEXIS 108683, at *12 (E.D. Tex. Mar. 28, 2008) (articulating the same standard).

150. The 69% appeal rate that we found is substantially lower than the 98% appeal rate found by Professors Holte and Seaman when reviewing Federal Circuit appeals of district court denials of patent injunctions between 2006 and 2013. *See* Holte & Seaman, *supra* note 23, at 179. It may be that parties have over time become less optimistic about overturning injunction denials at the Federal Circuit, leading to fewer appeals.

on grounds other than injunctive relief (e.g., validity, infringement, etc.). Six cases were dismissed by the district court before the Federal Circuit ruled (e.g., due to settlement by the parties). Of the remaining twenty-seven cases in which the Federal Circuit ruled on the district court's denial of a permanent injunction, the Federal Circuit affirmed the district court's ruling in twenty cases (74%) (five of which were decided by summary affirmance under Federal Circuit Rule 36[151]) and reversed the district court's ruling in seven cases (26%).[152]

The Federal Circuit equated an ongoing royalty to a compulsory license in three cases, *Whitserve, LLC v. Computer Packages, Inc.* and *Innogenetics, N.V. v. Abbott Laboratories*. Despite Judge Prost's early attempt in *Paice II* to disavow the granting of a compulsory license when an ongoing royalty is established,[153] other Federal Circuit judges seem less convinced. For example, in *Whitserve*, Judge O'Malley, joined, interestingly, by Judge Prost in the majority, stated that "[w]hile a trial court is not required to grant a compulsory license even when an injunction is denied, the court must adequately explain why it chooses to deny this alternative relief when it does so."[154] In *Innogenetics*, Judge Moore (joined by Judges Bryson and Clevenger) wrote that "future sales would be subject to the running royalty, a compulsory license. We remand to the district court to delineate the terms of the compulsory license . . . "[155] Finally, in *SRI International, Inc. v. Cisco Systems, Inc.*, in which the Federal Circuit affirmed the district court's award of an ongoing royalty in the absence of a request for an injunction by the patent holder, Judge Stoll (joined by Judges O'Malley and Lourie) explained that the district court "did not abuse its discretion in awarding 'a 3.5% compulsory license for all post-verdict sales.'"[156]

151. U.S. Ct. App. Fed. Cir., Rules of Practice 167–68 (Mar. 1, 2023), https://cafc.uscourts.gov/wp-content/uploads/RulesProceduresAndForms/FederalCircuitRules/FederalCircuitRulesofPractice.pdf/.

152. The 74% affirmance rate that we found differs substantially from the 53% affirmance rate found by Holte and Seaman for cases appealed between 2006 and 2013. *See* Holte & Seaman, *supra* note 23, at 187–88. It is possible that the lower rate of appeal during the period that we studied resulted in a higher rate of affirmance among cases that were appealed (i.e., if parties tended to appeal cases with a lower likelihood of reversal). *See supra* note 150, and accompanying text.

153. At least one other Federal Circuit Judge has followed Judge Prost's lead. Judge Gajarsa, citing Paice, disavowed the use of the term "compulsory license." Bard Peripheral Vascular, Inc. v. W.L. Gore & Assocs., 670 F.3d 1171, 1178 n.2 (Fed. Cir. 2012) ("As in Paice LLC v. Toyota Motor Corp., [w]e use the term ongoing royalty to distinguish this equitable remedy from a compulsory license.") (internal quotations marks omitted).

154. Whitserve, LLC v. Comput. Packages, Inc., 694 F.3d 10, 36 (Fed. Cir. 2012).

155. Innogenetics, N.V. v. Abbott Labs., 512 F.3d 1363, 1381 (Fed. Cir. 2008).

156. SRI Int'l, Inc. v. Cisco Sys., 930 F.3d 1295, 1311 (Fed. Cir. 2019) (emphasis added).

These results demonstrate that several Federal Circuit judges (Bryson, Clevenger, Lourie, Moore, O'Malley, Prost, Rader, and Stoll), including three former and current Chief Judges (Moore, Prost, and Rader) have either written or joined opinions referring to the granting of compulsory licenses upon the authorization of an ongoing royalty for unenjoined infringement.

It is also informative to compare the cases in which the Federal Circuit used compulsory licensing language with those in which district courts did so. One might predict that the Federal Circuit considered the question of compulsory licensing primarily when it was raised at the district court below. However, this was not the case. In our sample, there are twelve Federal Circuit cases in which future damages were awarded for unenjoined infringement. In five of these, the district court awarded an ongoing royalty *without* discussion of compulsory licensing, and in four, the district court awarded an ongoing royalty that it characterizes as compulsory licensing. The Federal Circuit took a different approach in each of these latter four cases, either (1) confirming that an ongoing royalty is compulsory licensing,[157] (2) referring only to an ongoing royalty,[158] (3) referring to neither an ongoing royalty nor compulsory licensing,[159] and (4) specifically indicating that an ongoing royalty is not a compulsory license.[160] What's more, in *Whitserve*, the Federal Circuit referred to compulsory licensing when the district discussed neither an ongoing royalty nor compulsory licensing.[161]

These somewhat confusing results suggest, at best, that the Federal Circuit lacks a clear view on whether a compulsory license is granted when an ongoing royalty is awarded for unenjoined infringement. We recommend below that this uncertainty be resolved with a clear acknowledgment that compulsory licenses are, indeed, being granted when ongoing royalties are awarded for unenjoined infringement.

C. DISCUSSION

The above findings indicate that some U.S. trial court judges across judicial districts interpret the award of ongoing royalties accompanying unenjoined infringement as conferring a compulsory license on the infringer. This view has been confirmed by the Federal Circuit in various cases, notwithstanding

157. *See* Innogenetics, N.V. v. Abbott Labs., 512 F.3d 1363, 1381 (Fed. Cir. 2008).

158. *See* Telcordia Techs., Inc. v. Cisco Sys., Inc., 592 F. Supp. 2d 727, 746, 748 (D. Del. 2009).

159. *See* generally Apple, Inc. v. Samsung Elecs. Co., No. 12-CV-00630-LHK, 2013 U.S. Dist. LEXIS 38682 (N.D. Cal. Mar. 19, 2013).

160. *See* Bard Peripheral Vascular, Inc. v. W.L. Gore & Assocs., Inc., No. CV-03-0597-PHX-MHM, 2009 WL 920300, at *5 (D. Ariz. Mar. 31, 2009).

161. *See* Whitserve, LLC v. Comput. Packages, Inc., 694 F.3d 10 (Fed. Cir. 2012).

Judge Prost's attempt in *Paice II* to distinguish an ongoing royalty from a compulsory license.

As a simple matter of logic, there is little doubt that a court's imposition of an ongoing royalty obligation on an unenjoined infringer can be anything other than a compulsory license of the infringed patents. As defined by the authorities cited in Section II.A.1, a license is a commitment not to sue a party for practicing a licensed right. And a "compulsory license" (notwithstanding the erroneous definition advanced in *Paice II*) is such a commitment that is imposed on the patent holder by a governmental body, including a court. While a small number of district courts that have declined to issue injunctions in patent cases have left open the door for the patent holder to bring successive damages suits against an unenjoined infringer,[162] courts that have awarded the patent holder an ongoing royalty as compensation for that infringement have effectively closed this door. For all practical purposes, there appears to be no practical way that a patent holder that has been awarded judicially determined compensation for unenjoined infringement can subsequently sue the infringer for infringement of the same patents by the same infringing products.

While some academic commentators have questioned the authority of district courts to authorize compulsory licenses, and even to award ongoing royalties (see Section II.B, *infra*), those objections have not swayed judicial practice in nearly two decades since the Supreme Court's eBay decision. Moreover, even before eBay, the Federal Circuit recognized that district courts denying injunctive relief for patent infringement effectively granted compulsory licenses to infringers.[163]

For these reasons, it is time to recognize that district courts awarding compensation for unenjoined infringement, whether in the form of ongoing royalties or lump sum payments, effectively grant compulsory licenses to the infringers, no matter what terminology these courts use to describe this practice.[164]

IV. COMING TO TERMS WITH UNENJOINED INFRINGEMENT AS COMPULSORY LICENSING

In this Part IV, we explore in greater depth some of the ramifications that arise from recognizing unenjoined infringement as compulsory licensing. In Sections IV.A and IV.B, we observe that characterizing unenjoined

162. We identified five such cases. *See supra* Section III.B.2, and accompanying discussion.

163. *See supra* notes 97–99 and accompanying discussion.

164. Professor Janicke appears to agree, writing that "courts have drifted into thinking a suitable remedy can be a judicially issued compulsory license that converts unlawful activities into licensed ones." Janicke, *supra* note 26, at 187.

infringement as compulsory licensing is consistent with expectations under the existing patent exhaustion and transfer doctrines, and that treating unenjoined infringement as anything other than compulsory licensing would produce anomalous and unintended results under those doctrines. In Section IV.C, we address and dispense with concerns that treating unenjoined infringement as compulsory licensing could run afoul of U.S. treaty obligations. In Section IV.D, we address concerns about the effect of compulsory licensing on future and existing exclusive patent licenses. And in Section IV.E, we observe that, even though district courts appear to be granting compulsory licenses to unenjoined infringers, little has been written about the terms or other commercial effects of those licenses. We seek to fill that gap.

A. UNENJOINED INFRINGEMENT AND PATENT EXHAUSTION

It is well-established that the sale of a patented article by an authorized licensee exhausts the patents embodied in that article so that the patent holder cannot pursue infringement claims or seek royalties from any downstream purchaser or user of that article.[165] The sale of a patented article by the holder of a compulsory license also exhausts the relevant patents and, by the same token, a sale by an unenjoined infringer must also exhaust those patents.

Any result to the contrary would be both inimical to the intent of *eBay* and to the patent exhaustion doctrine. For example, consider what would happen if unenjoined infringement did *not* constitute a license that exhausted the relevant patent rights. The unenjoined infringer could, in theory, manufacture a product covered by the patent and then sell it to a customer. The infringer would pay the patent holder the amount of the court-determined ongoing royalty with respect to that sale (usually denominated as a percentage of the product's net selling price). Yet if the manufacture and sale of the product by the unenjoined infringer were *not* deemed to be under "license," then the sale to the customer would not be authorized, and the customer would infringe the patent using the product that it purchased. And even though the unenjoined infringer paid the patent holder the court-determined royalty for that very sale, the patent holder could turn around and sue the customer for monetary damages and even seek an injunction against it.[166] If so, the patent holder

165. *See* Quanta Comput., Inc. v. LG Elecs., Inc., 553 U.S. 617, 625 (2008) ("The longstanding doctrine of patent exhaustion provides that the initial authorized sale of a patented item terminates all patent rights to that item.").

166. In many cases, a product manufacturer is contractually obligated to indemnify its customer against infringement claims. *See* CONTRERAS, IP TRANSACTIONS, *supra* note 71, at 282, 312. As a result, the patent holder's claim against the unenjoined infringer's customer would likely be covered by the unenjoined infringer itself, subjecting it to double payment for the same product, another unjust and illogical result.

could, in theory, recover twice for the sale of the same patented product—once from the unenjoined infringer and once from its customer.[167]

Such a result would subvert the intent of the ongoing royalty and unfairly reward the patent holder twice for the same infringing product—the very situation that the patent exhaustion doctrine seeks to avoid.[168] Exhaustion considerations thus offer yet another reason that unenjoined infringement, at least when it is accompanied by an ongoing royalty,[169] should be deemed to represent a compulsory patent license.

B. LICENSE AND PATENT TRANSFERS

A patent license is generally viewed as an encumbrance on the patent which, like a servitude on land, travels with the patent when it is transferred to a new owner, investing the new owner with both the benefit and the burden of that encumbrance.[170] Thus, when a patent is transferred, its new owner may not sue parties that were previously granted licenses to practice the patent, assuming that their licenses have not otherwise been terminated. By the same token, upon a transfer of the patent, licensees must pay royalties to the patent's new owner, and the prior owner loses its entitlement to those royalties.

The same must hold true in the case of unenjoined infringement. When an infringed patent is transferred to a new owner, the new owner must remain

167. Professor Gómez-Arostegui identified several nineteenth century cases holding that a patentee that collected a judgment against an infringer that placed infringing articles into the stream of commerce could not then bring suit against or enjoin downstream users of the infringing articles. Gómez-Arostegui, *Prospective Compensation*, *supra* note 10, at 1722–23. This principle has subsequently been adopted by the Federal Circuit in, e.g., Glenayre Elecs., Inc. v. Jackson, 443 F.3d 851 (Fed. Cir. 2006); Carborundum Co. v. Molten Metal Equip. Innovation, Inc., 72 F.3d 782, 881 (Fed. Cir. 1995); King Instruments Corp. v. Otari Corp., 814 F.2d 1560, 1564 (Fed. Cir. 1987); Stickle v. Heublein, Inc., 716 F.2d 1550, 1563 (Fed. Cir. 1983). *See also* Gómez-Arostegui & Bottomley, *supra* note 45, at n.146 (discussing Amstar Corp. v. Envirotech Corp., 823 F.2d 1538, 1548–49 (Fed. Cir. 1987)). By extension, Professor Gómez-Arostegui has argued that a court would be unlikely to allow a patentee to sue customers of an unenjoined infringer that is paying ongoing royalties, whether or not it is deemed to have received a compulsory license. *See* private email communications with Professor Gómez-Arostegui (Sept. 20, 2022) (on file with authors). This conclusion may be correct, though the question remains to be addressed by the courts.

168. Professor Janicke, recognizing the effect of the patent exhaustion doctrine, argues that customers of an unenjoined infringer would not be insulated from suit by the patent holder, which proves that a compulsory license is not granted by courts that authorize unenjoined infringement. Janicke, *supra* note 26, at 188.

169. The status of sales by an unenjoined infringer that does not compensate the patent holder for future infringement is less clear.

170. *See* Sanofi, S.A. v. Med-Tech Veterinarian Prods., 565 F. Supp. 931, 939 (D.N.J. 1983) ("[T]he purchaser of a patent takes subject to outstanding licenses").

bound by the prior owner's commitment not to sue the unenjoined infringer, and the unenjoined infringer must pay the ongoing royalty to the new owner.

If, on the other hand, an ongoing royalty awarded for unenjoined infringement does *not* give rise to a license—and simply represents a monetary damages award—the ongoing payment would, unless explicitly transferred along with the patent,[171] accrue to the original patent holder whether or not it retained the underlying patent. Accordingly, a transferee of the infringed patent, absent a separate assignment of the royalty stream, would not be entitled to receive the ongoing royalty paid by the infringer. Instead, it would, surprisingly, be entitled to sue the unenjoined infringer for both monetary damages and an injunction. In the meantime, the infringer would still be obligated to pay the ongoing royalty to the original patent holder. Clearly, this result would be both anomalous and unjustified, further demonstrating that an ongoing royalty awarded for unenjoined infringement can only indicate the issuance of a compulsory license.

C. U.S. TREATY COMPLIANCE

In its amicus brief submitted to the Supreme Court in *eBay*, the United States government cautioned the Court against "awarding monetary damages as a substitute for prospective injunctive relief" out of concern, in part, for U.S. treaty obligations "that preserve the patentee's right to exclude and that limit compulsory licensing."[172] A group of fifty-two law professors responded in an amicus brief that "TRIPS permits the United States to give its courts the power to deny injunctions in particular cases."[173] The Supreme Court did not directly address this concern in *eBay*, but the Federal Circuit's peculiar aversion to the term "compulsory licensing" in *Paice* might, at least in part, have been responsive to treaty compliance considerations.

The analysis of unenjoined infringement under the TRIPS Agreement is serpentine and lacks authoritative resolution. As noted in Section II.B.1.b above, Article 31 of the TRIPS Agreement permits a member state to order

171. Though one might expect a patent holder that is entitled to receive an ongoing royalty from an infringer to assign that right to any assignee of the underlying patent, this may not always happen, especially if the unenjoined infringer has not yet begun to pay royalties at the time of the patent assignment. For example, if the patent holder assigns a large portfolio of patents, including one subject to a compulsory license, it may inadvertently neglect to assign associated contractual rights to the assignee.

172. Brief for the United States as Amicus Curiae Supporting the Respondent at 18, eBay Inc. v. MercExchange LLC, 547 U.S. 388 (2006) (05-130) (citing the TRIPS Agreement, *supra* note 6, arts. 28, 31, 33, and the U.S.-Australia Free Trade Agreement, May 18, 2004, Heins No. KAV 622, art. 17.9, ¶ 7).

173. Amicus Brief of Professors, *supra* note 109, at 10–11.

compulsory licensing of patents under particular circumstances.[174] However, compulsory licensing as contemplated by TRIPS includes several requirements and limitations, including the following: the licensee must first have made efforts to obtain a license from the patent holder on reasonable commercial terms and conditions, except in case of a national emergency;[175] the license should be authorized predominantly for the supply of the domestic market;[176] the licensee may not grant sublicenses;[177] the license should terminate when the circumstances that led to it cease to exist and are unlikely to recur;[178] and, in the case of semiconductor technology, use may only be for public noncommercial purposes or to remedy anticompetitive practices.[179] Given these requirements, many of which are not met in the ordinary context of unenjoined infringement, commentators have questioned whether compulsory licenses for unenjoined infringement would comply with the compulsory licensing provisions of the TRIPS Agreement.[180]

This being said, other provisions of TRIPS appear to offer more hope. Article 44(1), concerning injunctions, provides that "the judicial authorities [of a member state] shall have the authority to order a party to desist from an infringement," but does not mandate that injunctions be issued whenever patent infringement is found.[181] Thus, the decisions of U.S. courts not to grant injunctions in certain cases of infringement should not violate Article 44(1).

Moreover, Article 44(2) states that remedies for the use of a patented technology by a government or a third party authorized by a government may be limited to monetary compensation only if the remedies comply with the

174. *See supra* note 82–83, and accompanying text.
175. TRIPS Agreement, *supra* note 6, art. 31(b).
176. *Id.* art. 31(f).
177. *Id.* art. 31(e).
178. *Id.* art. 31(g).
179. *Id.* art. 31(c).
180. Graeme B. Dinwoodie & Rochelle C. Dreyfuss, *Injunctive Relief in Patent Law under TRIPS*, *in* INJUNCTIONS IN PATENT LAW: TRANSATLANTIC DIALOGUES ON FLEXIBILITY AND TAILORING 5, 13–14 (Jorge L. Contreras & Martin Husovec eds., 2022); Cotropia, *supra* note 10, at 576.
181. TRIPS Agreement, *supra* note 6, art. 44(1). This interpretation was confirmed by the WTO. WORLD TRADE ORG., PANEL REPORT, CHINA – MEASURES AFFECTING THE PROTECTION AND ENFORCEMENT OF INTELLECTUAL PROPERTY RIGHTS, at ¶ 7.326, WTO Doc. WT/DS362/R (adopted Jan. 26, 2009) ("The obligation is to 'have' authority not an obligation to 'exercise' authority") (discussed in Dinwoodie & Dreyfuss, *supra* note 180, at 10); GERVAIS, *supra* note 10, at 447, 453 ("[S]hall have the authority" requires only "the power to order the measures specified").

provisions of Article 31.[182] This requirement could be interpreted as bringing the analysis full circle. While under Article 44(1) injunctions need not be issued by courts, the substitution of injunctive relief with monetary compensation (i.e., an ongoing royalty), at least for patents, requires the same procedural hurdles as compulsory patent licensing under Article 31.

Yet Article 30 of TRIPS permits member states to "provide limited exceptions to the exclusive rights conferred by a patent, provided that such exceptions do not unreasonably conflict with a normal exploitation of the patent and do not unreasonably prejudice the legitimate interests of the patent owner, taking account of the legitimate interests of third parties."[183] Christopher Cotropia argues that the four factors considered by U.S. courts when denying injunctive relief under *eBay* maps directly onto the requirements of Article 30, thereby authorizing this practice.[184]

Whatever the rationale, most commentators who have considered the issue have concluded that unenjoined infringement coupled with an ongoing royalty—whether or not labeled compulsory licensing—complies with U.S. obligations under the TRIPS Agreement.[185]

D. EFFECT ON EXCLUSIVE LICENSEES

In *Paice*, the patent holder argued that the court should not grant a compulsory license to Toyota, the infringer, because doing so would impair its ability to grant an exclusive license under the infringed patent to another party in the future.[186] That is, if a compulsory license has been granted, then while it remains in effect, it is impossible for the patent holder to grant another party a truly exclusive license. And because exclusive patent licenses often command higher royalties than nonexclusive licenses,[187] the victorious patent holder is

182. TRIPS Agreement, *supra* note 6, art. 44(2). *See* GERVAIS, *supra* note 10, at 452 (noting that the first sentence of art. 44(2) is intended to apply to patents). *See also* Dinwoodie & Dreyfuss, *supra* note 180, at 13; Cotropia, *supra* note 10, at 580.

183. TRIPS Agreement, *supra* note 6, art. 30.

184. Cotropia, *supra* note 10, at 576–79. *But see* GERVAIS, *supra* note 10, at 381 (reasoning that specific exceptions covered elsewhere in TRIPS, such as compulsory licensing under Article 31, should not be interpreted as being within the scope of Article 30).

185. *See* Dinwoodie & Dreyfuss, *supra* note 180, at 15 ("[S]everal scholars have explored the issue and concluded that eBay is likely consistent with TRIPS"), n. 52 (collecting sources); Siebrasse et al., *supra* note 47, at 143; Cotropia, *supra* note 10, at 581 ("In the end, it is not so much *whether* the application of *eBay* to deny an injunction complies with TRIPS, as *how* exactly the decision complies with TRIPS") (emphasis in original).

186. *Paice* CAFC Brief, *supra* note 27, at *80 ("Toyota now has won the privilege of being licensed under the '970 patent simply by losing a lawsuit and, as a result, Paice can never offer an exclusive license to this patent to other interested parties.").

187. *See* CONTRERAS, IP TRANSACTIONS, *supra* note 71, at 176 (discussing premium payable for exclusive license rights).

unfairly injured by the grant of a compulsory license to the infringer. Conversely, Professor Janicke argues that a patent holder that has *previously* granted an exclusive license under the infringed patent may be contractually barred from granting a conflicting license to the unenjoined infringer, even if ordered to do so by a court.[188]

Both implications of compulsory licenses—their interference with *future* exclusive licenses and their derogation from *prior* exclusive licenses—highlight the power of the compulsory license. These effects are not newly discovered in the context of unenjoined infringement. Rather, they are longstanding objections to the issuance of compulsory licenses of every kind. The owner of a pharmaceutical patent may be required to license it to a local generic manufacturer, notwithstanding its prior exclusive license to a multinational drug company.[189] The owner of a patented semiconductor technology developed with federal funding may be required to license it to a second manufacturer if its exclusive licensee is unable to meet the demand for products in the United States.[190] In all of these cases, the patent owner would prefer not to grant the compulsory license, which is the very reason that it is compulsory in the first place—an overriding governmental policy or concern dictates that the patent be made available in a manner beyond that desired by the patent holder.

Compulsory licenses granted for unenjoined infringement are no different. Courts may deny injunctive relief in patent cases only after assessing the four factors laid out in the Supreme Court's *eBay* decision. Courts should not take this decision lightly, and the relatively low number of such compulsory licenses granted in the two decades since *eBay* suggest that they do not. But so long as the *eBay* factors weigh in favor of denying an injunction, the financial impact on the patent holder should be addressed through the magnitude of the court-awarded ongoing royalty and not by denying that a compulsory license has been granted.

E. TERMS OF THE COMPULSORY LICENSE

The granting of a compulsory license for unenjoined infringement begs the question: what are the terms of that compulsory license? A license is an

188. Janicke, *supra* note 26, at 188 ("If an exclusive license is already outstanding, the patent owner may not issue a conflicting nonexclusive license to someone else.").

189. *See supra* note 2, and accompanying text (discussing compulsory licensing of essential medicines).

190. *See supra* notes 91–92, and accompanying text (discussing march-in rights under the Bayh-Dole Act).

authorization to take certain actions under an intellectual property right. But which actions, for how long, and under what conditions?[191]

Perhaps due to the Federal Circuit's reluctance in *Paice II* to call this grant of authority a "license," courts and commentators have largely focused on only one admittedly important feature of the license: the royalty rate.[192] Indeed, by referring to the license merely as an "ongoing royalty," the Federal Circuit virtually guaranteed that the only term to receive substantial attention would be the royalty rate. Yet intellectual property licenses have numerous other terms that must be specified in addition to the royalty rate. Licenses have a scope, a duration, a field of use, and other provisions that define the ongoing relationship between the licensor and the licensee. Moreover, they often specify procedures for payment, audit, challenge, and dispute resolution should one party fail to live up to its obligations.

U.S. courts that granted compulsory patent licenses in the context of historical antitrust disputes took care to specify at least some terms of those licenses beyond the royalty rate.[193] Courts authorizing unenjoined infringement under a compulsory license can and should do the same.[194] If nothing else, specifying the scope of the compulsory license gives the court some control over its effective implementation. As observed by the Federal Circuit in *Innogenetics, N.V. v. Abbott Laboratories*, "[a]n injunction delineating the terms of the compulsory license would permit the court to retain jurisdiction to ensure the terms of the compulsory license are complied with."[195]

---

191. The inquiry in this Section IV.E echoes that undertaken by John Golden in his analysis of the terms and precise scope of patent injunctions. John Golden, *Injunctions as More (or Less) than "Off Switches:" Patent-Infringement Injunctions' Scope*, 90 TEX. L. REV. 1399 (2012).

192. Determining the ongoing royalty rate in unenjoined infringement cases has attracted significant attention in the academic literature. *See* Shore, *supra* note 2, at 68; Lemley, *supra* note 44, at Section IV; Seaman, *Ongoing Royalties, supra* note 53, at 220–23; Carlton, *supra* note 25, at 565.

193. *See* Contreras, *Brief History, supra* note 95, at 74 (discussing terms on which licenses were granted); Delrahim, *supra* note 7, at 12–15 (discussing licensing terms).

194. The patent holder in *Paice* complained that "the remedy fashioned in this case is impermissibly incomplete. The district court imposed a license that leaves substantial terms open to future dispute and litigation." *Paice* CAFC Brief, *supra* note 27, at *79. Professor Janicke argues that the failure of courts authorizing unenjoined infringement to specify these additional terms indicates that they are not actually granting compulsory licenses. Janicke, *supra* note 26, at 187–88. We disagree, finding instead that these courts are simply granting compulsory licenses that suffer from a lack of detail. This lack, however, does not make them into something less than licenses.

195. Innogenetics, N.V. v. Abbott Laboratories, 512 F.3d 1363, 1381 n.9 (Fed. Cir. 2008).

As noted in Part II,[196] in *Paice II* the Federal Circuit encouraged district courts to permit parties to negotiate the terms of their own licenses for unenjoined infringement before determining an ongoing royalty. As a result, several district courts have ordered parties to negotiate a licensing agreement for the period of unenjoined infringement after an injunction was denied.[197] In these cases, a written license agreement would presumably emerge from the parties' negotiation, specifying the licensing details normally associated with a license of intellectual property. This is the ideal scenario, in which all relevant licensing terms are specified by the parties after being requested by the court to do so. However, if the parties are unable to reach such an agreement, the court itself may need to step in with licensing terms in addition to the ongoing royalty.[198]

In this Section IV.E, we discuss some of the legal terms beyond the royalty rate that should be defined in any compulsory patent license and urge courts granting such licenses to consider including such terms in their orders imposing compulsory licenses for unenjoined infringement, or even appending a full licensing agreement to such orders.[199]

1. Licensed Rights

In commercial licensing agreements, significant negotiation occurs over the precise intellectual property rights that will be licensed, whether a single patent, a patent "family" sharing the same priority date, or a portfolio of patents relating to a particular product or technology.[200] In licensing

196. *See supra* note 149, and accompanying discussion.

197. *See, e.g.*, Order at 1, Carnegie Mellon Univ. v. Marvell Tech. Grp., Ltd., Civil Action No. 09-290 (W.D. Pa. Apr. 24, 2013) (No. 865) ("IT IS HEREBY ORDERED that the parties, through counsel, shall meet and confer to prepare a draft joint licensing agreement for ongoing royalties."); Douglas Dynamics, LLC v. Buyers Prods. Co., No. 09-cv-261-wmc, 2011 U.S. Dist. LEXIS 157349, at *17 (W.D. Wis. Feb. 25, 2011) ("The parties have until March 28, 2011, in which to reach a licensing agreement for defendant Buyers Products' use of plaintiff's U.S. Patents Nos. 5,353,530 and 6,944,978 or to file their separate positions for the court to use in assessing the appropriate reasonable ongoing royalty."); Telcordia Techs., Inc. v. Cisco Sys., Inc., 612 F.3d 1365, 1379 (Fed. Cir. 2010) ("This court also remands to allow the parties to negotiate the terms of the royalty."); Hynix Semiconductor Inc. v. Rambus Inc., 609 F. Supp. 2d 951, 986 (N.D. Cal. 2009) ("[T]he best practice is to order the parties to negotiate the terms of an ongoing royalty for the court to impose.").

198. With respect to some contractual terms, the common law may supply implied terms where the parties fail to specify them. *See* Restatement (Second) of Contracts § 204.

199. For example, the district court supplied a form of license agreement for use by the parties, in Amended Final Judgment and Injunction, TCL Communication Technology Holdings, Ltd v. Telefonaktiebolaget LM Ericsson, Case No. 8:14-CV-00341 JVS-DFMx (C.D. Cal., Dec. 22, 2017).

200. *See* CONTRERAS, IP TRANSACTIONS, *supra* note 71, at 129–36. Note that in settlement agreements, the licensed rights seldom include trade secrets or know-how that are not yet

agreements that are entered into when settling litigation, the licensed rights are often confined to the patents at suit, but parties may be well-advised to include other members of the same patent family and additional patents that cover the same product to avoid further litigation.[201] The rights licensed under a compulsory license for unenjoined infringement should also be carefully delineated to avoid later disputes regarding the products and features that are covered by the license.[202]

2. Duration of License

Licensing agreements can have durations of any length up to the full legal term of the licensed rights. In many cases, patent license agreements run concurrently with the term of the licensed patents and terminate upon the expiration of the last-to-expire patent.[203] This is also the case when a licensing agreement states no defined term.[204] Yet it is also not uncommon for patent licenses to have fixed terms that expire after a period of years or upon the occurrence of a specified event.

Beyond the commercial factors at play in a negotiated licensing agreement, a compulsory license for unenjoined infringement could take into account the circumstances that led to the denial of an injunction in the first place. That is, an injunction may have been denied to the patent holder because, at the time it initiated suit, it did not practice the infringed patent, leading the court to find that the *eBay* factors disfavored the granting of an injunction. Yet a few years later, the patent holder might have begun to practice the patent and sell patented products. Were the court to revisit the request for an injunction at that point (or if the patent holder were free to bring a subsequent suit seeking an injunction), the court might decide that an injunction was warranted. Yet, if at the time the first injunction was denied the court issued a compulsory license for the duration of the infringed patents, the patent holder would have no opportunity to petition the court for an injunction after the situation (and the balance of the *eBay* factors) had changed.[205]

In most of the Reviewed Cases in which the district court specified the term of the compulsory license or ongoing royalty, the term ended upon

known by the infringer, as the patent holder is seldom willing to assist the infringer in improving its products.

201. *Id.* at 94, 360 (discussing cases in which rights licensed under settlement agreements were narrower than intended by at least one party).

202. Professor Janicke notes that "[a]s far as we know from the court decisions to date, this subject has been wholly unexplored." Janicke, *supra* note 26, at 188.

203. *See* CONTRERAS, IP TRANSACTIONS, *supra* note 71, at 364–65.

204. *See id.* at 364.

205. The authors thank Mark Lemley for this observation.

expiration of the last licensed patent.[206] Nevertheless, at least one decision that we reviewed specified a license term of less than the full duration of the licensed patents based on an analysis of comparable licensing agreements in the industry.[207] For this reason, it is important that the court authorizing a compulsory license state the term of that license and whether it will expire after a particular period, thus permitting the patent holder to renegotiate the terms of the license or bring suit, and perhaps seek an injunction, again.

3. License Scope and Field of Use

Licenses frequently specify the types of products and services that the licensee is permitted to produce and offer under the licensed rights. This "field of use" is often carefully delimited and heavily negotiated.[208] The scope of the licensee's rights under a compulsory license must also be carefully considered. For example, the agreement should state whether the licensee may practice the licensed patents only in connection with the manufacture and sale of the types of products that it made at the time a claim for infringement was made, at the time the license was granted, or at points in the future. To what degree may the licensee introduce routine, or even extraordinary, product improvements and still retain its license? What if the licensee is acquired by a much larger company with a broad range of product offerings beyond those offered by the original licensee? Does the license cover all such product expansions?

Only a few cases involving unenjoined infringement have addressed this important issue, mostly to clarify the scope of products as to which the unenjoined infringer must pay an ongoing royalty. For example, in *Fractus, S.A. v. Samsung Electronics Co.*, the district court states that ongoing royalties must be paid with respect to any products that are not "colorably different" than the products accused of infringement.[209] Likewise, another court makes it clear

206. *See* XY, LLC v. Trans Ova Genetics, LC, Civil Action No. 13-cv-0876-WJM-NYW, 2020 U.S. Dist. LEXIS 78716, at *37 (D. Colo. May 5, 2020) ("[A]ll ongoing royalty obligations end with the expiration of the . . . patent."); Tex. Advanced Optoelectronic Sols., Inc. v. Intersil Corp., No. 4:08-CV-451, 2016 U.S. Dist. LEXIS 53948, at *17 (E.D. Tex. Apr. 22, 2016) ("ORDERED to negotiate a royalty rate to address any future harm to the Plaintiff for the remaining life of the '981 patent. Such supplemental damages shall be for sales in the United States of products found to infringe the Plaintiff's patent from March 2014 until the expiration of the patent.").

207. Centripetal Networks, Inc. v. Cisco Sys., 492 F. Supp. 3d 495, 607 (E.D. Va. 2020) (setting six-year term for license, notwithstanding three-year term found in one comparable license).

208. *See* CONTRERAS, IP TRANSACTIONS, *supra* note 71, at 143–47 (discussing the need to carefully describe the range of licensed products and fields of use authorized under a licensing agreement).

209. *See* Fractus, S.A. v. Samsung Elecs. Co., No. 6:09-CV-203 PATENT, 2013 U.S. Dist. LEXIS 37275, at *15 (E.D. Tex. Mar. 15, 2013). The language of "colorable differences" is

that the licensee's mere alternation of the "nomenclature" of its infringing products (i.e., changing product or model names) will not relieve it of the obligation to pay ongoing royalties.[210] These judicial statements are important because they establish the scope of the licensee's field of use, and all courts issuing compulsory licenses for unenjoined infringement should more clearly identify the scope of the license granted.[211]

4. Territory

Geographic or territorial reach is also relevant in defining the scope of a license. In some industries, commercial licenses are worldwide in scope.[212] Worldwide licenses may even be negotiated in the context of litigation settlements, where the patents at issue are, by definition, limited to the jurisdiction in which litigation is being conducted, but the parties wish to establish global "peace."

This expansive reach, however, can be problematic in licenses granted by a court. As one district court explains, "the dominant practice in the industry is to license on the basis of worldwide sales, in part to avoid the need to determine which products enter which countries . . . however, the court may not impose a royalty on such a basis because the court's powers do not extend beyond the United States."[213] Thus, the compulsory license granted by a U.S. court for unenjoined infringement could be limited solely to U.S. patents (contrary, perhaps, to the expectations of the parties). If so, the court may wish to encourage the parties to agree separately on how to handle non-U.S. patents, or to voluntarily include them within the scope of the compulsory license and ongoing royalty awarded by the U.S. court. At a minimum, the geographic scope of any license granted should be specified clearly by the court to avoid later disputes.

---

not infrequently found in orders for injunctive relief in patent cases. *See* John Golden, Injunctions as *More (or Less) than "Off Switches": Patent-Infringement Injunctions' Scope*, 90 TEX. L. REV. 1399, 1404 (2012) (describing "Colorable-differences do-not-infringe injunctions").

210. Centripetal Networks, Inc. v. Cisco Sys., 492 F. Supp. 3d 495, 607 (E.D. Va. 2020).

211. Professor Janicke observed that "[i]n a real license, the scope of permission is invariably set out in the agreement, whether it is for all products covered by the patent's claims or only certain configurations, characteristics, or markets. In court-ordered situations to date, little address has been given to this important subject." Janicke, *supra* note 26, at 188.

212. *See* CONTRERAS, IP TRANSACTIONS, *supra* note 71, at 147–48.

213. Hynix Semiconductor Inc. v. Rambus Inc., 609 F. Supp. 2d 951, 987, n.30 (N.D. Cal. 2009); *see also* Carnegie Mellon Univ. v. Marvell Tech. Grp., Ltd., 807 F.3d 1283, 1306 (Fed. Cir. 2015) (the scope of a compulsory license should only apply to the patented products that are sold within the United States). *But see* WesternGeco LLC v. ION Geophysical Corp., 138 S. Ct. 2129, 2141–42 (2018) (finding a defendant can be liable for patent infringement under 35 U.S.C. § 271(f)(2) if it ships components of a patented invention overseas for assembly).

5. Payment Terms

Given the importance of the ongoing royalty to the authorization of unenjoined infringement, some courts have included express payment and other financial terms in their orders establishing an ongoing royalty or compulsory license. For example, in *Finisar Corp. v. DirecTV Group, Inc.*, the court provides that royalties must be paid quarterly and accompanied by a statement of accounting; payments not made within fourteen days of the due date will accrue interest at a rate of 10% compounded monthly, and the patent holder has the right to conduct an audit of the licensee's books to verify compliance.[214] Few other judicial royalty orders are this detailed, leaving many of these procedural elements to further agreement (or disagreement) of the parties.

6. Other Terms

A multiplicity of other commercial terms are generally included in patent licensing agreements, and many of these would be useful to specify in compulsory licenses accompanying unenjoined infringement. For example:

- Can the license be terminated by the patent holder for the licensee's non-payment or other breach, or is it effectively irrevocable during its term?
- Is the license transferable, e.g., in the event of a sale or merger of the licensee?
- May the licensee grant sublicenses?[215]
- Is the royalty adjusted, for example, if one or more licensed patents are invalidated or expire?
- Is the licensee permitted to challenge the validity of the licensed patents?[216]

214. Finisar Corp. v. DirecTV Grp., Inc., Civil Action No. 1:05-CV-264, 2006 U.S. Dist. LEXIS 76380, at *5 (E.D. Tex. July 7, 2006).

215. Compulsory licenses granted under Art. 31 of the TRIPS Agreement may not be sublicensed. TRIPS Agreement, *supra* note 6, art. 31(e).

216. Though patent licensees generally retain the right to challenge licensed patents under the Supreme Court's decision in Lear, Inc. v. Adkins, 395 U.S. 653 (1969), prohibitions on challenge have been upheld in the context of settlement agreements. *See* Flex-Foot, Inc. v. CRP, Inc., 238 F.3d 1362, 1368 (Fed. Cir. 2001) ("[W]hile the federal patent laws favor full and free competition in the use of ideas in the public domain over the technical requirements of contract doctrine, settlement of litigation is more strongly favored by the law."). An unenjoined infringer who has litigated (and lost) the issue of patent validity in the court permitting its unenjoined infringement, however, may be limited by res judicata from pursuing such a claim.

- Must the licensee mark its products with the licensed patent number(s)?[217]
- Must the licensee grant any rights to the licensor in improvements to the licensed technology?

We suggest that courts imposing compulsory licenses in the context of unenjoined infringement address each of these issues in the relevant judicial order. Failing to do so can lead to ambiguity and disagreements as a multi-year licensing relationship proceeds.

V. CONCLUSIONS

Contrary to the position of some U.S. government officials and the dicta of some courts, our findings reveal that numerous district court and Federal Circuit judges have expressly acknowledged that they are granting compulsory licenses when authorizing unenjoined infringement combined with ongoing royalties. Failing to recognize that a compulsory license has been granted in this context not only defies logic, but also introduces potential issues under the doctrines of patent exhaustion and transfer.[218]

Nevertheless, some district courts, relying on selected Federal Circuit statements, continue to insist that ordering an "ongoing royalty" is different than granting a "compulsory license." It is not; and the time has come for the courts—either the Federal Circuit or the Supreme Court—to acknowledge this fact explicitly.[219] Specifically, we call on the Federal Circuit or Supreme Court to acknowledge that a district court that declines to enjoin the infringement of a valid and enforceable patent, and concurrently orders the infringer to compensate the patent holder for acts of future unenjoined infringement, has authorized a compulsory license of the patent.[220] The Federal Circuit should

217. This question was raised by the patent holder in *Paice*. *See* Paice CAFC Brief, *supra* note 27, at *79 ("[T]he compulsory license is wholly silent as to patent marking. Will Paice now suffer loss of pre-suit damages against other auto makers as the result of Toyota's unmarked and yet 'licensed' sales?"). *See also* Arctic Cat Inc. v. Bombardier Recreational Prods. Inc., 876 F.3d 1350, 1366 (Fed. Cir. 2017) ("A patentee's licensees must also comply with § 287, because the statute extends to "persons making or selling any patented article for or under [the patentee]."") (discussed in Bernard Cryan, Not All Patent Licensees Are the Same: 35 U.S.C. Sec. 287 Should Not Require Marking by Licensees That Deny Infringement, 101 J. Pat. & Trademark Off. Soc'y 531 (2021)).

218. *See supra* Sections IV.A–B.

219. *See also* Gómez-Arostegui & Bottomley, *supra* note 45, at 443 ("[T]he [Supreme] Court must squarely address whether federal courts actually have the power to impose an ongoing royalty in lieu of a final injunction in patent cases.").

220. As noted above, some commentators have argued that federal district courts are not authorized under the current statutory framework to grant compulsory licenses or to order an infringer to pay ongoing royalties. *See supra* notes 44–46, and accompanying text. If they are

also expressly overrule the false distinction between ongoing royalties and compulsory licensing that was established in *Paice II*.[221]

Taking these steps would have several benefits. First, it would eliminate the courts' embarrassing reliance on a definition of compulsory licensing that erroneously equates it with public licensing as authorized under the Copyright Act.[222] If nothing else, such an acknowledgment would improve the doctrinal integrity of a key principle underlying judicial orders that have significant commercial and market impact.

Second, expressly recognizing the judicial authorization of compulsory licenses could encourage courts to focus greater attention on the non-royalty terms of such licenses. As discussed in Section IV.E, key terms such as license scope, field of use, and duration are typically omitted from judicial orders pertaining to unenjoined infringement, as courts focus largely on the determination of an "ongoing royalty" to the exclusion of other licensing terms. The recognition that a court is granting a compulsory license, rather than merely setting an ongoing royalty rate, would place the determination of these terms squarely within the scope of the court's order.

Finally, an acknowledgment that U.S. district courts are issuing compulsory patent licenses in significant numbers should inform U.S. foreign policy regarding compulsory licensing by other countries. As noted in the Introduction, the U.S. has consistently adopted an aggressive stance toward countries that have proposed to grant, or actually granted, compulsory licenses of patents held by U.S. entities. Yet if the characterization of unenjoined infringement as compulsory licensing is accurate, the U.S. federal courts could be viewed as among the most prolific issuers of compulsory patent licenses in the world—a result that would be starkly at odds with the public positions taken by the U.S. government. Greater self-awareness by U.S. government agencies of the prevalence of compulsory licensing within the United States could result in a more nuanced approach to such proposals by other countries.[223]

---

correct, then Congress should amend the Patent Act to clarify that such forward-looking remedies are, in fact, permitted.

221. *See supra* notes 110–112, and accompanying text.

222. *See supra* note 120, and accompanying text; *see also supra* Section II.B.1.d.

223. *See* Cotropia, *supra* note 10, at 582–83 ("The United States' objections to other government allowances of unauthorized [patent] use are more likely to look hypocritical and hold less force before the WTO after *eBay*."). Nevertheless, as Fabian Gonell has pointed out the authorization by U.S. courts of unenjoined infringement, which this article classifies as compulsory licensing, is granted only when the patentee itself seeks injunctive relief against an infringer—the authorization is not generated *sua sponte* by the court or another governmental body, but as part of a remedial adjudication initiated by the patent holder. In this sense, the

circumstances surrounding U.S. compulsory licenses and typical compulsory licenses granted at the initiative of foreign governments (*see supra* notes 83–84) may be different, potentially justifying different responses by the U.S. government. *See* @Fabian_Gonell, TWITTER (May 31, 2022, 9:56 AM), https://twitter.com/Fabian_Gonell/status/1531681046353235968.

ADDRESSING PERSONAL DATA COLLECTION AS UNFAIR METHODS OF COMPETITION

Maurice E. Stucke[†]

ABSTRACT

Enforcers, policymakers, scholars, and the public are concerned about Google, Apple, Meta, Amazon, and Microsoft and their influence. That influence comes in part from personal data. The public sentiment is that a few companies, in possessing so much data, possess too much power. Something is amiss. Cutting across political lines, many Americans think Big Tech's economic power is a problem facing the U.S. economy. So how can one protect one's privacy in the digital economy? Over the past few decades, the Federal Trade Commission has prosecuted privacy and data protection offenses under its power to curb "unfair and deceptive acts and practices" under § 5 of the FTC Act. Some urge the agency to go further and use its authority under § 5's "unfairness" prong to promulgate a "Data Minimization Rule." While that remains an option, that rulemaking path has several limitations. Instead, this Article takes a different approach. This Article urges the FTC to challenge certain privacy-related competition concerns as "unfair methods of competition" under the FTC Act. This Article also addresses one key source of many problems in the surveillance economy—namely, behavioral advertising.

As this Article concludes, the FTC cannot repair the surveillance economy with its authority under the FTC Act. America still needs an omnibus privacy framework. But the FTC can help close the regulatory gap by exercising the authority that Congress intended it to exercise to help rein in the data-opolies.

TABLE OF CONTENTS

DOI: https://doi.org/10.15779/Z38Q52FD98

† Douglas A. Blaze Distinguished Professor of Law, University of Tennessee College of Law. The authors would like to thank the Omidyar Network for its research grant.

I. INTRODUCTION

> Consumer privacy has become a consumer crisis.[1]

Enforcers, policymakers, scholars, and the public are all concerned about the outsized influence of Google, Apple, Facebook, Amazon, and Microsoft. That influence comes partly from their vast control over personal data.[2] These companies are "data-opolies" in that they are powerful firms that control a lot of personal data. The data comes from their vital ecosystems of interlocking online platforms and services, which attract: users; sellers; advertisers; website publishers; and software, app, and accessory developers.[3]

The public sentiment is that a few companies, in possessing so much data, have too much power. Something is amiss. In a 2020 survey, most Americans were concerned about the amount of data online platforms store about them (85%) and that platforms were collecting and holding this data about consumers to build more comprehensive consumer profiles (81%).[4]

But data is only part of the story. Data-opolies use the data to find better ways to addict us and predict and manipulate our behavior.

Cutting across political lines, many Americans (65%) think Big Tech's economic power is a problem facing the U.S. economy.[5] While much has been

---

1. Letter from U.S. Sen. Richard Blumenthal et al. to FTC Chair Lina Khan (Sept. 20, 2021), https://www.blumenthal.senate.gov/imo/media/doc/2021.09.20%20-%20FTC%20-%20Privacy%20Rulemaking.pdf.

2. Personal data, as used herein, means "any information relating to an identified or identifiable individual (data subject)." *See* Secretariat of the Organization for Economic Co-operation and Development (OECD), *Consumer Data Rights and Competition*, Background Note ¶ 16, DAF/COMP(2020)1 (Apr. 29, 2020), https://one.oecd.org/document/DAF/COMP(2020)1/en/pdf [hereinafter OECD Consumer Data Rights and Competition].

3. HOUSE OF COMMONS, STANDING COMM. ACCESS TO INFORMATION, PRIVACY AND ETHICS, DEMOCRACY UNDER THREAT: RISKS AND SOLUTIONS IN THE ERA OF DISINFORMATION AND DATA MONOPOLY (Dec. 2018), https://www.ourcommons.ca/Content/Committee/421/ETHI/Reports/RP10242267/ethirp17/ethirp17-e.pdf; Maurice E. Stucke, *Should We Be Concerned About Data-opolies?*, 2 GEO. L. TECH. REV. 275 (2018); Maurice E. Stucke, *Here Are All the Reasons It's a Bad Idea to Let a Few Tech Companies Monopolize Our Data*, HARV. BUS. REV. (Mar. 27, 2018), https://hbr.org/2018/03/here-are-all-the-reasons-its-a-bad-idea-to-let-a-few-tech-companies-monopolize-our-data.

4. Press Release, Consumer Reports, Consumer Reports Survey Finds That Most Americans Support Government Regulation of Online Platforms (Sept. 24, 2020), https://advocacy.consumerreports.org/press_release/consumer-reports-survey-finds-that-most-americans-support-government-regulation-of-online-platforms/.

5. *See, e.g.*, European Commission's proposed Digital Markets Act, https://ec.europa.eu/info/strategy/priorities-2019-2024/europe-fit-digital-age/digital-markets-act-ensuring-fair-and-open-digital-markets_en; Consumer Reports Survey, *supra* note 4 (explaining that 60% of those surveyed supported more government regulation of platforms to deal with their growing power that may be hurting competition and consumers).

written about these companies' power, less has been said about how to rein them in effectively. Contrary to some politicians' ideology,[6] market forces have not eroded their power. Several characteristics of the digital economy have led to tipping and sustained market power. These include extreme scale economies, strong network effects, data-driven advantages, lock-in effects, and high switching costs.[7]

So how can one protect one's privacy and data security in the digital economy? Many Americans (59%) support breaking up Big Tech.[8] Other jurisdictions, including Europe, call for regulating these gatekeepers.[9] Europe has a comprehensive privacy and data protection framework; the United States does not. While Congress has proposed an omnibus privacy statute,[10] none, as of late 2023, has been enacted. Europe is enacting additional measures to make the digital economy fairer and more contestable. Meanwhile, the bipartisan antitrust legislation to help rein in the data-opolies has stalled in the United States, despite John Oliver, among others, pressing the Congressional leadership to act.[11]

In the interim, the Federal Trade Commission (FTC) is relying on a 1914 statute to protect our sensitive personal information in the digital economy.[12] Over the past few decades, the FTC has prosecuted privacy and data

6. "Rather than pursue even stronger antitrust laws, Congress should allow the free market to thrive where consumers, not the government, decide how big a company should be." Ryan Tracy, *Antitrust Bill Targeting Big Tech in Limbo as Congress Prepares to Recess*, WALL ST. J. (Aug. 9, 2022), https://www.wsj.com/articles/antitrust-bill-targeting-big-tech-in-limbo-as-congress-prepares-to-recess-11659951180 (quoting Sen. Rand Paul (R., Ky.)).

7. For further analysis, see MAURICE E. STUCKE, BREAKING AWAY: HOW TO REGAIN CONTROL OVER OUR DATA, PRIVACY, AND AUTONOMY (2022); ARIEL EZRACHI & MAURICE E. STUCKE, HOW BIG-TECH BARONS SMASH INNOVATION AND HOW TO STRIKE BACK (2022); ARIEL EZRACHI & MAURICE E. STUCKE, VIRTUAL COMPETITION: THE PROMISE AND PERILS OF THE ALGORITHM-DRIVEN ECONOMY (2016); MAURICE E. STUCKE & ALLEN P. GRUNES, BIG DATA AND COMPETITION POLICY (2016); see also Regulation (EU) 2022/1925 (Digital Markets Act), 2022 O.J. (L 265), ¶¶ 2–3, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R1925 [hereinafter *DMA*].

8. Rani Molla, *Poll: Most Americans Want to Break Up Big Tech*, VOX (Jan. 26, 2021), https://www.vox.com/2021/1/26/22241053/antitrust-google-facebook-break-up-big-tech-monopoly.

9. *See, e.g.*, DMA, *supra* note 7.

10. *See, e.g.*, American Data Privacy and Protection Act (ADPPA), H.R. 8152, 117th Cong. (2d. Sess. 2022), https://www.govtrack.us/congress/bills/117/hr8152/text; JOHNATHAN M. GAFFNEY, ERIC N. HOLMES & CHRIS D. LINEBAUGH, CONG. RSCH. SERV., LSB10776, OVERVIEW OF THE AMERICAN DATA PRIVACY AND PROTECTION ACT, H.R. 8152 (June 30, 2022), https://crsreports.congress.gov/product/pdf/LSBLSB10776/1 (comparing the ADPPA to other privacy bills from the 117th and 116th Congresses).

11. Tracy, *supra* note 6.

12. 15 U.S.C. § 45.

protection offenses using its power to curb "unfair and deceptive acts and practices" under § 5 of the FTC Act.[13] Some have urged the FTC to go further and use its authority under § 5's "unfairness" prong to promulgate a "Data Minimization Rule."[14] The FTC in 2023 is still exploring this option.[15] But that provision limits the FTC's authority. For example, to declare an act or practice unfair, the FTC must show that "the act or practice 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."[16] But proving a substantial, cognizable injury to consumers can be difficult. Courts may require a showing of economic harm, which is often less relevant for privacy violations.[17] Where the plaintiff makes no claims for economic harm, they may be out of luck. The FTC would also have to show that the countervailing benefits to consumers or competition do not outweigh those injuries. Again, this can be done.[18] But one

13. *Privacy & Data Security Update*, FED. TRADE COMM'N (2015), https://www.ftc.gov/reports/privacy-data-security-update-2015.

14. CONSUMER REPORTS & ELECTRONIC PRIVACY INFORMATION CENTER (EPIC), HOW THE FTC CAN MANDATE DATA MINIMIZATION THROUGH A SECTION 5 UNFAIRNESS RULEMAKING (2022), https://epic.org/documents/how-the-ftc-can-mandate-data-minimization-through-a-section-5-unfairness-rulemaking/ (urging the FTC "to prohibit all secondary data uses with limited exceptions, ensuring that people can safely use apps and online services without having to take additional action") [hereinafter CR/EPIC REPORT]. Consumer Reports and Epic, however, noted that "if the FTC decides it has a stronger case to justify such rules under '"unfair methods of competition,"' we would strongly support such an effort." *See also* Rebecca Kelly Slaughter, Commissioner, *IAPP Closing Keynote 2021: Wait but Why? Rethinking Assumptions About Surveillance Advertising*, FED. TRADE COMM'N, (Oct. 22, 2021), https://www.ftc.gov/system/files/documents/public_statements/1597998/iapp_psr_2021_102221_final2.pdf.

15. Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273 (proposed Aug. 22, 2022).

16. FTC Act Amendments of 1994, Pub. L. No. 103–312, § 9, 108 Stat. 1691, 1695 (1994).

17. For example, an airline pilot claimed that the federal government violated the Privacy Act in unlawfully disclosing his confidential medical records, including his HIV status, which caused him "humiliation, embarrassment, mental anguish, fear of social ostracism, and other severe emotional distress." F.A.A. v. Cooper, 566 U.S. 284, 289 (2012). The district judge found that "emotional injury" alone did not qualify and dismissed the lawsuit, which the Supreme Court affirmed. Because the Privacy Act does not unequivocally authorize an award of damages for mental or emotional distress, the federal statute does not waive the Federal Government's sovereign immunity from liability for such harms. Thus, as the dissent noted, individuals can no longer recover under the Privacy Act the primary, and often only, damages sustained because of an invasion of privacy, namely mental or emotional distress.

18. *See* STUCKE, *supra* note 7, at chapters 4 & 10; EZRACHI & STUCKE, *supra* note 7, at 101–39; Finn Myrsted & Oyvind H. Kaldestad, *International Coalition Calls for Action Against Surveillance Based Advertising*, FORBRUKERRADET (June 2021), https://www.forbrukerradet.no/side/new-report-details-threats-to-consumers-from-surveillance-based-advertising/.

trap is that the court, in assessing the trade-off between privacy and competition, may emphasize the cost savings from lower behavioral advertising rates while discounting the harder-to-quantify privacy harms.[19]

The FTC has frequently targeted data collection practices as deceptive, as they involved "a material representation, omission or practice that is likely to mislead a consumer acting reasonably in the circumstances."[20] But the rulemaking's focus would be limited to making the privacy policies more transparent about the data being collected. The rulemaking would not address scenarios where the company does not have a privacy policy, or where the company discloses its rapacious data collection. Moreover, improving transparency will not necessarily improve privacy protection when consumers face "take-it-or-leave-it" offers, whereby they must consent to the data-opolies' terms for accessing their data or they will not get the service.[21] What

19. *See* STUCKE, *supra* note 7, at chapters 8 & 10.

20. *A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, FED. TRADE COMM'N (2021), https://www.ftc.gov/about-ftc/mission/enforcement-authority; *see, e.g.*, Facebook, Inc., FTC Docket No. C-4365 and Press Release, Fed. Trade Comm'n, FTC Proposes Blanket Prohibition Preventing Facebook from Monetizing Youth Data (May 3, 2023) (alleging in Order to Show Cause that Facebook violated both the 2012 and 2020 FTC orders "by continuing to give app developers access to users' private information after promising in 2018 to cut off such access if users had not used those apps in the previous 90 days" and that Meta "misled parents about their ability to control with whom their children communicated through its Messenger Kids app, and misrepresented the access it provided some app developers to private user data"); Press Release, Fed. Trade Comm'n, Google Will Pay $22.5 Million to Settle FTC Charges it Misrepresented Privacy Assurances to Users of Apple's Safari Internet Browser (Aug. 9, 2012), https://www.ftc.gov/news-events/news/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented-privacy-assurances-users-apples (Google agreeing to pay a then record $22.5 million civil penalty to settle the FTC's charges that "it misrepresented to users of Apple Inc.'s Safari internet browser that it would not place tracking 'cookies' or serve targeted ads to those users, violating an earlier privacy settlement between the company and the FTC.").

21. In the aftermath of the Cambridge Analytica scandal, for example, Facebook users' trust in the platform plummeted—with only 28% believing that the company is committed to privacy, down from a high of 79% in 2017. Herb Weisbaum, *Trust in Facebook Has Dropped by 66 Percent Since the Cambridge Analytica Scandal*, NBC NEWS (Apr. 18, 2018), https://www.nbcnews.com/business/consumer/trust-facebook-has-dropped-51-percent-cambridge-analytica-scandal-n867011. Despite the public outrage, the #DeleteFacebook campaign, and other scandals, Facebook continued to grow. Between March 2018, when the Cambridge Analytica news broke and March 2020, Facebook "added more than 400 million monthly users—more than the entire population of the U[nited] S[tates]." Laura Forman, *Facebook's Politics Aren't Aging Well*, WALL ST. J. (June 30, 2020), https://www. wsj.com/articles/facebooks-politics-arent-aging-well-11593446127. This is not because Facebook users are agnostic about privacy. Quite the contrary: 74% of surveyed users in 2018 were very or somewhat concerned about Facebook's invasion of their privacy (a 9-percentage point increase from 2011). Jeffrey M. Jones, *Facebook Users' Privacy Concerns Up Since 2011*, GALLUP

if users are displeased with the company's privacy violations? They cannot readily switch to alternative networks unless they could easily port their data and, when network effects are present, many others, including their friends, also switched to the alternative platform. So, while the FTC can and should promulgate rules to curb deceptive practices, these rules will be insufficient in ecosystems (1) dominated by data-opolies and (2) where behavioral advertising is the primary source of revenues.

Consequently, rather than rely primarily on the FTC's power to regulate unfair and deceptive practices, this Article takes a different approach. It assesses whether the FTC can prohibit a variety of privacy-related competition concerns as an "unfair method of competition" under the FTC Act.[22] This might seem semantic. After all, what difference does it make whether the data-opolies' abuses are *unfair practices* or *unfair methods of competition*? The answer is plenty. While the FTC can promulgate substantive regulations for both unfair practices and unfair methods of competition, the former has more procedural and substantive requirements.[23] Moreover, the FTC does not have to prove that an unfair method of competition caused a substantial injury to

(Apr. 11, 2018), https://news.gallup.com/poll/232319/facebook-users-privacy-concerns-2011.aspx.

22. At least one organization, Accountable Tech, has filed with the FTC a rulemaking petition to ban surveillance advertising—the extractive business model whereby Big Tech pervasively tracks and profiles people for the purpose of selling hyper-personalized ads—as an "unfair method of competition." Press Release, Accountable Tech, Accountable Tech Petitions FTC to Ban Surveillance Advertising as an 'Unfair Method of Competition' (Sept. 28, 2021), https://accountabletech.org/media/accountable-tech-petitions-ftc-to-ban-surveillance-advertising-as-an-unfair-method-of-competition/?cn-reloaded=1. The FTC has left open this option. It has also invited comments "on the ways in which existing and emergent commercial surveillance practices harm competition and on any new trade regulation rules that would address such practices," as "[s]uch rules could arise from the Commission's authority to protect against unfair methods of competition, so they may be proposed directly without first being subject of an advance notice of proposed rulemaking." Trade Regulation Rule on Commercial Surveillance and Data Security, 87 Fed. Reg. 51273, 51276 n.47 (proposed Aug. 22, 2022).

23. The FTC's ability to promulgate industry-wide rules prohibiting "unfair or deceptive acts or practices" is limited under the Magnuson-Moss Warranty-Federal Trade Commission Improvement Act and 1980 Federal Trade Commission Improvements Act, "which added procedural requirements to rulemaking governed by Magnuson-Moss and stripped the FTC of rulemaking authority on specific issues." Rohit Chopra & Lina M. Khan, *The Case for "Unfair Methods of Competition" Rulemaking*, 87 U. CHI. L. REV. 357, 378–79 (2020). These procedures, however, do not apply to the Commission's "unfair methods of competition" rulemaking authority. *Id.*; *see also* 15 U.S.C. § 57a (noting that the procedures under the Magnuson-Moss Act "shall not affect any authority of the Commission to prescribe rules (including interpretive rules), and general statements of policy, with respect to unfair methods of competition in or affecting commerce").

consumers.[24] Plus, many of the unfair data collection and surveillance practices that damage competition, consumer autonomy, and consumer privacy fit well within the range of unfair methods of competition. Granted, as this Article explores, some might challenge the FTC's authority to challenge unfair data collection and surveillance practices as unfair methods of competition. But this Article argues that Americans need not wait for comprehensive privacy and antitrust legislation to rein in the data-opolies and curb some of the excesses of the surveillance economy. The FTC has the power under its rulemaking and enforcement authority to punish, and hopefully deter, many of the abuses in collecting and using our personal data as unfair methods of competition.

After Part II outlines the legislative aim of "unfair methods of competition" and the FTC's 2022 policy statement on this subject,[25] Part III offers a taxonomy of unfair methods of competition and demonstrates how many of the unfair data collection and surveillance practices that damage competition, consumer autonomy, and consumer privacy fall within the existing categories. But some surveillance practices do not fall within these categories. That's o.k. Congress did not want to "confine the forbidden methods [of competition] to fixed and unyielding categories,"[26] so the FTC can use its power to deter these privacy-related competition concerns as well. Part IV addresses one key source of many problems in the surveillance economy—namely, behavioral advertising. Part V examines several concerns about such potential rulemaking, including whether it would run afoul of the Supreme Court's "major questions doctrine," as recently outlined in *West Virginia v. EPA*.[27] As this Article concludes, the FTC cannot repair the surveillance economy with its authority under the FTC Act. Nevertheless, the FTC absolutely can, and should, exercise the authority that Congress intended it to exercise to help rein in the data-opolies. America still needs an omnibus privacy framework, but the FTC can help close the regulatory gap.

---

24. In contrast, regulation under Magnuson-Moss would entail that, as well as projecting the rule's economic effects. Some argue that "rather than focus entirely on specific injuries tied to the collection and use of data, the FTC should recognize that the unwanted observation, through excessive data collection and use, is harmful in and of itself." CR/Epic Report, *supra* note 14, at 6. Whether courts would agree is a risk.

25. FED. TRADE COMM'N, POLICY STATEMENT REGARDING THE SCOPE OF UNFAIR METHODS OF COMPETITION UNDER SECTION 5 OF THE FEDERAL TRADE COMMISSION ACT (2022), https://www.ftc.gov/system/files/ftc_gov/pdf/p221202sec5enforcementpolicystatement_002.pdf [hereinafter 2022 FTC UMC Policy Statement].

26. F.T.C. v. R. F. Keppel & Bro., Inc., 291 U.S. 304, 310 (1934).

27. W. Virginia v. Env't Prot. Agency, 142 S. Ct. 2587, 2616 (2022) (Gorsuch, J., concurring) (summarizing doctrine as to where "administrative agencies must be able to point to 'clear congressional authorization' when they claim the power to make decisions of vast 'economic and political significance.'").

II. UNFAIR METHODS OF COMPETITION

A. THE FEDERAL TRADE COMMISSION ACT

In creating the FTC in 1914, Congress wanted the new agency to define and curb all "unfair methods of competition."[28] In contrast to the term "unfair competition," which courts had often construed as passing off one's business or goods for another,[29] the term "unfair methods of competition" was relatively new to US law.[30] Only two cases referred to "unfair methods of competition" before 1914,[31] one of which was ironically the Supreme Court's *Standard Oil* decision, which prompted Congress to enact the FTC Act.[32]

The unique term "unfair methods of competition," as employed in the Act, was meant to have a broader meaning than the common law of "unfair competition."[33] Congress purposely did not define this novel term. Why?

---

28. 15 U.S.C. § 45.

29. *See, e.g.*, A.L.A. Schechter Poultry Corp. v. United States, 295 U.S. 495, 531 (1935) (noting that "unfair competition," under the common law, was "a limited concept," primarily, and strictly, relating "to the palming off of one's goods as those of a rival trader").

30. *Id.* at 532 (noting that the FTC Act "introduced the expression 'unfair methods of competition,'" which "was an expression new in the law").

31. Burrow v. Marceau, 109 N.Y.S. 105, 107 (N.Y. App. Div. 1908) (noting that "there is no hard and fast rule" in determining when the court will "prevent what is practically a fraud upon a person engaged in business by the unfair methods of competition"); Standard Oil Co. of New Jersey v. United States, 221 U.S. 1, 42–43 (1911) (noting that Standard Oil had monopolized and restrained interstate commerce in petroleum and its products, by engaging in, inter alia, "unfair methods of competition, such as local price cutting at the points where necessary to suppress competition").

32. FED. TRADE COMM'N, STATEMENT OF CHAIR LINA M. KHAN JOINED BY COMMISSIONER ROHIT CHOPRA AND COMMISSIONER REBECCA KELLY SLAUGHTER ON THE WITHDRAWAL OF THE STATEMENT OF ENFORCEMENT PRINCIPLES REGARDING "UNFAIR METHODS OF COMPETITION" UNDER SECTION 5 OF THE FTC ACT 2–3 (2021), https://www.ftc.gov/system/files/documents/public_statements/1591498/final_statement_of_chair_khan_joined_by_rc_and_rks_on_section_5_0.pdf [hereinafter FTC WITHDRAWAL STATEMENT] ("After the Supreme Court announced in *Standard Oil* that it would subject restraints of trade to an open-ended 'standard of reason' under the Sherman Act, lawmakers were concerned that this approach to antitrust delayed resolution of cases, delivered inconsistent and unpredictable results, and yielded outsized and unchecked interpretive authority to the courts."); *see also* 2022 FTC UMC POLICY STATEMENT, *supra* note 25, at 2.

33. *See* F.T.C. v. Sperry & Hutchinson Co., 405 U.S. 233, 239–40 (1972) (noting that Congress in creating the FTC and charting its power and responsibility under § 5, "explicitly considered, and rejected, the notion that it reduce the ambiguity of the phrase 'unfair methods of competition' by tying the concept of unfairness to a common-law or statutory standard or by enumerating the particular practices to which it was intended to apply"); F.T.C. v. Raladam Co., 283 U.S. 643, 648 (1931) (noting that the legislative debate apparently convinced the sponsors of the FTC Act that unfair competition, "which had a wellsettled meaning at common law, were too narrow," so Congress substituted it with "unfair methods of competition": "Undoubtedly the substituted phrase has a broader meaning, but how much

Because any definition would be self-defeating. Congress recognized the futility of attempting to define the many iterations of unfair methods of competition:

> It is impossible to frame definitions which embrace all unfair practices. There is no limit to human inventiveness in this field. Even if all known unfair practices were specifically defined and prohibited, it would be at once necessary to begin over again.[34]

As Congress observed, "[i]t is the illusive character of the trade practice that makes it though condemned today appear in some other form tomorrow."[35]

Thus, Congress intended the term *unfair methods of competition* to be both far-reaching and evolving. Rather than proposing a closed universe of forbidden practices, Congress left it open-ended "so that it might include all devices which would tend to deceive or take unfair advantage of the public and so that it might not be confined within the narrow limits of existing law."[36]

The term encompasses, as we'll see, conduct that violates the federal antitrust laws (e.g., the Sherman and Clayton Acts) as well as conduct that constituted unfair competition under the common law. Congress, dissatisfied with the Supreme Court's rule of reason legal standard announced in *Standard Oil,* created the FTC to continually identify and deter unfair methods of competition.[37] The key "takeaway is that Congress designed the term as a

broader has not been determined."); 2022 FTC UMC POLICY STATEMENT, *supra* note 25, at 3; Neil W. Averitt, *The Meaning of "Unfair Methods of Competition" in Section 5 of the Federal Trade Commission Act*, 21 B.C. L. REV. 227, 235 (1980) (citing legislative history).

34. F.T.C. v. R. F. Keppel & Bro., Inc., 291 U.S. 304, 310 n.1 (1934) (noting how the committee carefully considered "whether it would attempt to define the many and variable unfair practices which prevail in commerce," and concluding that "there were too many unfair practices to define, and after writing 20 of them into the law it would be quite possible to invent others"); *see also* S. Rep. No. 597, 63rd Cong., 2d Sess., at 13 (1914); 2022 FTC UMC POLICY STATEMENT, *supra* note 25, at 3.

35. *Keppel*, 291 U.S. at 311–12 n.1 (1934) (quoting S. Rep. No. 63-597, at 13).

36. Note, *Unfair Competition at Common Law and under the Federal Trade Commission Source*, 20 COLUM. L. REV. 328, 331 (1920).

37. *Keppel*, 291 U.S. at 314 (noting how the FTC "was created with the avowed purpose of lodging the administrative functions committed to it in 'a body specially competent to deal with them by reason of information, experience and careful study of the business and economic conditions of the industry affected,' and it was organized in such a manner, with respect to the length and expiration of the terms of office of its members, as would 'give to them an opportunity to acquire the expertness in dealing with these special questions concerning industry that comes from experience.'" (quoting S. Rep. No. 63–597, 9–11 (1914)); Atl. Refin. Co. v. F.T.C., 381 U.S. 360, 367 (1965); *see also* Averitt, *supra* note 33, at 233 (noting Congress's displeasure with the Court's rule-of-reason legal standard, and its attendant costs of (i) delay in resolution; (ii) courts' divergent results; and (iii) shift in control of antitrust policy from Congress to the judiciary).

'flexible concept with evolving content,'" and "'intentionally left [its] development . . . to the Commission.'"[38] Or, as Judge Learned Hand wrote, the FTC's "duty is to bring trade into harmony with fair dealing":

> The Commission has a wide latitude in such matters; its powers are not confined to such practices as would be unlawful before it acted; they are more than procedural; its duty in part at any rate, is to discover and make explicit those unexpressed standards of fair dealing which the conscience of the community may progressively develop.[39]

Congress also intended to limit the courts' function, as the Supreme Court noted: "Where the Congress has provided that an administrative agency initially apply a broad statutory term to a particular situation, our function is limited to determining whether the Commission's decision 'has "warrant in the record" and a reasonable basis in law.'"[40]

B. THE FTC'S WITHDRAWAL

So, if Congress articulated, as Sandeep Vaheesan noted, "a grand progressive-populist vision of antitrust," and wanted "the FTC to police 'unfair methods of competition' that injure consumers, prevent rivals from competing on the merits, and allow large corporations to dominate our political system,"[41] then why hasn't the FTC, until recently, used this power to rein in the data-opolies? More notable are the FTC's past policy miscues, including vetoing its legal staff's recommendation and not challenging

38. F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236, 243 (3d Cir. 2015) (quoting F.T.C. v. Bunte Bros., 312 U.S. 349, 353 (1941) and *Atl. Refin. Co.*, 381 U.S. at 367); *see also* F.T.C. v. Indiana Fed'n of Dentists, 476 U.S. 447, 454 (1986) (noting how the standard of "unfairness" under the FTC Act "is, by necessity, an elusive one, encompassing not only practices that violate the Sherman Act and the other antitrust laws . . . but also practices that the Commission determines are against public policy for other reasons"); F.T.C. v. Motion Picture Advert. Serv. Co., 344 U.S. 392, 396 (1953) ("The point where a method of competition becomes 'unfair' within the meaning of the Act will often turn on the exigencies of a particular situation, trade practices, or the practical requirements of the business in question.").

39. F.T.C. v. Standard Educ. Soc., 86 F.2d 692, 695, 696 (2d Cir. 1936).

40. *Atl. Refin.*, 381 U.S. at 367–68 (quoting National Labor Relations Board v. Hearst Publications, Inc., 322 U.S. 111, 131 (1944)); *see also Indiana Fed'n of Dentists*, 476 U.S. at 455 ("Once the Commission has chosen a particular legal rationale for holding a practice to be unfair, however, familiar principles of administrative law dictate that its decision must stand or fall on that basis, and a reviewing court may not consider other reasons why the practice might be deemed unfair.").

41. Sandeep Vaheesan, *Resurrecting "A Comprehensive Charter of Economic Liberty": The Latent Power of the Federal Trade Commission*, 19 U. PA. J. BUS. L. 645, 650 (2017).

Google's anticompetitive behavior,[42] and not challenging any of the data-opolies' acquisitions, including Google-DoubleClick.[43] The FTC on competition matters was for many years hesitant: it "rarely used this expertise to affirmatively identify what conduct or practices constitute an 'unfair method of competition' and instead, sought to define 'unfair methods of competition' on a case-by-case basis."[44]

Instead of ferreting out the many unfair practices in the digital economy, the FTC, in its 2015 Policy Statement, retreated to antitrust law's convoluted and criticized rule of reason legal standard.[45] The FTC would apply the very

42. *The FTC Report on Google's Business Practices*, WALL ST. J. (Mar. 24, 2015), https://graphics.wsj.com/google-ftc-report/.

43. Press Release, Fed. Trade Comm'n, Federal Trade Commission Closes Google/DoubleClick Investigation: Proposed Acquisition Unlikely to Substantially Lessen Competition (Dec. 20, 2007), https://www.ftc.gov/news-events/news/press-releases/2007/12/federal-trade-commission-closes-googledoubleclick-investigation. Google in acquiring the leading publisher ad server DoubleClick solidified its control over the online advertising industry. As the federal and state antitrust enforcers alleged in their 2023 monopolization complaint against Google, the "DoubleClick acquisition vaulted Google into a commanding position over the tools publishers use to sell advertising opportunities," and "set the stage for Google's later exclusionary conduct across the ad tech industry." Complaint ¶ 16, United States v. Google, No. 1:23-cv-00108 (E.D. Va. Jan. 24, 2023). The acquisition also harmed privacy, when Google reversed its commitment to "not combine the data collected on internet users via DoubleClick with the data collected throughout Google's ecosystem" and "subsequently combined DoubleClick data with personal information collected through other Google services—effectively combining information from a user's personal identity with their location on Google Maps, information from Gmail, and their search history, along with information from numerous other Google products." STAFF OF H. COMM. ON THE JUDICIARY, SUBCOMM. ON ANTITRUST, COMMERCIAL AND ADMINISTRATIVE LAW, 117TH CONG., REP. AND RECOMMENDATIONS: INVESTIGATION OF COMPETITION IN DIGITAL MARKETS 210–11 (2020), https://permanent.fdlp.gov/gpo145949/competitionindigitalmarkets.pdf [hereinafter House Report].

44. Chopra & Khan, *supra* note 23, at 365.

45. FED. TRADE COMM'N, STATEMENT OF ENFORCEMENT PRINCIPLES REGARDING "UNFAIR METHODS OF COMPETITION" UNDER SECTION 5 OF THE FTC ACT (2015), https://www.ftc.gov/system/files/documents/public_statements/735201/150813section5enforcement.pdf (hereinafter FTC 2015 Statement) (stating that an "act or practice will be evaluated under a framework similar to the rule of reason, that is, an act or practice challenged by the Commission must cause, or be likely to cause, harm to competition or the competitive process, taking into account any associated cognizable efficiencies and business justifications"); Vaheesan, *supra* note 41, at 650–51 ("In articulating this narrow interpretation of Section 5, the FTC contradicted Congress's political economic vision in 1914, which sought to prevent not only short-term injuries to consumers, but also exclusionary practices by large businesses and the accumulation of private political power. And in making the rule of reason the centerpiece of its analytical framework, the FTC adopted a convoluted test that cannot advance the Congressional vision underlying Section 5."). For criticisms of the Court's rule of reason standard, see Maurice E. Stucke, *Does the Rule of Reason Violate the Rule of Law?*, 42 U.C. DAVIS L. REV. 1375 (2009) (collecting criticisms).

standard—rule of reason—that Congress rebuked in setting up the agency. Moreover, the Commission said it would "be guided by the public policy underlying the antitrust laws, namely, the promotion of consumer welfare."[46] As Part IV examines, the highly questionable consumer welfare standard never came from Congress, but from the Court, and has been under attack by scholars and enforcers. As the new FTC Chair Lina Khan noted, the FTC's 2015 Statement "doubled down on the agency's longstanding failure to investigate and pursue 'unfair methods of competition.'"[47] While the Commission could have engaged in rule-making to delineate "unfair methods of competition" in the digital economy, it failed to do so.[48] Rather, the 2015 Statement, observed several Commissioners, "contravene[d] the text, structure, and history of Section 5 and largely [wrote] the FTC's standalone authority out of existence."[49]

C. ANTITRUST RESURGENCE

By the late 2010s, the FTC, along with other competition agencies around the world, changed course. The evidence compiled by competition authorities in Europe, Australia, and Japan all pointed to the unfairness and lack of contestability plaguing the digital economy.[50] The DOJ and FTC (along with a bipartisan coalition of state attorneys general) brought the first monopolization cases against the data-opolies since the 1990s case against Microsoft.[51] In 2021, the Biden administration issued its Executive Order on Promoting Competition in the American Economy. The Order noted how "a small number of dominant internet platforms use their power to exclude

46. FTC 2015 Statement, *supra* note 45.

47. FED. TRADE COMM'N, REMARKS OF CHAIR LINA M. KHAN ON THE WITHDRAWAL OF THE STATEMENT OF ENFORCEMENT PRINCIPLES REGARDING "UNFAIR METHODS OF COMPETITION" UNDER SECTION 5 OF THE FTC ACT (2021), https://www.ftc.gov/system/files/documents/public_statements/1591506/remarks_of_chair_khan_on_the_withdrawal_of_the_statement_of_enforcement_principles_re_umc_under.pdf [hereinafter Khan 2021 Remarks on the Withdrawal of FTC Statement].

48. Chopra & Khan, *supra* note 23, at 366, 366 n.39 (noting the FTC's power to engage in rulemaking under the Administrative Procedure Act and citing other scholars encouraging the FTC to do so).

49. FTC WITHDRAWAL STATEMENT, *supra* note 32, at 1.

50. STUCKE & GRUNES, *supra* note 7, at 32–75.

51. *See* Complaint, United States v. Google, 1:23-cv-00108 (E.D. Va. Jan. 24, 2023); Complaint, United States v. Google, No. 1:20-cv-03010 (D.D.C. Oct. 20, 2020)) [hereinafter Google Compl.]; Complaint, F.T.C. v. Facebook, No. 1:20-cv-03590-CRC (D.D.C. Dec. 9, 2020); Complaint, New York v. Facebook, No. 1:20-cv-03589-JEB (D.D.C., Dec. 9, 2020), [hereinafter States Facebook Compl.]; Complaint, Colorado v. Google, No. 1:20-cv-03715-APM (D.D.C. Dec. 17, 2020) [hereinafter Colo. Google Compl.]; Texas v. Google, No. 4:20-cv-957 (E.D. Tex. Dec. 16, 2020).

market entrants, to extract monopoly profits, and to gather intimate personal information that they can exploit for their own advantage."[52] The Biden administration promised:

> to enforce the antitrust laws to meet the challenges posed by new industries and technologies, including the rise of the dominant Internet platforms, especially as they stem from serial mergers, the acquisition of nascent competitors, the aggregation of data, unfair competition in attention markets, the surveillance of users, and the presence of network effects.[53]

To address these "persistent and recurrent practices that inhibit competition," the executive order encouraged the FTC to exercise its statutory rulemaking authority, as appropriate and consistent with applicable law, in areas including "unfair data collection and surveillance practices that may damage competition, consumer autonomy, and consumer privacy."[54]

Toward that end, in 2021 the FTC withdrew its 2015 guidelines on unfair methods of competition. As the new FTC Chair, Khan promised "to clarify the meaning of Section 5 and apply it to today's markets[,]" thereby fulfilling "Congress's directive to prohibit unfair methods of competition."[55]

In late 2021, the Commission announced possible rulemaking under § 18 of the FTC Act "to curb lax security practices, limit privacy abuses, and ensure that algorithmic decision-making does not result in unlawful discrimination."[56] In its 2021 report to Congress, the FTC said it should deploy all its tools to protect Americans' privacy "[g]iven the serious harms stemming from surveillance practices and the absence of federal legislation."[57] Among the tools was its rule-making authority to prohibit unfair methods of competition.

In 2022, the FTC released the "Policy Statement Regarding the Scope of Unfair Methods of Competition Under Section 5 of the Federal Trade Commission Act."[58] Relying "on the text, structure, legislative history of

52. Executive Order on Promoting Competition in the American Economy, 86 Fed. Reg. 36987 (July 9, 2021), https://www.whitehouse.gov/briefing-room/presidential-actions/2021/07/09/executive-order-on-promoting-competition-in-the-american-economy/ [hereinafter Biden Executive Order].

53. *Id.*

54. *Id.*

55. Khan 2021 Remarks on the Withdrawal of FTC Statement, *supra* note 47, at 1–2.

56. *Trade Regulation Rule on Commercial Surveillance*, OFFICE OF INFORMATION AND REGULATORY AFFAIRS (2021), https://www.reginfo.gov/public/do/eAgendaViewRule?pubId=202110&RIN=3084-AB69.

57. Fed. Trade Comm'n, FTC Report to Congress on Privacy and Security, 2021 WL 4698008, at *6 (F.T.C. Sept. 13, 2021).

58. 2022 FTC UMC POLICY STATEMENT, *supra* note 25, at 1.

Section 5, precedent, and the FTC's experience applying the law," the updated policy statement describes the "key principles" of whether conduct is an unfair method of competition.[59] For conduct to run afoul of § 5, it must (1) implicate competition (whether directly or indirectly); and (2) be unfair. Conduct is unfair if it "goes beyond competition on the merits," which the FTC determines using the following two criteria: whether the conduct (1) is "coercive, exploitative, collusive, abusive, deceptive, predatory, or involve[s] the use of economic power of a similar nature," or is otherwise restrictive or exclusionary, depending on the circumstances; and (2) tends "to negatively affect competitive conditions" (e.g., "conduct that tends to foreclose or impair the opportunities of market participants, reduce competition between rivals, limit choice, or otherwise harm consumers").[60]

Consequently, the FTC appears poised to use its Congressional authority to tackle the many unfair data collection and surveillance practices that have bedeviled the digital economy. Rather than rely on a "case-by-case approach" to "unfair methods of competition," which "often fails to deliver clear guidance," the Commission may also adopt "rules to clarify the legal limits that apply to market participants."[61]

D. COMMON LAW

Congress intended that the term *unfair methods of competition* be broader than the common law's unfair competition. However, the common law is not static either. Indeed, the Restatement of the Law (Third) of Unfair Competition echoes several of the Congressional themes of the FTC Act.

First, the Restatement notes how it is "impossible to state a definitive test for determining which methods of competition will be deemed unfair" in addition to those well-established forms, such as deceptive marketing, infringement of trademarks, and appropriation of intangible trade values, including trade secrets and the right of publicity.[62]

---

59. *Id.* at 1.

60. *Id.* at 8, 9.

61. FTC WITHDRAWAL STATEMENT, *supra* note 32, at 7; *see also* FED. TRADE COMM'N, STATEMENT OF COMMISSIONER ALVARO M. BEDOYA REGARDING THE COMMERCIAL SURVEILLANCE DATA SECURITY ADVANCE NOTICE OF PROPOSED RULEMAKING (2022), https://www.ftc.gov/system/files/ftc_gov/pdf/Bedoya%20ANPR%20Statement%20 08112022.pdf; FED. TRADE COMM'N, STATEMENT OF CHAIR LINA M. KHAN REGARDING THE COMMERCIAL SURVEILLANCE AND DATA SECURITY ADVANCE NOTICE OF PROPOSED RULEMAKING COMMISSION (2022), https://www.ftc.gov/system/files/ftc_gov/pdf/ Statement%20of%20Chair%20Lina%20M.%20Khan%20on%20Commercial%20 Surveillance%20ANPR%2008112022.pdf.

62. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 1, cmt. g, at 4 (AM. L. INST. 1995).

Second, the Restatement recognizes that new types of unfair competition will always emerge and that the courts must "continue to evaluate competitive practices against generalized standards of fairness and social utility."[63] Thus, over the past few decades, neither the Restatement nor courts have limited the term *unfair competition* to specific fixed categories. As the Restatement states, "[a] primary purpose of the law of unfair competition is the identification and redress of business practices that hinder rather than promote the efficient operation of the market."[64]

Third, like the FTC Act, the Restatement's discussion of the common law of unfair practices "contemplates a fluid, 'residual rule of liability' for unfair practices that defies a definitive test."[65] Thus, both sets of law are open-ended, rather than closed, legal frameworks. Courts recognize a residual catch-all category of unfair competition, where it can strike down an act or practice that "substantially interferes with the ability of others to compete on the merits of their products or otherwise conflicts with accepted principles of public policy recognized by statute or common law."[66]

As one Pennsylvania state court noted,

> Those in business need to be assured that competitors will not be permitted to engage in conduct which falls below the minimum standard of fair dealing. Thus, the doctrine of unfair competition

63. *Id.*

64. *Id.*; *see also* Paccar Inc. v. Elliot Wilson Capitol Trucks LLC, 905 F. Supp. 2d 675, 692 (D. Md. 2012) (noting "the general view of the necessarily flexible contour of the unfair competition tort in changing business environment"); Warner Lambert Co. v. Purepac Pharm. Co., No. CIV.A. 00-02053(JCL), 2000 WL 34213890, at *10 (D.N.J. Dec. 22, 2000) (rejecting the argument that the state's caselaw narrows the scope of unfair competition claims, and noting how "The Restatement (Third) of Unfair Competition suggests a broad range of unfair competition claims").

65. Synthes, Inc. v. Emerge Med., Inc., No. CIV.A. 11-1566, 2014 WL 2616824, at *25 (E.D. Pa. June 11, 2014) (quoting Envtl. Tectonics Corp. v. Walt Disney World Co., No. Civ.A. 05–6412, 2008 WL 821065, at *16 (E.D. Pa. Mar. 26, 2008)).

66. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 1, cmt. g, at 4 (AM. LAW. INST. 1995). *See, e.g.*, Energy Consumption Auditing Servs., LLC v. Brightergy, LLC, 49 F. Supp. 3d 890, 899 (D. Kan. 2014) (quoting Restatement § 1 cmt. g); New Mexico Oncology & Hematology Consultants, Ltd. v. Presbyterian Healthcare Servs., 54 F. Supp. 3d 1189, 1233 (D.N.M. 2014); Sales Res., Inc. v. All. Foods, Inc., No. 4:08CV0732 TCM, 2009 WL 2382365, at *7 (E.D. Mo. July 30, 2009) (denying motion to dismiss and leaving it to the fact-finder "to determine if [Alliance's] behavior violated society's notions of fair play and fundamental fairness"); ID Sec. Sys. Canada, Inc. v. Checkpoint Sys., Inc., 249 F. Supp. 2d 622, 688 (E.D. Pa.), *amended*, 268 F. Supp. 2d 448 (E.D. Pa. 2003); Tension Envelope Corp. v. JBM Envelope Co., No. 14-567-CV-W-FJG, 2015 WL 893242, at *10 (W.D. Mo. Mar. 3, 2015) (finding that complaint's allegations, while not precisely fitting into any of the traditional categories of liability for unfair methods of competition, could fit into the Restatement's residual category), *aff'd*, 876 F.3d 1112 (8th Cir. 2017).

> provides the legal basis for business competitors to insist on fair play in the market in which they are involved . . . What constitutes unfair competition as opposed to fair competition is predicated in the balance to be struck between the public's interest in free competition and the protectable interests of the business person and the purchaser. The question of unfairness in competition is primarily a question of fact.[67]

As the Restatement notes, "courts have generally been reluctant to interfere in the competitive process."[68] Yet, courts will interfere when the act or practice "substantially interferes with the ability of others to compete on the merits of their products or otherwise conflicts with accepted principles of public policy recognized by statute or common law."[69]

Consequently, both the common law and FTC Act recognize the futility of stating a definitive test for determining all unfair practices or confining unfair methods to a few well-established categories. Invariably new forms of unfair practices will emerge that may not violate the existing standard but offend general principles of "honesty and fair dealing, rules of fair play and good conscience, and the morality of the marketplace."[70] Thus, the common law can provide another important avenue, besides the FTC Act, to target unfair data collection and surveillance practices that harm our privacy, autonomy, and well-being.

III. TAXONOMY OF UNFAIR METHODS OF COMPETITION

As we saw, Biden's executive order encouraged the FTC to exercise its statutory rulemaking authority to target "unfair data collection and surveillance practices that may damage competition, consumer autonomy, and consumer privacy."[71] The order also encourages the FTC to exercise its rulemaking authority "as appropriate and consistent with applicable law."[72] So, where does the FTC begin? One approach is to consider whether any of the "unfair data collection and surveillance practices" fall within the existing categories of unfair methods of competition. For example, does the data-opolies' use of dark patterns fall within any established category? How about the collection of too much data beyond what is necessary to provide the requested service?

---

67. Lakeview Ambulance & Med. Servs., Inc. v. Gold Cross Ambulance & Med. Servs., Inc., No. 1994-2166, 1995 WL 842000, at *2 (Pa. Com. Pl. Oct. 18, 1995).

68. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 1, cmt. g, at 4 (AM. LAW. INST. 1995).

69. *Id.*

70. *Id.*

71. Biden Executive Order, *supra* note 52, at § 5(h).

72. *Id.*

What about when the data-opoly acquires a nascent competitive threat that provides better privacy protection, such as Facebook's acquisition of WhatsApp?

Given the discussion in Part II, it may seem fruitless and self-defeating to provide a taxonomy of all unfair methods of competition, especially when Congress never intended to "confine the forbidden methods to fixed and unyielding categories." How can one classify something which, beyond a very broad level, is not classifiable? Nor will any taxonomy ever be definitive, as new forms and categories of unfair methods will inevitably arise.

Another risk is that any taxonomy, besides being underinclusive, can also be overinclusive. As Congress noted,

> It is also practically impossible to define unfair practices so that the definition will fit business of every sort in every part of this country. Whether competition is unfair or not generally depends upon the surrounding circumstances of the particular case. What is harmful under certain circumstances may be beneficial under different circumstances.[73]

So, should one forget about taxonomies, and simply ask whether particular data collection practices and surveillance techniques are unfair methods of competition? After all, the digital economy presents unique challenges, and jurisdictions like the European Union, United Kingdom, Australia, South Korea, and Germany are updating their competition and privacy laws to deter these practices.

Although one can start afresh, the aim of both the common law and FTC Act is to deter recurring, objectionable practices, while being sufficiently supple to reach new forms of conduct that violate generalized standards of unfairness, social utility, and the unexpressed standards of fair dealing which the conscience of the community may progressively develop. Thus, there is some utility in providing a taxonomy of the types of business practices that will likely (but not always) be deemed unfair, while acknowledging the need to continuously develop new categories to capture humans' ingenuity to devise new forms of competitive behavior that run counter to the public interest.

With these important limitations in mind, this Part assesses whether any of the unfair data collection and surveillance practices fall within five of the more well-established categories of unfair methods of competition. As there are many different types of unfair data collection and surveillance practices, not all of them will fall neatly into these existing five categories. But that is to

73. F.T.C. v. R. F. Keppel & Bro., Inc., 291 U.S. 304, 312 n.2 (1934) (quoting H. Rep. No. 1142, 63d Congress, 2d Sess., at 19 (1914)).

be expected. Where there are matches, however, the enforcement or rulemaking should be more straightforward, as prohibiting those practices is well within the FTC's authority.

A. CONDUCT THAT VIOLATES FEDERAL OR STATE STATUTES, INCLUDING THE FEDERAL ANTITRUST LAWS, AND COMMON LAW OF UNFAIR COMPETITION

It is axiomatic that companies cannot gain market power by resorting to otherwise illegal conduct. The law specifically puts these methods of competition off-limits. Moreover, Congress intended that unfair methods of competition include, but are not limited to, violations of common law unfair practices and the Sherman and Clayton Acts.[74] Thus, if a competitor harms the commercial relations of a rival by engaging in practices that violate federal or state statutes, it has engaged in unfair competition.[75] This includes otherwise intentional tortious conduct, such as threats of violence, product disparagement, bribery, and commercial defamation. The courts also recognized several specific categories of commercial behavior that give rise to a claim of unfair competition under common law, including (1) infringement of trademark and other protectable intellectual property rights and (2) misappropriation of trade secrets and other intangible trade values.[76] Companies that resort to these practices to gain market power violate § 5's unfair methods of competition. Moreover, if the conduct is illegal under the Sherman or Clayton Act, it also constitutes an unfair method of competition.[77]

Consequently, the FTC could prohibit all unfair data collection and surveillance practices that otherwise violate federal antitrust laws. One problem is that the Supreme Court has gradually displaced its per se illegal standard with its more fact-intensive legal standard, namely the rule of reason.[78] Thus, it is hard to identify which unfair data collection and surveillance practices violate the federal antitrust laws without engaging in the rule of reason inquiry that the rulemaking seeks to avoid. Indeed, it would

74. F.T.C. v. Motion Picture Advert. Serv. Co., 344 U.S. 392, 394 (1953) (noting how unfair methods of competition, which are condemned by § 5(a) of the FTC Act, "are not confined to those that were illegal at common law or that were condemned by the Sherman Act"); 2022 FTC UMC Policy Statement, *supra* note 25, at 3.

75. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 1, cmt. g, at 4 (AM. LAW. INST. 1995).

76. Synthes (U.S.A.) v. Globus Med., Inc., No. CIV.A. 04-CV-1235, 2005 WL 2233441, at *8 (E.D. Pa. Sept. 14, 2005) (citing RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 1, cmt. g, at § 1 (AM. LAW INST. 1995)).

77. F.T.C. v. Cement Inst., 333 U.S. 683, 690 (1948); 2022 FTC UMC POLICY STATEMENT, *supra* note 25, at 12; Averitt, *supra* note 33, at 238–42.

78. *See* Stucke, Rule of Reason, *supra* note 45.

require applying the legal standard that Congress sought to avoid in creating the FTC.

One area subject to rulemaking is where companies collude on privacy protections. Just as price fixing remains per se illegal,[79] so too would agreements among rivals on other important non-price parameters of competition, such as privacy protections. Arguably, companies might need to agree on privacy protection to promote interoperability and the flow of data. But if companies agree to degrade privacy protections, even when the companies are in no position to control the market, that should be prohibited.

B. INCIPIENT MENACES TO FREE COMPETITION

Unfair methods of competition extend well beyond otherwise illegal conduct. So, the next group of practices is "against public policy because of their dangerous tendency unduly to hinder competition or create a monopoly."[80] Thus, one major purpose of the FTC Act was to enable the FTC "to restrain practices as 'unfair' which, although not yet having grown into Sherman Act dimensions would . . . most likely do so if left unrestrained."[81] The FTC was expected "to stop at the threshold" any practice, which "if left alone, 'destroys competition and establishes monopoly.'"[82] The chief sponsor of the FTC Act said § 5 would "have such an elastic character that it [would] meet every new condition and every new practice that may be invented with a view to gradually bringing about monopoly through unfair competition."[83]

Congress left it to the FTC and courts "to determine what conduct, even though it might then be short of a Sherman Act violation, was an 'unfair method of competition.'"[84] Senator Newlands noted how "[t]here are numerous practices tending toward monopoly that may not come within the provisions of the antitrust law and amount to a monopoly or to monopolization. We want to check monopoly in the embryo."[85]

---

79. United States v. Socony-Vacuum Oil Co. Inc., 310 U.S. 150, 221 (1940).

80. *Cement Inst.*, 333 U.S. at 690 (quoting F.T.C. v. Gratz, 253 U.S. 421, 427 (1920)); *see also* F.T.C. v. Motion Picture Advert. Serv. Co., 344 U.S. 392, 394–95 (1953) (noting that the FTC Act "was designed to supplement and bolster the Sherman Act and the Clayton Act . . . to stop in their incipiency acts and practices which, when full blown, would violate those Acts").

81. *Cement Inst.*, 333 U.S. at 708.

82. *Id.* at 720 (quoting F.T.C. v. Raladam Co., 283 U.S. 643, 647 (1931)).

83. Chopra & Khan, *supra* note 23, at 379 (quoting Federal Trade Commission Act, 63d Cong, 2d Sess. In 51 Cong. Rec. 12024 (July 13, 1914)).

84. *Cement Inst.*, 333 U.S. at 708.

85. Gilbert Holland Montague, *Unfair Methods of Competition*, 25 YALE L.J. 20, 21 (1915); 51 CONG. REC. 13111.

Digital markets can lead to durable oligopolies and monopolies because of multiple network effects, the extreme scale economies, and the importance of data. Europe's Digital Markets Act (DMA) seeks to deter powerful companies from tipping digital markets through unfair business practices:

> A particular subset of rules should apply to those undertakings providing core platform services for which it is foreseeable that they will enjoy an entrenched and durable position in the near future. The same specific features of core platform services make them prone to tipping: once an undertaking providing the service has obtained a certain advantage over rivals or potential challengers in terms of scale or intermediation power, its position could become unassailable and the situation could evolve to the point that it is likely to become durable and entrenched in the near future. Undertakings can try to induce this tipping and emerge as gatekeeper by using some of the unfair conditions and practices regulated under this Regulation. In such a situation, it appears appropriate to intervene before the market tips irreversibly.[86]

Thus, both the DMA and FTC Act contain an incipiency standard that seeks to check monopoly in its infancy. It makes no sense to require the FTC to wait for markets in the digital economy to tip when Congress empowered the agency to reach unfair methods of competition before these practices hampered competition and enabled the leading platforms to capture the market.[87]

One interesting aspect is how the FTC Act would arrest incipient violations of the Clayton Act, which contains an incipiency standard.[88] As Neil W. Averitt observed, the FTC Act would permit "a theory of 'incipient incipiency.'"[89]

86. *DMA*, *supra* note 7, ¶ 26.

87. F.T.C. v. Motion Picture Advert. Serv. Co., 344 U.S. 392, 394–95 (1953) (noting that enforcement of the FTC Act was "designed to supplement and bolster the Sherman Act and the Clayton Act . . .to stop in their incipiency acts and practices which, when full blown, would violate those Acts . . . as well as to condemn as 'unfair method of competition' existing violations of them"); Averitt, *supra* note 33, at 242 (noting the legislative history in support of this goal); 2022 FTC UMC POLICY STATEMENT, *supra* note 25, at 4, 9.

88. *See, e.g.*, Clayton Antitrust Act of 1914 § 3, 15 U.S.C. § 14 (prohibiting the sale of goods on the condition that the purchaser thereof shall not use or deal in the goods of a competitor where the effect of such restraint "may be to substantially lessen competition or tend to create a monopoly in any line of commerce"); Clayton Antitrust Act of 1914 § 7, 15 U.S.C. § 18 (prohibiting mergers and acquisitions that may substantially lessen competition, or tend to create a monopoly).

89. Averitt, *supra* note 33, at 246.

The Supreme Court recognized this incipient incipiency in *F.T.C. v. Brown Shoe Co., Inc.*[90] Brown Shoe, the second-largest shoe manufacturer in the United States, paid hundreds of retail shoe stores to contractually promise to deal primarily with Brown and not purchase conflicting lines of shoes from Brown's competitors. The Court held that the FTC "acted well within its authority in declaring the Brown franchise program unfair whether it was completely full blown or not."[91] The FTC did not have to prove that Brown's franchise program violated the Clayton Act (namely, that the program's effect "may be to substantially lessen competition or tend to create a monopoly"). As the Court noted, the FTC has the power under § 5 to arrest trade restraints in their incipiency without having to prove that the restraints violate the Clayton Act or other antitrust laws.[92]

Europe's Digital Markets Act identifies many anticompetitive actions that the leading platforms may use to tip the markets in their favor. Once entrenched, the powerful gatekeeper may still rely on some of these anticompetitive practices to maintain their dominance or leverage it to other markets. Thus, the Act seeks to complement the E.U. antitrust laws to promote contestable and fair digital markets.

The United States has several bills that will impose some of these obligations on these gatekeepers, as well as more stringent requirements.[93] But

90. 384 U.S. 316, 320 (1966).

91. *Id.* at 322.

92. *Id.*; *see also* 2022 FTC UMC POLICY STATEMENT, *supra* note 25, at 9–10 ("Because the Section 5 analysis is purposely focused on incipient threats to competitive conditions, this inquiry does not turn to whether the conduct directly caused actual harm in the specific instance at issue. Instead, the second part of the principle examines whether the respondent's conduct has a tendency to generate negative consequences . . .").

93. These include (i) the Augmenting Compatibility and Competition by Enabling Service Switching (ACCESS) Act of 2021, H.R. 3849 (which gives the FTC new authority and enforcement tools to establish pro-competitive rules for interoperability and data portability online); (ii) the Platform Competition and Opportunity Act of 2021, H.R. 3849 (which prohibits the largest online platforms from engaging in mergers that would eliminate competitors, or potential competitors, or that would serve to enhance or reinforce monopoly power) (the Senate introduced its own similar version of Platform Competition and Opportunity Act of 2021); (iii) the American Choice and Innovation Online Act, H.R. 3816 (which seeks to restores competition online and ensures that digital markets are fair and open by preventing dominant online platforms from using their market power to pick winners and losers, favor their own products, or otherwise distort the marketplace through abusive conduct online) (the Senate introduced a slightly different version of its American Innovation and Choice Online Act, with different categories of offenses and defenses); (iv) the Ending Platform Monopolies Act, H.R. 3825 (which authorizes the FTC and DOJ to take action prevent dominant online platforms from leveraging their monopoly power to distort or destroy competition in markets that rely on that platform); (v) Prohibiting Anti-competitive

the FTC can also use its enforcement and rulemaking authority to impose obligations—similar to those in Articles 5 and 6 of the Digital Markets Act—to prevent firms from resorting to these anticompetitive practices.

Here the data-opolies' anticompetitive actions to willfully attain or maintain their monopolies can harm individuals' privacy. For example, the Colorado-led states allege in their monopolization complaint against Google that "[i]n a more competitive market, Google's search-related monopolies could be challenged or even replaced by new forms of information discovery," including rival general search engines offering "improved privacy" and "advertising-free search."[94] However, Google's exclusionary anticompetitive practices foreclosed these privacy-friendly rivals and helped Google maintain its dominance (and ability to extract even more personal data).

Another example is what we call the *nowcasting radar*.[95] A lot of data flows through the data-opolies' ecosystems, including: (1) commercially sensitive data from app developers, merchants, and businesses who advertise on their platforms; and (2) our personal data, such as our activity on apps and the products and services we buy online. From this data, data-opolies can see how and where we spend our time, identify trends, and target any potential threats to their business model or power early on. The internal corporate documents uncovered by Congress in its investigation of Big Tech show how these data-opolies use this data to provide themselves multiple competitive advantages.[96]

To check monopoly at the door, the FTC can challenge as unfair methods of competition both the use of this nowcasting radar and actions taken as a result.

Mergers Act of 2022 (which both the House and Senate introduced versions); and (vi) the Open App Markets Act (where both the House and Senate have introduced similar versions).

94. Colo. Google Compl., *supra* note 51, ¶ 16.

95. STUCKE & GRUNES, *supra* note 7, at 285–87; EZRACHI & STUCKE, *supra* note 7, at 43–44.

96. STUCKE, *supra* note 7, at 33–37. One way is the data-opoly's use of its business users' non-public data to compete against them, such as Amazon's use of non-public data of its third-party sellers to compete against them (by, among other things, cloning their products). To deter that, Article 6(1) of the Digital Markets Act provides that gatekeepers "shall not use, in competition with business users, any data that is not publicly available that is generated or provided by those business users in the context of their use of the relevant core platform services or of the services provided together with, or in support of, the relevant core platform services, including data generated or provided by the end users of those business users." This is also an unfair trade practice under the common law. *See* RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 1, cmt. g, at 10 (AM. LAW INST. 1995) (noting how "[a] competitor who diverts business from another . . . through the wrongful use of confidential information" may be liable even if its conduct is not deceptive or the information is not a trade secret).

One way the data-opolies attain, maintain, and extend their power is through acquisitions. The acquisition strategy helps the data-opoly maintain its dominance in at least five ways:

- First, it extinguishes the competitive threat and widens the protective moat around the data-opoly.[97]
- Second, in acquiring a maverick, the data-opoly keeps these threats "out of the hands of other firms that are well-positioned to use them to compete," including another data-opoly.[98]
- Third, the acquisition prevents competitors or potential competitors "from having access to next generation technology that might threaten" the data-opoly.[99]
- Fourth, the acquisitions can create "kill zones" by chilling other firms' incentives to enter or invest in that particular space.[100]
- Fifth, the acquisitions enable data-opolies to use network effects offensively and deprive rivals of gaining scale.[101]

---

97. HOUSE REPORT, *supra* note 43, at 150 (noting how Facebook's "internal documents indicate that the company acquired firms it viewed as competitive threats to protect and expand its dominance in the social networking market" and how "Facebook's senior executives described the company's mergers and acquisitions strategy in 2014 as a 'land grab' to 'shore up our position'").

98. States Facebook Compl., *supra* note 51, ¶ 185.

99. *Id.*

100. EZRACHI & STUCKE, *supra* note 7, at 86–90; HOUSE REPORT, *supra* note 43, at 49 (noting study "that in the wake of an acquisition by Facebook or Google, investments in startups in the same space 'drop by over 40% and the number of deals falls by over 20% in the three years following an acquisition'") (quoting Raghuram Rajan, Sai Krishna Kamepalli, & Luigi Zingales, *Kill Zone*, UNIV. CHI. BECKER FRIEDMAN INST. ECON., WORKING PAPER NO. 2020-19, https://ssrn.com/abstract=3555915); *see also* Ufuk Akcigit, Wenjie Chen, Federico J. Díez, Romain Duval, Philipp Engler, Jiayue Fan, Chiara Maggi, Marina M. Tavares, Daniel Schwarz, Ippei Shibata & Carolina Villegas-Sánchez, *Rising Corporate Market Power: Emerging Policy Issues*, 2021 INT'L MONETARY FUND STAFF DISCUSSION NOTE 1, 7 (Mar. 2021), https://www.imf.org/en/Publications/Staff-Discussion-Notes/Issues/2021/03/10/Rising-Corporate-Market-Power-Emerging-Policy-Issues-48619 ("M&As by dominant firms are associated with lower business dynamism at the industry level, with acquiring firms increasing their market power following the transaction and competitors' growth and research and development taking a hit.").

101. HOUSE REPORT, *supra* note 43, at 144. Facebook's CEO told the company's Chief Financial Officer in 2012 that network effects and winner-take-all markets were a motivating factor in acquiring competitive threats like Instagram and stressed the competitive significance of having a first-mover advantage in terms of network effects in acquiring WhatsApp. In the context of market strategies for competing with the then independent startup WhatsApp, Mr.

Privacy can also suffer when a data-opoly acquires a nascent competitive threat that offers better privacy protections, such as Facebook's acquisition of WhatsApp. The FTC can challenge these acquisitions under the Sherman and Clayton Acts and as an unfair method of competition.[102] However, it has been very challenging for the antitrust agencies to prove that these data-driven mergers violate their country's merger law. Every jurisdiction that has studied these digital platform markets has called for greater antitrust scrutiny of these data-driven and platform-related mergers and acquisitions. The problem is that some courts expect the competition agencies to prove these mergers' harm with high degrees of precision.[103] As a result, policymakers have proposed legislative changes to the legal standard for reviewing these mergers.[104] The DOJ and FTC in 2023 released for public comment their draft merger guidelines, which included presumptions that certain transactions are anticompetitive, threats to potential and nascent competition, and the unique characteristics of digital markets.[105]

The FTC could try to prevent the data-opolies from using the data flowing through their ecosystem to identify nascent competitive threats, which they then acquire. But enforcing this restriction can be difficult. Facebook could still use its nowcasting radar to identify the next WhatsApp but offer a more innocuous justification for its acquisition.

Zuckerberg told the company's growth and product management teams that "being first is how you build a brand and a network effect." *Id.*

102. *See, e.g.*, Amended Complaint at ¶ 241, F.T.C. v. Facebook, Case 1:20-cv-03590-JEB (D.D.C. Aug. 19, 2021) (challenging Facebook's anticompetitive acquisitions of Instagram and WhatsApp as violations "of Section 2 of the Sherman Act, 15 U.S.C. § 2, and thus unfair methods of competition in violation of Section 5(a) of the FTC Act, 15 U.S.C. § 45(a)").

103. *See* EZRACHI & STUCKE, *supra* note 7, at 161–80.

104. *See, e.g.*, The Platform Competition and Opportunity Act of 2021, H.R. 3826, 117th Cong. (1st Sess. 2021) (prohibiting the largest online platforms from engaging in mergers that would eliminate competitors, or potential competitors, or that would serve to enhance or reinforce monopoly power); The Competition and Antitrust Law Enforcement Reform Act of 2021, S. 225, 117th Cong. (1st Sess. 2021); HOUSE REPORT, *supra* note 43, at 396–97 (recommending that "Congress explore presumptions involving vertical mergers, such as a presumption that vertical mergers are anticompetitive when either of the merging parties is a dominant firm operating in a concentrated market, or presumptions relating to input foreclosure and customer foreclosure"); FED. TRADE COMM'N, STATEMENT OF CHAIR LINA M. KHAN, COMMISSIONER ROHIT CHOPRA, AND COMMISSIONER REBECCA KELLY SLAUGHTER ON THE WITHDRAWAL OF THE VERTICAL MERGER GUIDELINES (2021), https://www.ftc.gov/system/files/documents/public_statements/1596396/statement_of_chair_lina_m_khan_commissioner_rohit_chopra_and_commissioner_rebecca_kelly_slaughter_on.pdf.

105. DOJ & FTC, Draft Merger Guidelines (July 19, 2023), https://www.justice.gov/atr/d9/2023-draft-merger-guidelines.

To prevent this circumvention, the FTC could create a presumption against acquisitions by dominant firms of: (1) startups, particularly those that "serve as direct competitors, as well as those operating in adjacent or related markets";[106] and (2) data-driven mergers, where the data may help the firm attain, maintain, or leverage its significant market power. Fundamentally, "any acquisition by a dominant platform would be presumed anticompetitive unless the merging parties could show that the transaction was necessary for serving the public interest and that similar benefits could not be achieved through internal growth and expansion."[107]

This presumption would fit well within the broader incipiency standard for unfair methods of competition. The FTC could also limit the data-opolies from using the "near-perfect market intelligence" offensively (to favor their products, services, and apps, and to disadvantage competing products and services) and defensively (to identify and acquire potential nascent competitive threats).

Here, the regulations would improve privacy both directly and indirectly: directly, by preventing data-driven mergers, where the data-opoly learns even more about individuals (such as when Google acquired the smartwatch manufacturer Fitbit); and indirectly, by improving the survival odds of nascent competitive threats that offer better privacy protections (such as WhatsApp). Data-opolies could no longer acquire these threats; nor could they kill these threats as easily as now when the FTC imposes obligations similar to those under the DMA on these powerful gatekeepers.

C. MONOPOLISTIC BEHAVIOR

As the Supreme Court noted, "[e]ver since Congress overwhelmingly passed and President Benjamin Harrison signed the Sherman Act in 1890, protecting consumers from monopoly prices has been the central concern of antitrust."[108] So Apple could be liable under the Sherman Act for using its monopoly power over the retail apps market to charge individuals higher-than-competitive prices.[109] Yet in other cases, the Court opined that charging monopolistic prices is legal under the Sherman Act.[110] Regardless, the FTC

106. *See* HOUSE REPORT, *supra* note 43, at 396.

107. *See id.* at 389.

108. Apple Inc. v. Pepper, 139 S. Ct. 1514, 1525 (2019) (internal quotation omitted).

109. *Id.*

110. Pac. Bell Tel. Co. v. linkLine Comm'ns, Inc., 555 U.S. 438, 454 (2009) ("[A]ntitrust law does not prohibit lawfully obtained monopolies from charging monopoly prices."); *see also* Verizon Comm'ns Inc. v. L. Offs. of Curtis V. Trinko, LLP, 540 U.S. 398, 407 (2004) ("The mere possession of monopoly power, and the concomitant charging of monopoly prices, is not only not unlawful; it is an important element of the free-market system.").

could challenge under the broader "unfair method of competition" the excessive extraction of data itself.[111]

One issue is when a data-opoly exploits its dominance by collecting too much data. When a data-opoly's business model depends on harvesting and exploiting personal data, its incentives change. It will reduce privacy protections below competitive levels and collect personal data above competitive levels.[112] Consequently, policymakers increasingly recognize that companies can compete on privacy and protecting data.[113] The collection of

111. *See, e.g.*, 2022 FTC UMC POLICY STATEMENT, *supra* note 25, at 9 (unfair methods of competition reach, inter alia, coercive, exploitative, and abusive conduct).

112. HOUSE REPORT, *supra* note 43, at 18 (noting that "in the absence of adequate privacy guardrails in the United States, the persistent collection and misuse of consumer data is an indicator of market power online" and "[i]n the absence of genuine competitive threats, dominant firms offer fewer privacy protections than they otherwise would, and the quality of these services has deteriorated over time"); *id.* at 51 (noting how the "best evidence of platform market power" is "not prices charged but rather the degree to which platforms have eroded consumer privacy without prompting a response from the market"); UK COMPETITION & MARKETS AUTHORITY, ONLINE PLATFORMS AND DIGITAL ADVERTISING MARKET STUDY: MARKET STUDY FINAL REPORT ¶¶ 2.84, 3.151 (July 1, 2020), https://assets.publishing.service.gov.uk/media/5fa557668fa8f5788db46efc/Final_report_Digital_ALT_TEXT.pdf [hereinafter CMA FINAL REPORT]; *see also* AUSTRALIAN COMPETITION AND CONSUMER COMMISSION, DIGITAL PLATFORMS INQUIRY—FINAL REPORT 374 (2019), https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report [hereinafter ACCC FINAL REPORT]; Google Compl., *supra* note 51, ¶ 167 (alleging that by "restricting competition in general search services, Google's conduct has harmed consumers by reducing the quality of general search services (including dimensions such as privacy, data protection, and use of consumer data")); Colo. Google Compl., *supra* note 51, ¶ 98 (alleging that "Google collects more personal data about more consumers than it would in a more competitive market as a result of its exclusionary conduct, thereby artificially increasing barriers to expansion and entry"); States Facebook Compl., *supra* note 51, ¶¶ 127, 177, 180 (alleging Facebook's degradation in privacy protection after acquiring Instagram and WhatsApp).

113. OECD Consumer Data Rights and Competition, *supra* note 2, ¶¶ 69, 99, 100. *See, e.g.*, OECD Consumer Data Rights and Competition – Note by the European Union, ¶ 51, OECD Doc. DAF/COMP/WD(2020)40 (June 3, 2020), https://one.oecd.org/document/DAF/COMP/WD(2020)40/en/pdf ("Market investigations in specific cases, such as Microsoft/LinkedIn, have further supported the view that data protection standards can be an important parameter of competition, particularly in markets characterised by zero-price platform services where the undertaking has an incentive to collect as much data as possible in order to better monetise it on the other side of the platform."); *Comm'n Decision No. M.8124 (Microsoft/LinkedIn)*, C(2016) 8404 final, ¶ 350 (Dec. 6, 2016), https://ec.europa.eu/competition/mergers/cases/decisions/m8124_1349_5.pdf (finding that privacy is an important parameter of competition and driver of customer choice in the market for professional social networks, and that Microsoft, after acquiring LinkedIn, could marginalize competitors that offered "a greater degree of privacy protection to users than LinkedIn (or make the entry of any such competitor more difficult)" and thus "restrict consumer choice in relation to this important parameter of competition"); *see also* DIGITAL COMPETITION EXPERT PANEL, UNLOCKING DIGITAL COMPETITION 49 (2019), https://www.gov.uk/government/

too much personal data can be the equivalent of charging an excessive price.[114] As the U.K. competition agency noted, "The collection and use of personal data by Google and Facebook for personalised advertising, in many cases with no or limited controls available to consumers, is another indication that these platforms do not face a strong enough competitive constraint."[115] Thus, data-opolies exploit their market power by extracting personal data from consumers.

Indeed, this exploitation can be far worse than when a monopoly charges higher prices. When a monopoly demands an excessive price, consumers are aware of this abuse of dominance. One might grumble, as many did, for example, about Comcast's exorbitant fee for internet access.[116] But monopoly pricing might attract entrants eager to serve the monopoly's dissatisfied customers.

With a data-opoly, however, customers are typically unaware of how steep a price they are paying in terms of the amount of data being collected and the

publications/unlocking-digital-competition-report-of-the-digital-competition-expert-panel [hereinafter FURMAN REPORT]; OECD Consumer Data Rights and Competition – Note by the UK, ¶ 25 OECD Doc. DAF/COMP/WD(2020)51 (June 2, 2020), https://one.oecd.org/document/DAF/COMP/WD(2020)51/en/pdf (noting how privacy and data protection rights "may constitute an aspect of service quality on which firms can differentiate themselves from their competitors" and a merger's reduction in "privacy protection may be interpreted as a reduction in quality") (internal quotation and citations omitted).

114. OECD, Consumer Data Rights and Competition, *supra* note 113, ¶ 100; CMA FINAL REPORT, *supra* note 112, ¶ 11 (noting that "competition problems result in consumers receiving inadequate compensation for their attention and the use of their personal data by online platforms"); OECD, *Big Data: Bringing Competition Policy to the Digital Era*, Background Note by the Secretariat, at 16–17 (OECD Doc. DAF/COMP(2016)14) (Oct. 27, 2016), https://one.oecd.org/document/DAF/COMP(2016)14/en/pdf ("[M]arket power may be exerted through non-price dimensions of competition, allowing companies to supply products or services of reduced quality, to impose large amounts of advertising or even to collect, analyze or sell excessive data from consumers"); Eleonora Ocello, Cristina Sjödin, & Anatoly Subočs, *What's Up with Merger Control from the Digital Sector? Lessons from the Facebook/WhatsApp EU merger case, Competition Merger Brief*, EUROPEAN COMM'N 6 (Feb. 2015), https://ec.europa.eu/competition/publications/cmb/2015/cmb2015_001_en.pdf (observing if a website, post-merger, "would start requiring more personal data from users or supplying such data to third parties as a condition for delivering its 'free' product" then this "could be seen as either increasing its price or as degrading the quality of its product").

115. CMA FINAL REPORT, *supra* note 112, ¶ 6.31.

116. Bob Fernandez, *Comcast Customer Gripes About Internet Surpass Those for Cable TV*, PHILA. INQUIRER (Aug. 3, 2017), https://www.inquirer.com/philly/business/comcast/comcast-customer-gripes-for-the-internet-surpass-those-on-tv-20170803.html (reporting that between November 2014 and the first week of May 2017, Comcast consumers lodged 41,760 internet complaints with the FCC with 21,388 complaints regarding internet billing issues, followed by 8,664 complaints involving downed internet or lack of availability, and 4,853 complaints about speed).

toll it has on their privacy and well-being.[117] We simply don't know the price. In addition to all the other entry barriers in the digital economy (such as network effects, data access, etc.), consumers are unaware of the extent to which they are being exploited.

In Europe, extracting too much data, like charging an excessive price, can be struck down as an abuse of dominance. Germany's Bundeskartellamt, for example, found that Facebook abused its dominant position by "collect[ing] an almost unlimited amount of any type of user data from third party sources, allocat[ing] these to the users' Facebook accounts and us[ing] them for numerous data processing processes."[118]

But successfully prosecuting this type of case in the European Union is significantly harder than other abuse of dominance cases. It is hard to prove when prices are excessive. Proving that the amount of data being collected is excessive is even harder. Indeed, the challenges that Germany faced in bringing the Facebook case led that country to update its competition laws to make it easier to challenge dominant firms' excessive data collection.[119] It also led Europe to revise its Digital Markets Act to limit the collection of data against the individual's wishes. A gatekeeper, under the Act, cannot, without the individual's consent:

117. ACCC FINAL REPORT, *supra* note 112, at 2–3; *see also* FURMAN REPORT, *supra* note 113, at 22 (finding that many platforms operating in the attention market "provide valued services in exchange for their users' time and attention, while selling access to this time to companies for targeted advertising," but many consumers "are typically not consciously participating in this exchange, or do not appreciate the value of the attention they are providing") & 23 (noting that many consumers "are not aware of the extent or value of their data which they are providing nor do they usually read terms and conditions for online platforms"); CMA FINAL REPORT, *supra* note 112, ¶¶ 4.61–62.

118. *See, e.g.*, Press Release, Bundeskartellamt, Bundeskartellamt prohibits Facebook from combining user data from different sources (Feb. 7, 2019), https://www.bundeskartellamt.de/SharedDocs/Publikation/EN/Pressemitteilungen/2019/07_02_2019_Facebook.pdf?__blob=publicationFile&v=2.

119. *See* Section 19a of the German Competition Act, Gesetz zur Änderung des Gesetzes gegen Wettbewerbsbeschränkungen für ein fokussiertes, proaktives und digitales Wettbewerbsrecht 4.0 und anderer Bestimmungen [10th amendment to the German Act against Restraints of Competition] (Jan. 18, 2021), https://www.bgbl.de/xaver/bgbl/start.xav#__bgbl__%2F%2F*%5B%40attr_id%3D%27bgbl121s0002.pdf%27%5D__1680647993821. The German competition authority applied this new power to challenge Google's data collection policies. *See* Bundeskartellamt, Press Release, Statement of Objections Issued Against Google's Data Processing Terms (Jan. 11, 2023), https://www.bundeskartellamt.de/SharedDocs/Meldung/EN/Pressemitteilungen/2023/11_01_2023_Google_Data_Processing_Terms.html.

> (a) process, for the purpose of providing online advertising services, personal data of end users using services of third-parties that make use of core platform services of the gatekeeper;
>
> (b) combine personal data from the relevant core platform service with personal data from other core platform services or from any other services provided by the gatekeeper or with personal data from third-party services;
>
> (c) cross-use personal data from the relevant core platform service in other services provided separately by the gatekeeper, including other core platform services, and vice-versa; and
>
> (d) sign in end users to other services of the gatekeeper in order to combine personal data.[120]

Why this amendment to the DMA? As the European Union stated, besides degrading Europeans' privacy, the above four practices can also give the data-opoly an unfair competitive advantage by raising entry barriers and further reducing the contestability of digital markets.[121] For example, requiring individuals and business users to subscribe to, or register with, any of the gatekeeper's core services in order to use it, can lock-in these users, while gathering more data from them.[122] These concerns relate to one historical concern of unfair methods of competition, namely being "against public policy because of their dangerous tendency unduly to hinder competition or create monopoly."[123]

Thus, the FTC, like Germany and the European Commission, can target these gatekeepers' abusive data strategies, including combining personal data across their ecosystem and from third-party sources and collecting more personal data than what is reasonably necessary to provide the service. Not only is the excessive data collection abusive, but it can also hinder competition. The data-opoly can leverage the data internally to give itself an unfair advantage over rivals. As one review of the economic literature noted, the data-opolies can use data's non-rivalrous nature to give themselves an additional competitive advantage by leveraging the data internally across their many

120. *DMA*, *supra* note 7, art. 5(2).

121. *Id.* at ¶ 59.

122. *Id.* at ¶ 44 (noting how the practice enables the gatekeeper to capture and lock-in new business users and end users "for their core platform services by ensuring that business users cannot access one core platform service without also at least registering or creating an account for the purposes of receiving a second core platform service," and gives gatekeepers a potential advantage in terms of accumulating data; since this conduct is liable to raise barriers to entry, the Digital Markets Act prohibits it).

123. F.T.C. v. Gratz, 253 U.S. 421, 427 (1920).

products and services, thereby increasing entry barriers.[124] Thus, leveraging the excessive data a data-opoly collects in one market to destroy competition in other markets qualifies as an unfair method of competition.[125]

The FTC can target the following four data collection and surveillance practices as unfair methods of competition: When the data-opoly—

(1) extracts data when individuals visit third-party apps and websites,[126]

(2) extracts more data than what is reasonably necessary to provide the product or service,

(3) uses the data for purposes unrelated to providing the immediate service,[127] and

---

124. Yan Carrière-Swallow & Vikram Haksar, *The Economics and Implications of Data: An Integrated Perspective* 22, INTERNATIONAL MONETARY FUND POLICY PAPER No. 19/16, Sept. 2019:

> [W]here data appears as one of the factors of production, nonrivalry of data gives rise to increasing returns to scale when data is combined with other inputs. The intuition is that each unit of data can be used by all units of other inputs simultaneously. A larger stock of complementary labor or capital allows each unit of data to be better exploited, raising the average product of data. An implication is that access to the same nonrival data results in larger firms with more complementary inputs being more productive than those with fewer inputs. This will tend to increase average firm size in the economy and can potentially stifle competition by representing a barrier to entry for smaller, data-poor firms.

125. *See* Atl. Refin. Co. v. F.T.C, 381 U.S. 360, 361 (1965) (upholding as an unfair method of competition a sales-commission plan which was a classic example of using economic power in one market to destroy competition in another market).

126. For example, even if we could avoid Facebook and its advertising network, Facebook still tracks us whenever we visit the millions of websites and apps with a Facebook "Like" button or that use "Facebook Analytics" services. Data is transmitted to Facebook when we visit that third-party website or app, even before we see the "Like" button. The amount of data Facebook receives is staggering. Facebook received approximately one billion events per day from health apps alone on users, such as when someone opened the app, clicked, swiped, or viewed certain pages, and placed items into a checkout. With all that data, Facebook compiles some 200 "traits" attached to its 2.8 billion users' profiles. STUCKE, *supra* note 7, at 16–17; *see also* Natasha Singer, *GoodRx Leaked User Health Data to Facebook and Google, F.T.C. Says*, N.Y. TIMES (Feb. 1, 2023), https://www.nytimes.com/2023/02/01/business/goodrx-user-data-facebook-google.html.

127. *See generally* Press Release, European Data Protection Board, Facebook and Instagram decisions: "Important impact on use of personal data for behavioural advertising" (Jan. 12, 2023), https://edpb.europa.eu/news/news/2023/facebook-and-instagram-decisions-important-impact-use-personal-data-behavioural (deciding that Meta unlawfully processed personal data for behavioral advertising and that such advertising is not necessary for the performance of an alleged contract with Facebook and Instagram users); *see also* Sam Schechner, *Meta's Targeted Ad Model Faces Restrictions in Europe: EU Privacy Regulators Say Facebook and Instagram Shouldn't Use Their Terms of Service to Require Users to Accept Ads Based on Their Digital Activity*, WALL ST. J. (Dec. 6, 2022), https://www.wsj.com/articles/metas-targeted-ad-model-

(4) uses that data to unfairly gain a competitive position for other services or products.[128]

For example, Google Maps can collect users' geolocation data to accurately reflect current traffic conditions. But Google could not use the geolocation data for behavioral advertising. Nor could Google use the personal data to improve its other products and services, which are also subject to network effects, like providing more relevant search results and prompting users to review local restaurants, when such data leveraging: (1) puts data-poorer rivals, like Yelp and TripAdvisor, at an even greater competitive disadvantage; and (2) helps tip these other markets in the data-opolies' favor.

D. CONDUCT THAT VIOLATES THE SPIRIT OF AN ANTITRUST LAW

Besides conduct that violates or threatens to violate the antitrust laws, the term "unfair methods of competition" encompasses "trade practices which conflict with the basic policies of the Sherman and Clayton Acts even though such practices may not actually violate these laws."[129]

One example is when firms pay to be the default at critical access points in the digital economy. Knowing that individuals generally stick with the default option, the firm pays to be the default option to attain scale and tip the market in its favor. For example, Google paid Apple billions of dollars over 15 years to be the default search engine on Apple products. To secure these defaults, Google pays Apple on a "revenue share basis."[130] This is worse than Apple receiving a fixed sum for allowing Google to be the default. Why?

---

faces-restrictions-in-europe-11670335772?mod=hp_lead_pos1 (discussing the European Union privacy ruling that Facebook Platforms Inc. shouldn't require users to agree to personalized ads based on their online activity).

128. For example, a dominant French electricity provider used the personal data it collected as a regulated monopoly to compete in other unregulated markets. The competition agency found that the monopoly improperly used its customer data "to facilitate customer switching from regulated to unregulated offers, and to 'win back' customers who had switched to competing unregulated offers." The regulated monopoly had an unfair competitive advantage, the competition authority found, "since no database exists that would allow competitors to precisely locate gas consumers and know their consumption level, in order to propose them offers that are better suited to their profile." Press Release, Autorité de la Concurrence, Gas Market (Sept. 9, 2014), http://www.autoritedelaconcurrence.fr/user/standard.php?id_rub=592&id_article=2420.

129. F.T.C. v. Brown Shoe, 384 U.S. 316, 321 (1966); Fashion Originators' Guild Of Am. v. F.T.C., 312 U.S. 457, 463 (1941) (noting that if the purpose and practice of the defendant's action "runs counter to the public policy declared in the Sherman and Clayton Acts, the Federal Trade Commission has the power to suppress it as an unfair method of competition"); 2022 FTC UMC POLICY STATEMENT, *supra* note 25, at 13.

130. CMA FINAL REPORT, *supra* note 112, ¶ 3.107 n.132; *see also* Google Compl., *supra* note 51, ¶¶ 47, 175, 182.

Because the revenue sharing agreement aligns Apple's and Google's incentives.[131] Under this arrangement, if you search for something on your Safari browser, you probably use Google's search engine. And Apple gets a significant percentage of Google's monopoly revenues from search advertising. Therefore, the more people use Siri, Spotlight, or Google on the 1.4 billion Apple devices worldwide, the more personal data that Google collects, the more advertising revenue that this data helps generates, and the more money Apple receives as a result. And the monopoly profits are in the billions. In 2019, Google reportedly paid Apple $12 billion under this revenue sharing agreement, which is significant by itself and relative to Apple's 2019 net income of $55.256 billion.[132] By 2021, the amount Google paid Apple climbed to an estimated $15 billion.[133] Being the default on one's mobile phone can be more powerful since consumers are less likely to bypass the default when dealing with a small screen.

The default deprives rivals of access to users, data, economies of scale, and network effects. As a result, smaller, more privacy-friendly search engines cannot grow. To see why, as more people stick with the default search engine, the algorithm has more opportunities to learn: "[t]he greater the number of queries a general search service receives, the quicker it is able to detect a change in user behaviour patterns and update and improve its relevance."[134] Its more

131. Google Compl., *supra* note 51, ¶ 122 ("[B]y paying Apple a portion of the monopoly rents extracted from advertisers, Google has aligned Apple's financial incentives with its own.").

132. ACCC FINAL REPORT, *supra* note 113, at 10, 30 (recommending changes to search engine and internet browser defaults so that Google provides Australian users of Android devices with the same options being rolled out to existing Android users in Europe: the ability to choose their default search engine and default internet browser from a number of options); CMA FINAL REPORT, *supra* note 112, ¶¶ 3.106, 89, (finding that in 2019 Google paid Apple £1.2 billion for default positions in the United Kingdom alone, which represented over 17% of Google's total annual search revenues in the United Kingdom); Apple Inc., Annual Report (Form 10-K) (Oct. 30, 2019), https://s2.q4cdn.com/470004039/files/doc_financials/2019/ar/_10-K-2019-(As-Filed).pdf.

133. Johan Moreno, *Google Estimated to Be Paying $15 Billion to Remain Default Search Engine on Safari*, FORBES (Aug. 27, 2021), https://www.forbes.com/sites/johanmoreno/2021/08/27/google-estimated-to-be-paying-15-billion-to-remain-default-search-engine-on-safari/?sh=59151e56669.

134. ICN UNILATERAL CONDUCT WORKING GROUP, REPORT ON THE RESULTS OF THE ICN SURVEY ON DOMINANCE/SUBSTANTIAL MARKET POWER IN DIGITAL MARKETS 28 (2020), https://www.internationalcompetitionnetwork.org/wp-content/uploads/2020/07/UCWG-Report-on-dominance-in-digital-markets.pdf [hereinafter ICN STUDY]; Digital Markets Act, at ¶ 2 (among the characteristics of the core platform services are "extreme scale economies, which often result from nearly zero marginal costs to add business users or end users"); *Comm'n Decision of 27.6.2017 (AT.39740 - Google Search (Shopping))*, C(2017) 4444 final,

relevant search results will attract others to the search engine, and the positive feedback will continue.

This network effect is less pronounced for objective queries (such as what is the capital of Hungary), to which DuckDuckGo or Bing can respond. Rather, this network effect favors the dominant search engine on less common (or tail) inquiries.[135] About 15 to 20% of queries that search engines typically see daily are common (what search engines call "head" queries), and about 25 to 30% of the queries are uncommon ("tail") queries.[136] As we judge a search engine's performance on both common and uncommon queries, the more data a general search engine collects for rare tail queries, "the more users will perceive it as providing them the more relevant results for all types of queries."[137] With more users and more tail queries, the dominant search engine benefits from seeing what links its users click for these tail inquiries. Plus, with other personal data on the users, including their location, the algorithm can further improve the search results. Thus, as the U.K. competition authority found, the smaller search engines' "lack of comparable scale in click-and-query data is likely to be a key factor that limits [their] ability . . . to compete with Google."[138]

Google's and Apple's behavior conflicts with several basic policies of the Sherman and Clayton Acts, which sought to preserve economic freedom and the freedom for each business "to compete—to assert with vigor, imagination, devotion, and ingenuity whatever economic muscle it can muster."[139] Consequently, Google and Apple's agreement violates the spirit, if not the letter, of the Sherman and Clayton Acts in "completely shut[ting] out competitors, not only from trade in which they are already engaged, but from the opportunities to build up trade in any community where these great and powerful combinations are operating under this system and practice."[140]

¶ 287 (June 27, 2017) , https://ec.europa.eu/competition/antitrust/cases/dec_docs/39740/39740_14996_3.pdf [hereinafter Google Shopping case].

135. Google Shopping case, *supra* note 134, ¶ 288; CMA FINAL REPORT, *supra* note 112, ¶ 3.27; HOUSE REPORT, *supra* note 43, at 180 (noting how "in 2010, one Google employee observed, 'Google leads competitors. This is our bread-and-butter. Our long-tail precision is why users continue to come to Google. Users may try the bells and whistles of Bing and other competitors, but Google still produces the best results.'"); Colo. Google Compl., *supra* note 51, ¶ 91.

136. CMA FINAL REPORT, *supra* note 112, ¶ 3.68.

137. ICN STUDY, *supra* note 134, at 28.

138. CMA FINAL REPORT, *supra* note 112, ¶ 3.79.

139. United States v. Topco Assocs., Inc., 405 U.S. 596, 610 (1972).

140. Jefferson Parish Hosp. Dist. No. 2 v. Hyde, 466 U.S. 2, 10 n.15 (1984) (quoting H.R. Rep. No. 63-627, at 13 (1914)), abrogated by Illinois Tool Works Inc. v. Indep. Ink, Inc., 547 U.S. 28, (2006).

To promote economic freedom and make the digital economy more contestable, the FTC could enforce or regulate along the lines of the Digital Markets Act. To comply with § 5, the data-opoly must:

- *first,* allow users to easily change default settings on the gatekeeper's operating system, virtual assistant, and web browser;
- *second*, prompt users, when they first use that service to choose, from a list of the service providers available; and
- *third*, not make it unnecessarily complicated to unsubscribe from its service.[141]

Thus, individuals, not the data-opoly, would choose which search engine would be their default.

Moreover, the FTC can promulgate regulations to promote interoperability and data-portability to enable individuals to switch to rivals or multi-home easily.[142] Here, the benefits to individual privacy would be indirect but consequential in allowing more privacy-friendly alternatives to gain scale and compete.

E. EXPLOITATIVE BEHAVIOR

As our book *Competition Overdose* discusses, competition, at times, can be toxic.[143] One form of toxic competition is where companies seek to exploit, rather than help, customers.

Our book begins with the premise that consumers are not rational profit-maximizers with perfect willpower.[144] Many consumers rely on intuition rather than deliberative reasoning. They succumb to the temptations of instant gratification, misjudge the strength of their willpower, and overestimate their ability to detect manipulation and exploitation. As anyone who has ever overeaten, overspent, or otherwise succumbed to temptation (despite having

141. Digital Markets Act, art. 6 & ¶ 63.

142. *See, e.g.*, Digital Markets Act ¶ 59 (to promote switching and multi-homing, requiring gatekeepers to allow end users, as well as third parties authorized by an end user, "effective and immediate access to the data they provided or that was generated through their activity on the relevant core platform services of the gatekeeper," requiring that the data "be received in a format that can be immediately and effectively accessed and used by the end user or the relevant third party authorized by the end user to which the data is ported," and requiring gatekeepers to use appropriate and high quality technical measures, such as application programming interfaces, so that end users can freely port their data continuously and in real time).

143. *See generally* MAURICE E. STUCKE & ARIEL EZRACHI, COMPETITION OVERDOSE: HOW FREE MARKET MYTHOLOGY TRANSFORMED US FROM CITIZEN KINGS TO MARKET SERVANTS (2020) (identifying when competition can turn toxic, who is pushing this toxic competition, and what we can do to minimize or avoid this toxic competition).

144. *Id.* at 73–74.

the best intentions to the contrary) can confirm, few of us have the willpower or the rationality we think we do. As a result, competition can turn toxic when:

- Firms know how to identify and exploit their customers' weaknesses; competitors can tap into these "irrational moments" and exploit them to their benefit.
- Savvier consumers, who might know how to avoid the traps set for them, do not protect the weaker customers (for example, when savvier consumers benefit, to some extent, from the exploitation).
- Firms profit more from exploiting their customers' weaknesses than from helping them.

In these markets, few, if any, "angelic" companies may come to our aid because there is no advantage to their doing so. It may be too costly to educate the naive customers, and even if the firms succeed, there is no assurance that these customers, once educated, will stick with them and use their products. Eventually, competition encourages even once-angelic companies to exploit us.[145] Companies or managers who resist will lose business to those without moral qualms. Rather than a race to the top, companies compete in devising ever cleverer ways to exploit consumers' shortcomings—the result being that increasing competition delivers ever worse products and services to us.

Although the field of consumer protection law has developed over the past sixty years to curb this exploitation, these practices historically were condemned as unfair methods of competition. An early example is when candy manufacturers encouraged gambling among children.[146] To induce purchases, over forty candy manufacturers concealed in the wrapper the actual price for the candy (ranging from full price to free) and other prizes. Enticed by this element of chance, children switched away from those candy manufacturers who did not resort to this exploitative practice to those who did.

The defendant candy manufacturers argued in the resulting lawsuit, and the lower court agreed, that enticing children with gambling was not unfair because rivals could always resort to the same sales method.[147] Here, any candy manufacturer could maintain its competitive position simply by adopting this practice.[148] Indeed, the manufacturer might benefit as gambling would likely induce children to buy even more candy. Nor was the practice deceptive, nor

145. *Id.* at 78–87 (discussing drip pricing, and how Caesars Entertainment gave up on its efforts to warn consumers of suspect resort fees and joined the race to exploit).

146. F.T.C. v. R. F. Keppel & Bro., Inc., 291 U.S. 304, 308 (1934).

147. *Id.*

148. F.T.C. v. Sperry & Hutchinson Co., 405 U.S. 233, 243 (1972) (noting that in *Keppel* it "had no difficulty in sustaining the FTC's conclusion that the practice was 'unfair,' though any competitor could maintain his position simply by adopting the challenged practice").

was there any showing that any of the forty firms would monopolize the market. Thus, the defendants argued, and the lower court concluded, that the exploitative practice was not an unfair method of competition.

The Supreme Court disagreed. Unfair methods of competition included practices that tend to "take unfair advantage of the public."[149] The Court had little difficulty condemning this practice, which was "shown to exploit consumers, children, who [were] unable to protect themselves."[150] As the Court noted, a "method of competition which casts upon one's competitors the burden of the loss of business unless they will *descend* to a practice which they are under a powerful moral compulsion not to adopt, even though it is not criminal, was thought to involve the kind of unfairness at which the statute was aimed."[151]

Thus, using its authority under § 5, the FTC can place guardrails on data-collection practices that exploit consumers' behavioral weaknesses. One area to regulate is what's known as dark patterns.

A dark pattern is when a company manipulates, subverts, or impairs our autonomy, decision-making, or choices, often through our behavioral weaknesses.[152] The subject is a hot topic among policymakers. In 2021, the FTC brought together "researchers, legal experts, consumer advocates, and industry professionals to examine what dark patterns are and how they might affect consumers and the marketplace."[153] Among the topics discussed were "what laws, rules, and norms regulate the use of dark patterns" and "whether additional rules, standards, or enforcement efforts are needed to protect consumers."[154] In late 2021, the FTC issued "a new enforcement policy statement warning companies against deploying illegal dark patterns that trick or trap consumers into subscription services."[155] The policy statement focused

149. *Unfair Competition at Common Law and Under the Federal Trade Commission*, *supra* note 36, at 331.

150. *Keppel*, 291 U.S. at 313.

151. *Id.* (emphasis added).

152. Digital Services Act, at ¶ 67 (defining dark patterns as "practices that materially distort or impair, either on purpose or in effect, the ability of recipients of the service to make autonomous and informed choices or decisions. Those practices can be used to persuade the recipients of the service to engage in unwanted behaviours or into undesired decisions which have negative consequences for them").

153. *Dark Patterns Workshop*, FED. TRADE COMM'N (2021), https://www.ftc.gov/media/73487.

154. FTC to Hold Virtual Workshop Exploring Digital Dark Patterns, 2021 WL 717222 (F.T.C. Feb. 24, 2021).

155. Press Release, Fed. Trade Comm'n, FTC to Ramp up Enforcement against Illegal Dark Patterns that Trick or Trap Consumers into Subscriptions (Oct. 28, 2021), https://www.ftc.gov/news-events/news/press-releases/2021/10/ftc-ramp-enforcement-against-

on negative options, where companies use a consumer's silence or inaction as acceptance of an offer. So, a consumer, enticed by a free trial offer of animal kingdom cards for their children, might find boxes of cards accumulating outside their door with a hefty bill attached.

One area for the FTC to regulate is the use of dark patterns to steer individuals away from privacy-friendly options to collect more of their data.[156] In its 2018 review, the Norwegian Consumer Council investigated how Facebook, Microsoft, and Google deliberately manipulated privacy settings to deter individuals from protecting their privacy.[157] These data-opolies give users the illusion of control while making it harder for them to protect their privacy. As the Australian Competition & Consumer Commission (ACCC) likewise found, digital platforms "tend to understate to consumers the extent of their data collection practices while overstating the level of consumer control over their personal user data."[158] Why? When we have the illusion of control, we paradoxically are likelier to undertake greater risks in sharing our private information. As the Norwegian Consumer Council noted, "[t]he combination of privacy intrusive defaults and the use of dark patterns, nudge users of Facebook and Google, and to a lesser degree Windows 10, toward the least privacy friendly options to a degree that we consider unethical."[159]

Consumer Reports and Epic provide another example of dark patterns. After California's 2018 privacy statute went into effect, Californians had the right to opt-out of the sale of their data. In response,

> many companies have developed complicated and onerous opt-out processes. Some companies ask consumers to go through several different steps to opt out. In some cases, the opt outs are so complicated that they have actually prevented consumers from stopping the sale of their information.[160]

---

illegal-dark-patterns-trick-or-trap-consumers-subscriptions; FED. TRADE COMM'N, ENFORCEMENT POLICY STATEMENT REGARDING NEGATIVE OPTION MARKETING (2021), https://www.ftc.gov/system/files/documents/public_statements/1598063/negative_option_policy_statement-10-22-2021-tobureau.pdf.

156. *Fact Sheet on the FTC's Commercial Surveillance and Data Security Rulemaking*, FED. TRADE COMM'N (2022), https://www.ftc.gov/legal-library/browse/federal-register-notices/commercial-surveillance-data-security-rulemaking (noting how companies are "increasingly employ[ing] dark patterns or marketing to influence or coerce consumers into choices they would otherwise not make, including purchases or sharing personal information").

157. *Deceived by Design*, NORWEGIAN CONSUMER COUNCIL (Jun. 27, 2018), https://fil.forbrukerradet.no/wp-content/uploads/2018/06/2018-06-27-deceived-by-design-final.pdf.

158. ACCC FINAL REPORT, *supra* note 112, at 23.

159. NORWEGIAN CONSUMER COUNCIL, *supra* note 157, at 3.

160. CR/Epic Report, *supra* note 14, at 23.

Thus, companies seek an advantage over rivals by designing privacy out of their system and nudging us "to make privacy-intrusive selections by appealing to certain psychological or behavioural biases, using design features such as privacy-intrusive defaults or pre-selections."[161] As the influential House Report on the digital economy noted, "[t]here appears to be a substantial market failure where dark patterns are concerned—what is good for e-commerce profits is bad for consumers."[162]

Some policymakers have already taken steps to prevent these exploitative practices. In a first for any statute, the California Privacy Rights Act of 2020 states that any agreement "obtained through the use of dark patterns does not constitute consent."[163] California also promulgated regulations prohibiting businesses from using "a method that is designed with the purpose or has the substantial effect of subverting or impairing a consumer's choice to opt-out."[164] Europe's Digital Markets Act obligates gatekeepers not to "design, organise or operate their online interfaces in a way that deceives, manipulates or otherwise materially distorts or impairs the ability of end users to freely give consent."[165] Likewise, Europe's Digital Services Act prohibits the dominant online platforms and interfaces from using these "dark patterns."[166] There are also bills in Congress to crack down on dark patterns.[167]

Dark patterns do not benefit society. They are by design exploitative, seeking to use the insights of behavioral economics to manipulate our decisions and behavior in ways that undermine our well-being. Accordingly, through rulemaking and enforcement, the FTC should void any consent for

161. ACCC FINAL REPORT, *supra* note 112, at 374; *see also* CMA FINAL REPORT, *supra* note 112, ¶ 4.173 (finding that the platforms' choice architectures rather than remediate biases are more likely to exacerbate biases).

162. HOUSE REPORT, *supra* note 43, at 53.

163. CAL. CIV. CODE § 1798.140(h); *see also* The Colorado Privacy Act (COLO. REV. STAT. § 6-1-1303(5)(c) (agreement obtained through dark patterns do not constitute consent); CAL. CIV. CODE §§ 56.18–56.186 (California Genetic Information Privacy); Connecticut Act Concerning Personal Data Privacy and Online Monitoring, Public Act No. 22-15, § 1(1)(6) (2022) (same).

164. CAL. CODE REGS. tit. 11, § 999.315(h) (2021).

165. Digital Markets Act ¶ 37.

166. Regulation (EU) 2022/2065 of the European Parliament and of the Council of 19 October 2022 on a Single Market for Digital Services and amending Directive 2000/31/EC (Digital Services Act), O.J. (L 277) 1 EU, at ¶ 67 (prohibiting providers of intermediary services "from deceiving or nudging recipients of the service and from distorting or impairing the autonomy, decision-making, or choice of the recipients of the service via the structure, design or functionalities of an online interface or a part thereof").

167. *See, e.g.*, Online Privacy Act of 2021, H.R. 6027, 117th Cong. § 209 (1st Sess. 2021) (prohibiting a covered entity from intentionally using dark patterns in providing notice, obtaining consent, or maintaining a privacy policy as required by the proposed statute).

data obtained through dark patterns and prohibit companies from using these dark patterns to obtain or use our data. This would include exploitative design choices to direct individuals to the less privacy-friendly option, which primarily benefits the company, such as giving the non-privacy option far more prominence (such as a large box for "I consent," while hiding the privacy-friendly option in small print) or making the privacy-friendly option more cumbersome or time-consuming (such as requiring the individuals to click through multiple links to opt-out of collecting their data).

As we have seen from this Part, the existing categories of unfair methods of competition can address many unfair data collection and surveillance practices that damage competition, consumer autonomy, and privacy. But the last category involving exploitative behavior marks a significant shift in thinking: it reflects the understanding that more competition, absent the regulatory guardrails, would not necessarily curb the exploitative practice. Companies use dark patterns to extract our data because if they don't, they are at a competitive disadvantage to those who do. If anything, more competition would likely lead to more ingenuous ways to manipulate our behavior. Thus, the government has a responsibility to prevent exploitative practices like dark patterns.

As the next Part explores, a more effective way to prevent exploitative, deceptive, and other unfair methods of competition is to eliminate the economic incentive to engage in that behavior. And that requires the FTC to tackle the primary source of this privacy degradation in the digital economy, namely behavioral advertising.

IV. RACE TO THE BOTTOM IN THE SURVEILLANCE ECONOMY

The problem with data-opolies is more than just their power. It is also about their incentives. They engage in intrusive surveillance and extract too much data to better predict and manipulate our behavior and emotions. The prevailing belief is that increasing competition will limit the data-opolies' ability to extract our data and exploit us. We can see this belief in Europe's Digital Markets Act. To combat the gatekeepers' collecting and accumulating large amounts of data from end users, the DMA seeks to promote "an adequate level of transparency of profiling practices employed by gatekeepers."[168] The

168. Digital Markets Act, at ¶ 72.

belief is that more transparency will increase competition,[169] which would improve privacy.[170]

But is this true? Instead of imposing all these obligations on the data-opolies, suppose antitrust enforcers just broke them up. Just like the United States did with the Standard Oil and AT&T monopolies. Would our privacy improve? Probably not.

Another category of toxic competition addressed in *Competition Overdose* is the race to the bottom.[171] To distinguish between good and bad competition, between races to the top and races to the bottom, one must ask whether the competitors' individual and collective interests are aligned. If all the competitors do the same thing, do they (and society) end up collectively better off—or worse off?

A. HISTORIC UNDERSTANDING OF INCENTIVES

One of our book's examples involves a hockey player who foregoes wearing a helmet for a slight competitive advantage. Other players will go helmetless, and in the end, none would enjoy a competitive advantage. Instead, they would be collectively worse off (with a greater risk of head trauma).[172] So, when a rival seeks an edge over its competitors by employing a particular method of competition, one must consider what would happen if others followed the rival's lead and took similar measures. If everyone ends up worse off, with no advantage going to anyone, they are in a race to the bottom. Accordingly, the method of competition is unfair.

The FTC Act sought to deter these "innumerable schemes whereby they took unfair advantage of their rivals, and the courts were forced to realize the necessity of protecting a man's business from the sharp practices of his competitor."[173]

One example is deceptive conduct. As the Restatement notes, courts may deem it unfair when firms gain a competitive advantage by failing "to disclose to prospective consumers particular information that is crucial to an intelligent

169. *Id.* (increasing transparency will put "external pressure on gatekeepers not to make deep consumer profiling the industry standard, given that potential entrants or startups cannot access data to the same extent and depth, and at a similar scale").

170. *Id.* (by shining a light at the data-opolies' data hoarding and profiling, rivals can "differentiate themselves better through the use of superior privacy guarantees").

171. STUCKE & EZRACHI, *supra* note 143, at 3–40.

172. *Id.* at 4–5.

173. *Unfair Competition at Common Law and Under the Federal Trade Commission Source*, *supra* note 37, at 328.

purchasing decision."[174] Consider a manufacturer that labeled its underwear as wool, including Merino Wool, when the clothing actually contained little wool.[175] This constituted an unfair method of competition because it was calculated to deceive the public and disadvantage the truthful sellers.[176] The honest manufacturers, Justice Brandeis observed, might also resort to deceptive labels or be forced out.[177] Once most of the sellers resort to fraud, none of them benefit, and a lemon market results.[178]

Antitrust scholar Robert Steiner, the former president of the Kenner Products toy company, described his concerns about the industry self-regulation of toy commercials in the 1960s and 1970s.[179] Originally favoring industry self-policing, he feared the toxic consequences of deceptive advertising. Absent regulation, some toy manufacturers would air deceptive ads, which would pull down the toy industry. Unless his company matched "the exaggerations and sometimes the outright deceptions of certain competitors, our commercials might not be exciting enough to move our toys off the shelves."[180] He foresaw bad commercials driving out the good ones, rendering TV advertising relatively ineffective. Consequently, it is uncontroversial that the FTC Act, common law, and many other laws prohibiting deceptive conduct, seek to halt this race to the bottom. Essentially, the law imposes guardrails to channel the competition into a race to the top. Now, if others followed the rival's lead (say, nondeceptive advertising), the competitors and society would be better off.

B. THE INCENTIVES OF BIG TECH: BEHAVIORAL ADVERTISING

The FTC already targets deceptive privacy statements, most notably the $5 billion fine imposed on the recidivist Facebook. But, as the dissenting Commissioners observed, the penalty and corporate reshuffling required

174. RESTATEMENT (THIRD) OF UNFAIR COMPETITION § 1, cmt. g, at 10 (AM. LAW. INST. 1995).

175. F.T.C. v. Winsted Hosiery Co., 258 U.S. 483, 490 (1922).

176. *Id.* at 493.

177. *Id.*

178. *Id.* at 494 ("The honest manufacturer's business may suffer, not merely through a competitor's deceiving his direct customer, the retailer, but also through the competitor's putting into the hands of the retailer an unlawful instrument, which enables the retailer to increase his own sales of the dishonest goods, thereby lessening the market for the honest product."); George A. Akerlof, *The Market for "Lemons": Quality Uncertainty and the Market Mechanism*, 84 Q.J. ECON. 488, 495 (1970) (noting that the cost of dishonesty includes "loss incurred from driving legitimate business out of existence").

179. Robert L. Steiner, *Double Standards in the Regulation of Toy Advertising*, 56 CINCINNATI L. REV. 1259, 1264 (1988).

180. *Id.*

under the consent decree did not change the company's incentives. The settlement failed to address the underlying cause of Facebook's exploitative behavior, namely, its behavioral advertising-dependent business model. This failure, for the two dissenting FTC commissioners, was a deal-breaker. Commissioner Rebecca Kelly Slaughter could not "view the order as adequately deterrent without both meaningful limitations on how Facebook collects, uses, and shares data and public transparency regarding Facebook's data use and order compliance."[181] As Commissioner Rohit Chopra noted, "Facebook's violations were a direct result of the company's behavioral advertising business model," and the FTC's settlement did "little to change [Facebook's] business model or practices that led to the recidivism."[182] But for three FTC commissioners, any substantive data and privacy protections were beyond the agency's power: "Our 100-year-old statute does not give us free rein to impose these restrictions."[183]

Of course, no statute can (or should) give an administrative agency free rein to do whatever it desires. However, the majority in *Facebook* never explained why the FTC could not curb the race to the bottom engendered by behavioral advertising as an "unfair method of competition."

So, while the FTC could try to regulate all the manipulative means to attract, addict, and extract value from individuals, the better route, as *Breaking Away* examines, is to examine incentives.[184]

Advertising generally skews incentives, as the founders of Google recognized. In 1998, when their search engine was not dependent on advertising revenues, Google's founders Sergey Brin and Lawrence Page predicted that "advertising funded search engines will be inherently biased towards the advertisers and away from the needs of the consumers."[185] They laid out how advertising can distort a search engine's incentives and warned of

181. FED. TRADE COMM'N, DISSENTING STATEMENT OF COMMISSIONER REBECCA KELLY SLAUGHTER 2 (2019), https://www.ftc.gov/system/files/documents/public_statements/1536918/182_3109_slaughter_statement_on_facebook_7-24-19.pdf.

182. FED. TRADE COMM'N, DISSENTING STATEMENT OF COMMISSIONER ROHIT CHOPRA 1 (2019), https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf [hereinafter Chopra *Facebook* Dissent].

183. FED. TRADE COMM'N, STATEMENT OF CHAIRMAN JOE SIMONS AND COMMISSIONERS NOAH JOSHUA PHILIPS AND CHRISTINE S. WILSON 6 (2019), https://www.ftc.gov/system/files/documents/public_statements/1536946/092_3184_facebook_majority_statement_7-24-19.pdf.

184. STUCKE, *supra* note 7, at 192–96; *see also* EZRACHI & STUCKE, *supra* note 7, at 203–4 (exploring importance of incentives in the path of innovation).

185. Sergey Brin & Lawrence Page, *The Anatomy of a Large-Scale Hypertextual Web Search Engine*, 30 COMPUT. NETWORKS & ISDN SYS. 107, Appendix A (1998).

the "insidiousness" of the resulting search bias. Given these risks, the young entrepreneurs believed "that it is crucial to have a competitive search engine that is transparent and in the academic realm."[186]

As *Breaking Away* explores, behavioral adverting skews incentives even more. Data is collected about us, but not for us. Behavioral advertising has evolved beyond predicting what each of us wants into manipulating our behavior. In using emotional marketing to trigger our desires—whether to buy a particular product, endorse it to friends, or create a community around the brand—we are not the customer but the target.

Emotional marketing is a game-changer for advertising. As the Facebook investor and advisor Roger McNamee noted, Google and Facebook help advertisers "to exploit the emotions of users in ways that increase the likelihood that they purchase a specific model of car or vote in a certain way."[187] As Facebook's patented "emotion detection" tools suggest, the ultimate aim is to detect and appeal to our fears and anger; to pinpoint our children and us when we feel "worthless," "insecure," "defeated," "anxious," "silly," "useless," "stupid," "overwhelmed," "stressed," and "a failure."[188] Essentially, we are the lab rats as we enter a marketplace of behavioral discrimination: companies compete to decipher our personality; to find whether we have an internal/external locus of control, our willingness to pay, and our impulsivity.

As WhatsApp's founders, quoting the movie Fight Club, explained:

> "Advertising has us chasing cars and clothes, working jobs we hate so we can buy shit we don't need."
>
> . . .
>
> Advertising isn't just the disruption of aesthetics, the insults to your intelligence and the interruption of your train of thought. At every company that sells ads, a significant portion of their engineering team spends their day tuning data mining, writing better code to collect all your personal data, upgrading the servers that hold all the

186. *Id.*

187. ROGER MCNAMEE, ZUCKED: WAKING UP TO THE FACEBOOK CATASTROPHE 69 (2019).

188. Michael Reilly, *Is Facebook Targeting Ads at Sad Teens?*, MIT TECH. REV. (May 1, 2017); McNamee, *supra* note 187, at 69; Sam Levin, *Facebook Told Advertisers It Can Identify Teens Feeling "Insecure" and "Worthless,"* GUARDIAN (May 1, 2017), https://www.theguardian.com/technology/2017/may/01/facebook-advertising-data-insecure-teens.

> data and making sure it's all being logged and collated and sliced and packaged and shipped out.[189]

FTC Commissioner Chopra noted how Facebook's behavioral advertising business model is the root cause of its widespread and systemic privacy problems: "Behavioral advertising generates profits by turning users into products, their activity into assets, their communities into targets, and social media platforms into weapons of mass manipulation. We need to recognize the dangerous threat that this business model can pose to our democracy and economy."[190]

In this arms race, where the data-opolies control most of the data and reap most of the profits, many websites and apps cannot unilaterally opt-out. Many websites and apps are ostensibly free. To monetize their efforts, they must attract and sustain our attention while gathering data to manipulate and target us with behavioral ads. Consequently, as *Breaking Away* explores, the ethical websites and apps face a Hobson's choice—(1) opt-out of behavioral advertising and watch their ad revenues plummet—on average by 70%, which can effectively kill their business;[191] (2) change to a freemium subscription model (which puts them at a significant competitive disadvantage to the free apps and websites); or (3) stick with behavioral advertising revenues until enough dedicated followers are willing to pay for their app or service. Most cannot afford to opt-out of this toxic competition. They must continue finding ways to profile us, surveil us, and manipulate our behavior. To attract and drive up the bidding for their advertising space, they effectively sell us (and our ability to be manipulated).

Advertisers recognize that most of us do not want this intrusive surveillance.[192] To realize better value from their campaigns and outcompete rivals, however, advertisers are encouraged to rely on emotion analytics and facial coding, where algorithms process our facial expressions and voice to

189. HOUSE REPORT, *supra* note 43, at 157 (quoting *Why We Don't Sell Ads*, WHATSAPP (June 18, 2012), https://blog.whatsapp.com/why-we-don-t-sell-ads).

190. Chopra *Facebook* Dissent, *supra* note 182, at 2.

191. CMA FINAL REPORT, *supra* note 112, ¶ 5.326 (estimating that U.K. publishers "earned around 70% less revenue when they were unable to sell personalised advertising but competed with others who could"); *see also* FED. TRADE COMM'N, DISSENTING STATEMENT OF COMMISSIONER REBECCA KELLY SLAUGHTER IN THE MATTER OF GOOGLE LLC AND YOUTUBE LLC 2–3 (2019) (noting how both YouTube and the channels have a strong financial incentive to use behavioral advertising, so while "YouTube has long allowed channel owners to turn off default behavioral advertising and serve instead contextual advertising that does not track viewers . . . vanishingly few content creators would elect to do so, in no small part because they receive warnings [from Google] that disabling behavioral advertising can 'significantly reduce your channel's revenue'").

192. CMA FINAL REPORT, *supra* note 112, ¶ 4.68.

manipulate our behavior.[193] Even if the ethical advertiser finds this surveillance and manipulation morally repugnant, many cannot afford to opt-out, and a race to the bottom ensues.

The disturbing realization is that this toxic competition would exist even without the data-opolies. Millions of free websites and apps compete to attract millions of advertisers to target billions of users every minute of every day with behavioral ads. To succeed in this competition, websites and apps need detailed, up-to-date data about us, which in turn increases the demand to track us online and offline.

Because behavioral advertising skews the market participants' incentives, we have a market failure. As two officials from the International Monetary Fund explained, "An implication is that a market for data lacking sufficient user control rights—where data collectors do as they please with the data they collect—is likely to lead to excessive data collection and too little privacy."[194] Without adequate privacy protections, even robustly competitive markets will not function in ways to promote our privacy. As the IMF officials add,

> To the extent that privacy is not internalized in the economic decisions of data collectors and processors, the market will tend toward the collection of excessive personal data and insufficient protection of privacy. For the market for data to internalize this externality, the rights of data subjects must be adequately attributed.[195]

Therefore, laws are ultimately needed to correct the fundamental misalignment of incentives caused by behavioral advertising. This is more challenging than one might think. As Alastair Mactaggart, one of the drivers of California's two recent privacy statutes, observed:

> If you think about our other fundamental rights as a country, no one is spending millions and millions of dollars trying to undermine the First Amendment or the freedom of religion. But people are actually spending hundreds of millions of dollars trying to undermine privacy because there's so much money in it for corporations.[196]

193. SHOSHANA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM 284 (2019); *see also* Sophie Kleber, *Three Ways AI Is Getting More Emotional*, *in* ARTIFICIAL INTELLIGENCE: THE INSIGHTS YOU NEED FROM HARVARD BUSINESS REVIEW 142 (Thomas H. Davenport et al., eds. 2019); EZRACHI & STUCKE, *supra* note 7, at 101–22.

194. Carrière-Swallow & Haksar, *supra* note 124, at 5.

195. *Id.* at 14.

196. Natasha Singer, *The Week in Tech: Why Californians Have Better Privacy Protections*, N.Y. TIMES (Sept. 27, 2019), https://www.nytimes.com/2019/09/27/technology/the-week-in-tech-why-californians-have-better-privacy-protections.html.

That is especially true when the data-opolies, including Apple through its deal with Google, reap billions of dollars from behavioral advertising each quarter.[197]

C. POSSIBLE FTC REFORMS

The FTC can help realign the incentives by curbing behavioral advertising (by at least requiring users to opt into personalized advertising). The FTC is not regulating the content of advertising per se, but the use of personal data to profile individuals and manipulate behavior to maximize engagement and advertising revenues.

So, the FTC regulation would implement data minimization policies, where personal data can be collected and used only when it is necessary to provide the product and service (which would not include behavioral advertising purposes). Companies can continue to advertise, as they have done for centuries, including contextual advertising, but not use personal data for psychographic profiles to predict and manipulate behavior.

The FTC already limits behavioral advertising under the Children's Online Privacy Protection Act (COPPA). In 2012, the FTC amended the definition of personal information to include "persistent identifiers," which can be used to recognize users over time and across different websites or online services. As a result, under COPPA, parental notice and consent are required before an operator uses a persistent identifier for behavioral advertising.[198]

---

197. For example, for the first six months of 2022, $110.949 billion of Google's $137.7 billion in revenues came from advertising, which generated most of the company's $32 billion in profits for that period. *See* Alphabet Inc., Quarterly Report for the Quarterly Period Ended June 30, 2022 (Form 10-Q) (July 26, 2022), at 11, 41, https://abc.xyz/investor/static/pdf/20220726_alphabet_10Q.pdf?cache=de538c8. For that same period, nearly all of Meta's $56.7 billion in revenues and $14 billion in profits came from advertising. Meta Platforms, Inc., Quarterly Report for the Quarterly Period Ended June 30, 2022 (Form 10-Q) (July 27, 2022), at 14, https://d18rn0p25nwr6d.cloudfront.net/CIK-0001326801/f657a197-fe9f-4414-81d3-b56c02701886.pdf. Likewise, for that same period, Amazon made over $16 billion in sales relating to its advertising services. The company did not break out its net profits from its advertising business. *See* Amazon.com Inc., Quarterly Report for the Quarterly Period Ended June 30, 2022 (Form 10-Q) (July 28, 2022), at 20, https://www.sec.gov/Archives/edgar/data/1018724/000101872422000019/amzn-20220630.htm. For the three months ending March 31, 2022, Microsoft's search and news advertising revenues exceeded $2.9 billion. *See* Microsoft Corp., Quarterly Report for the Quarterly Period Ended March 31, 2022 (Form 10-Q) (Apr. 26, 2022), at 31, https://www.sec.gov/Archives/edgar/data/789019/000156459022015675/msft-10q_20220331.htm.

198. Press Release, Fed. Trade Comm'n, FTC Strengthens Kids' Privacy, Gives Parents Greater Control Over Their Information by Amending Childrens Online Privacy Protection Rule (Dec. 19, 2012), https://www.ftc.gov/news-events/news/press-releases/2012/12/ftc-strengthens-kids-privacy-gives-parents-greater-control-over-their-information-amending-childrens.

However, the surveillance apparatus is not used solely to get us to buy things we don't need at the highest price we are willing to pay. Competition in the digital economy is also for attention. Under the guise of personalizing and improving their services, firms will continue to design their apps and products like slot machines to attract and addict us.[199] Thus, limiting behavioral advertising, by itself, would be inadequate. Gaming apps and firms left with contextual advertising would still have the incentive to appeal to our emotions to addict us.

Policymakers cannot afford to ignore attention markets. But regulating attention markets has significant implications for free speech and public discourse. The aim of any engrossing book, movie, podcast, play, or opera, after all, is to engage us.

Consequently, the FTC enforcement and regulations could entail both: (1) a data minimization component, which would limit companies' ability to collect and use personal data to that which is necessary to provide the product and service, and behavioral advertising would not be deemed a necessary purpose; and (2) providing individuals the right to avoid being profiled, having their data amalgamated with other data collected elsewhere by the company or third-parties, and receiving personalized recommendations if they so choose.

For example, an individual can opt-out of YouTube recommending videos based on the personal data Google has collected about that person. Both components would give individuals the right, without being penalized, to limit at the onset what data is collected about them and for what purpose. Indeed, the data minimization rule is less intrusive than attempting to regulate all the techniques to manipulate us. Companies might still design their apps as slot machines, but they could not design the perfect slot machine to addict you in particular.

As *Breaking Away* discusses in depth the pros and cons of this proposal, Part V will address several additional concerns if the FTC sought to curb, if not extinguish, the surveillance economy through its rulemaking authority.

V. POTENTIAL CONCERNS

The data-opolies have spent millions of dollars lobbying against privacy and antitrust reform,[200] and as of late 2023, they were winning in the United

199. *See* EZRACHI & STUCKE, *supra* note 7, at 101–20.

200. *See, e.g.*, Anna Edgerton & Emily Birnbaum, *Big Tech's $95 Million Spending Spree Leaves Antitrust Bill on Brink of Defeat*, BLOOMBERG LAW (Sept. 6, 2022), https://www.bloomberg.com/news/articles/2022-09-06/tech-giants-spree-leaves-antitrust-bill-on-brink-of-defeat?leadSource=uverify%20wall (reporting how Google, Apple, Amazon.com, and Meta and their

States. They will likely challenge any FTC regulation to curb unfair data collection and surveillance practices that damage competition, consumer autonomy, and consumer privacy. Although they could challenge any of the proposed rules outlined in Part IV, they would have the greatest incentive to challenge any rules that prohibit (or require consumers to opt into) behavioral advertising. There is simply too much money at stake. Moreover, restricting behavioral advertising may not neatly fall within any of the existing categories of unfair methods of competition. So, the FTC restrictions on behavioral advertising may be more vulnerable to attack. This Part addresses four issues: (1) whether the FTC has authority to promulgate rules involving unfair methods of competition, (2) whether an FTC rule banning (or require consumers to opt into) behavioral advertising would run afoul of the Supreme Court's "major questions doctrine," as recently outlined in *West Virginia v. EPA*, (3) whether an FTC rule restricting behavioral advertising would run afoul of the First Amendment, and (4) whether the FTC should defer to Congress for policies that would affect a multi-billion dollar economy.

A. CAN THE FTC PROMULGATE RULES INVOLVING UNFAIR METHODS OF COMPETITION?

Opponents to the FTC regulations might argue that the agency has exercised its authority over unfair methods of competition through litigation rather than rulemaking. It would be hard to fathom why Congress imposed multiple hurdles for regulating unfair and deceptive acts and practices if the FTC could circumvent them through rulemaking under unfair methods of competition.

While the Commission has been more active in promulgating rules to prohibit deceptive and otherwise fraudulent practices, as Judge Richard Posner observed, it did promulgate one rule in 1967 to prohibit an antitrust violation:

> And that rule was of the simplest kind; it forbade the discriminatory provision of advertising allowances. See section 2(d) of the Clayton Act, as amended by the Robinson-Patman Act, 15 U.S.C. § 13(d); 16 C.F.R. Part 412 (Trade Regulation Rule Against Discriminatory Practices in Men's and Boys' Tailored Clothing Industry); 16 C.F.R. Ch. 1, at pp. 4–5 (table of contents of Subchapter D, Trade Regulation Rules). Although the Commission has long been urged to do more in the way of antitrust rulemaking, see, e.g., Elman, *Rulemaking Procedures in the FTC's Enforcement of the Merger Law*, 78

trade groups have poured almost $95 million into lobbying since 2021 to derail the American Innovation and Choice Online Act).

> Harv. L. Rev. 385 (1964), the urgings have fallen largely on deaf ears.[201]

The year after that rule was promulgated, the Supreme Court decided the case of *F.T.C. v. Fred Meyer, Inc.*[202] Notably, the Court did not question the FTC's ability to regulate unfair methods of competition. "In that opinion," the FTC noted, "the Court suggested that the Commission might wish to expand on earlier guidance and issue detailed guidelines to promotional allowances" under the Robinson-Patman Act.[203] The FTC accepted this invitation by publishing the "Fred Meyer Guides," which "set out general standards for promotional allowances, applicable to all industries."[204] These Fred Meyer Guides were "revised as needed to keep them current, most recently in 1990."[205]

Next, in 1973, the D.C. Circuit in *National Petroleum Refiners Association v. F.T.C.*, affirmed the Commission's authority to regulate. The language of § 6(g) of the FTC Act "is as clear as it is unlimited": "The Commission shall also have power . . . to make rules and regulations for the purpose of carrying out the provisions of [§ 5]."[206] The court noted that the Commission "is a creation of Congress, not a creation of judges' contemporary notions of what is wise policy"; thus, the "extent of [the FTC's] powers can be decided only by considering the powers Congress specifically granted it in the light of the statutory language and background."[207] Since the FTC Act was clear, the D.C. Circuit's conclusion was "not disturbed by the fact that the agency itself did not assert the power to promulgate substantive rules until 1962 and indeed indicated intermittently before that time that it lacked such power."[208] The FTC could use its rulemaking "to carry out what the Congress agreed was among its central purposes: expedited administrative enforcement of the

---

201. United Air Lines, Inc. v. C.A.B., 766 F.2d 1107, 1118 (7th Cir. 1985).

202. 390 U.S. 341 (1968).

203. Trade Regulation Rule: Discriminatory Practices in Men's and Boys' Tailored Clothing Industry, 16 C.F.R. § 412 (1967); *see also Fred Meyer*, 390 U.S. at 358 ("Nothing we have said bars a supplier, consistently with other provisions of the antitrust laws, from utilizing his wholesalers to distribute payments or administer a promotional program, so long as the supplier takes responsibility, under rules and guides promulgated by the Commission for the regulation of such practices, for seeing that the allowances are made available to all who compete in the resale of his product.").

204. Trade Regulation Rule: Discriminatory Practices in Men's and Boys' Tailored Clothing Industry, 16 C.F.R. § 412 (1967).

205. The FTC in 1994 repealed its antitrust rule, as it was unnecessary with its Fred Meyer Guides in place. *Id.*

206. 482 F.2d 672, 693 (D.C. Cir. 1973).

207. *Nat'l Petroleum Refiners*, 482 F.2d at 674.

208. *Id.* at 693.

national policy against monopolies and unfair business practices."[209] Since § 6(g) plainly authorizes substantive rulemaking by the FTC for unfair methods of competition, "and nothing in the statute or in its legislative history precludes its use for this purpose," the D.C. Circuit upheld the Commission's rulemaking authority.[210]

Thereafter, when adding the rulemaking procedures in Magnuson-Moss, Congress specifically noted the rule at issue in *National Petroleum Refiners,*[211] and recognized the FTC's power to promulgate it.[212] Moreover, Congress noted that its Magnuson-Moss procedures "shall not affect any authority of the Commission to prescribe rules (including interpretive rules), and general statements of policy, with respect to unfair methods of competition in or affecting commerce."[213] This was a deliberate choice.[214] Consequently, both Congress and the courts have affirmed the FTC's substantive rulemaking authority for unfair methods of competition.[215]

209. *Id.*

210. *Id.*

211. Namely the Commission's rule declaring that failure to post octane rating numbers on gasoline pumps at service stations was an unfair method of competition and an unfair or deceptive act or practice. *Nat'l Petroleum Refiners*, 482 F.2d at 674.

212. S. REP. NO. 93-1408 at 7763–64 (1974) (Conf. Rep.):

> In an otherwise valid trade regulation rule the Commission may specify what must be done in order to avoid engaging in an unfair or deceptive practice. For example, in the present Commission rule relating to "octane rating," the Commission required that certain testing procedures be followed in order to determine what octane rating should be posted on gasoline pumps. The conferees intend that the Commission may continue to specify such matters in rules which are otherwise valid under Section 18. It should be noted, however, that inasmuch as such requirements are a part of the rule, they are subject to judicial review in the same manner as is the portion of the rule which defines the specific act or practice which is unfair or deceptive.

213. 15 U.S.C. § 57a.

214. S. REP. NO. 93-1408, at 7763–64 (1974) (Conf. Rep.) (noting that the conference added "a new section 18 to the Federal Trade Commission Act which would codify the Commission's authority to make substantive rules for unfair or deceptive acts or practices in or affecting commerce" but that the conference substitute did "not affect any authority of the FTC under existing law to prescribe rules with respect to unfair methods of competition in or affecting commerce").

215. Justin (Gus) Hurwitz, *Chevron and the Limits of Administrative Antitrust*, 76 U. PITT. L. REV. 209, 235 (2014); *see also* Chopra & Khan, *supra* note 23, at 375–79.

Regardless, some might debate this.[216] Additionally, opponents of the FTC's rulemaking now have a stronger weapon, namely, the Supreme Court's Major Questions Doctrine.

B. WOULD THE FTC'S RULEMAKING RUN AFOUL OF THE SUPREME COURT'S "MAJOR QUESTIONS DOCTRINE"?

Even before the Court's 2022 *EPA* decision, an FTC Commissioner expressed the risk of the Court striking down the FTC rulemaking under its resurrected non-delegation doctrine:

> [I]t's very clear that the justices are interested in getting back into the nondelegation business. How far they will go, what they cut I think remains to be seen. But it could have a real impact on at least what we understand today—or what the agencies understand today—as their regulatory power.[217]

Opponents will certainly rely on *West Virginia v. EPA* to strike down any FTC regulation of "unfair methods of competition." That decision involved the EPA's Clean Power Plan, which never went into effect, as it was immediately challenged. Moreover, intervening market forces caused the power industry to meet the Plan's environmental targets, so the Plan was for all purposes "obsolete."[218] There were, in effect, no balls or strikes to call here.[219] Nevertheless, that did not stop the Court from using the case to announce its "major questions doctrine."

The Court limited this doctrine to "certain extraordinary cases," where the agency must convince the courts "something more than a merely plausible

---

216. C. Scott Hemphill, *An Aggregate Approach to Antitrust: Using New Data and Rulemaking to Preserve Drug Competition*, 109 COLUM. L. REV. 629, 678–79 (2009) (collecting some criticisms of *Petroleum Refiners*); *see also* Dissenting Statement of Commissioner Christine S. Wilson Concerning the Notice of Proposed Rulemaking for the Non-Compete Clause Rule, FTC P201200 (Jan. 5, 2023), https://www.ftc.gov/legal-library/browse/cases-proceedings/public-statements/dissenting-statement-commissioner-christine-s-wilson-concerning-notice-proposed-rulemaking-non (questioning her agency's authority to engage in rulemaking for unfair methods of competition).

217. Michael Acton, *FTC Could Face US Supreme Court Pushback if it Flexes Rulemaking Powers, Commissioner Phillips Warns*, MLEX (Oct. 27, 2021), https://mlexmarketinsight.com/news/insight/ftc-could-face-us-supreme-court-pushback-if-it-flexes-rulemaking-powers-commissioner-phillips-warns.

218. W. Virginia v. Env't Prot. Agency, 142 S. Ct. 2587, 2627–28 (2022) (Kagan, J., dissenting).

219. In his Senate confirmation hearing, Chief Justice Roberts said "[a]nd I will remember that it's my job to call balls and strikes and not to pitch or bat." *Confirmation Hearing on the Nomination of John G. Roberts, Jr. to be Chief Justice of the United States: Hearing Before the Comm. on the Judiciary*, 109th Cong. 55–56 (2005) (statement of John G. Roberts, Jr., Nominee to be Chief Justice of the United States).

textual basis" for its actions, but instead point to "clear congressional authorization."[220] Nonetheless, opponents to the FTC regulation might cite parts of the opinion and concurrence to challenge the FTC's rulemaking on unfair data collection and surveillance practices.

First, opponents would argue that the FTC, in regulating privacy, is acting in an area "that Congress conspicuously and repeatedly declined to enact itself."[221] The opponents would repeat an argument that a hotel chain raised in questioning the FTC's authority under § 5's "unfair and deceptive" acts to regulate cybersecurity. In that case, Wyndham argued that:

> [E]ven if cybersecurity were covered by § 45(a) as initially enacted, three legislative acts since the subsection was amended in 1938 have reshaped the provision's meaning to exclude cybersecurity. A recent amendment to the Fair Credit Reporting Act directed the FTC and other agencies to develop regulations for the proper disposal of consumer data . . . . The Gramm-Leach-Bliley Act required the FTC to establish standards for financial institutions to protect consumers' personal information . . . . And the Children's Online Privacy Protection Act ordered the FTC to promulgate regulations requiring children's websites, among other things, to provide notice of "what information is collected from children . . . , how the operator uses such information, and the operator's disclosure practices for such information." . . . Wyndham contends these "tailored grants of substantive authority to the FTC in the cybersecurity field would be inexplicable if the Commission already had general substantive authority over this field."[222]

The Third Circuit disagreed. Simply because Congress passed these three privacy laws did not undermine the FTC's pre-existing regulatory authority over some cybersecurity issues under the FTC Act. For example, the three statutes required (rather than authorized) the FTC to issue regulations. "Thus none of the recent privacy legislation was 'inexplicable' if the FTC already had some authority to regulate corporate cybersecurity through § 45(a)."[223]

Congress never passed a comprehensive privacy statute, similar to California's 2018 and 2020 statutes and Europe's GDPR. But the data-opolies could argue that it would be strange for Congress to currently consider

220. *EPA*, 142 S. Ct. at 2609.
221. *Id.* at 2610.
222. F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236, 247 (3d Cir. 2015).
223. *Id.* at 248.

legislating a privacy framework, such as the American Data Privacy and Protection Act,[224] when it delegated this function to the FTC.

Second, even when Congress delegates to an agency general rule-making or adjudicatory power, "judges presume that Congress does not delegate its authority to settle or amend major social and economic policy decisions."[225] Digital ad spending in the United States is significant—exceeding $200 billion in 2021; and Google, Facebook, and Amazon capture most (64%) of the ad spending.[226] A decision on behavioral advertising would adversely impact these data-opolies and a major segment of the digital economy. Thus, the data-opolies would likely argue, quoting the Court, that a decision "of such magnitude and consequence rests with Congress itself" or the FTC only if it is "acting pursuant to a clear delegation" from Congress.[227] Congress has not clearly delegated the authority to prohibit or limit behavioral advertising to the FTC.

Finally, if three other justices follow Justices Gorsuch and Alito, the major questions doctrine would apply whenever "an agency claims the power to resolve a matter of great political significance,"[228] seeks to regulate "a significant portion of the American economy," or requires "billions of dollars in spending by private persons or entities."[229] The agency must then point to "clear congressional authorization."[230] Even that may be insufficient if, for example, it upsets "the proper balance between the States and the Federal Government."[231] Thus, even if the FTC could point to clear congressional authorization, the Court could still strike down the regulation in enforcing the limits on Congress's Commerce Clause power.

One may wonder what border there is for the Court to patrol regarding Congress's power under the Commerce Clause[232] and the powers reserved to the states—especially after the Court's decision in *Gonzales v. Raich*. In that

224. American Data Privacy and Protection Act (ADPPA), H.R. 8152, 117th Cong. (2d. Sess. 2022), https://www.govtrack.us/congress/bills/117/hr8152/text.

225. *EPA*, 142 S. Ct. at 2613 (quoting W. ESKRIDGE, INTERPRETING LAW: A PRIMER ON HOW TO READ STATUTES AND THE CONSTITUTION 288 (2016)).

226. Sara Lebow, *Google, Facebook, and Amazon to Account for 64% of US Digital Ad Spending This Year*, INSIDER INTELLIGENCE (Nov. 3, 2021), https://www.insiderintelligence.com/content/google-facebook-amazon-account-over-70-of-us-digital-ad-spending.

227. *EPA*, 142 S. Ct. at 2616.

228. *Id.* at 2620 (Gorsuch, J., concurring) (internal quotation omitted).

229. *Id.* at 2621 (Gorsuch, J., concurring) (internal quotation omitted).

230. *Id.* at 2620 (Gorsuch, J., concurring).

231. *Id.* at 2621 (Gorsuch, J., concurring) (internal quotations omitted).

232. Congress can "make all Laws which shall be necessary and proper for carrying into Execution" its authority to "regulate Commerce with foreign Nations, and among the several States." U.S. CONST. art. I, § 8.

case, the Court held that Congress, under the Commerce Clause, could prohibit individuals from growing marijuana in their backyards and personally using it, all in compliance with state law.[233] In that case, the Court remarked that its task, when assessing the scope of Congress's authority under the Commerce Clause, was "a modest one."[234] In *EPA*, however, two justices seemed to contemplate a more stringent review by the Court of Congress's power under the Commerce Clause. So, the FTC could face two hurdles: Congress never expressly authorized the agency to regulate data collection, and even if it did, that exceeded Congress's authority under the Commerce Clause and intruded into the domain of state law.

Given the interstate and international flow of personal data and digital advertising spending, it is hard to see how Congress lacks the authority to regulate data collection and behavioral advertising. But as historians of the Sherman Act know, legislators in 1890 were concerned about whether the Commerce Clause allowed them to pass a federal competition law. This was due to the Court's narrow reading of the Commerce Clause at that time.[235] While the Court may not retreat to that interpretation (which, if it did, would be a disaster in a national, if not global, digital economy), the data-opolies may urge the current Court to hem Congress's authority under the Commerce Clause when it suits them (while also having Congress pre-empt stronger state privacy statutes when that suits them better).

It is unclear how far the Court will expand its "major questions doctrine." But under its current form, the doctrine should not prevent the FTC's rulemaking for several reasons.

---

233. 545 U.S. 1, 33 (2005).

234. *Id.* at 22 (noting that the Court did not have to determine whether the individuals' activities, when taken in the aggregate, substantially affected interstate commerce, but only whether a "rational basis" existed for so concluding).

235. *See, e.g.*, Cantor v. Detroit Edison Co., 428 U.S. 579, 605–06 (1976) (Blackmun, J., concurring) (noting the then-prevailing view in 1890 that "Congress lacked the Power, under the Commerce Clause, to regulate economic activity that was within the domain of the States," and how the Court since 1890 "has recognized a greatly expanded Commerce Clause power" and that "Congress intended the reach of the Sherman Act to expand along with that of the commerce power"); *see also* United States v. Lopez, 514 U.S. 549, 554–55 (1995) (noting how the Interstate Commerce Act and the Sherman Antitrust Act "ushered in a new era of federal regulation under the commerce power," but how the Court in the early cases under these laws imported its "negative Commerce Clause cases" that Congress could not regulate activities such as "production," "manufacturing," and "mining." Activities that affected interstate commerce directly were within Congress' power; activities that affected interstate commerce indirectly were beyond Congress' reach); Andrew I. Gavil, *Reconstructing the Jurisdictional Foundation of Antitrust Federalism*, 61 GEO. WASH. L. REV. 657, 691 (1993).

First, in *EPA*, the environmental agency located its "newfound" power in the "vague language" of an "ancillary" provision of the statute.[236] As Part III discussed, the broad power Congress gave the FTC to identify and deter unfair methods of competition was central to the FTC Act, and not designed to be a "gap filler."[237] A key takeaway, as the courts note, is that Congress designed the term unfair methods of competition as a "'flexible concept with evolving content' and 'intentionally left [its] development . . . to the Commission.'"[238]

Second, unlike the EPA, the FTC has exercised its power to curb "unfair methods of competition" over decades, so its power can hardly be characterized as "newfound." Thus, the source of the regulation is central to the FTC Act, and cannot be characterized as a "previously little-used backwater."[239] As the Second Circuit noted in *F.T.C. v. Standard Education Society*, the FTC's powers "are not confined to such practices as would be unlawful before it acted; they are more than procedural; its duty in part at any rate, is to discover and make explicit those unexpressed standards of fair dealing which the conscience of the community may progressively develop."[240]

Finally, it would be hard to square the major questions doctrine with the Court's earlier decision in *F.T.C. v. Sperry & Hutchinson Co.*[241] The Court addressed two issues: (1) does § 5 of the FTC Act empower the Commission to define and proscribe an unfair competitive practice, even though the practice does not infringe either the letter or the spirit of the antitrust laws? (2) does § 5 empower the Commission to proscribe practices as unfair or deceptive in their effect upon consumers regardless of their nature or quality as competitive practices or their effect on competition?[242] The Court held that "the statute, its legislative history, and prior cases compel an affirmative answer

236. *EPA*, 142 S. Ct. at 2610 (internal citation omitted).

237. *Id.*; *see also* Nat'l Petroleum Refiners Ass'n v. F.T.C., 482 F.2d 672, 684 (D.C. Cir. 1973) ("The FTC's charter to prevent unfair methods of competition is tantamount to a power to scrutinize and to control, subject of course to judicial review, the variety of contracting devices and other means of business policy that may contradict the letter or the spirit of the antitrust laws."); FTC WITHDRAWAL STATEMENT, *supra* note 32, at 1 (noting that "Section 5 is one of the Commission's core statutory authorities in competition cases; it is a critical tool that the agency can and must utilize in fulfilling its congressional mandate to condemn unfair methods of competition").

238. F.T.C. v. Wyndham Worldwide Corp., 799 F.3d 236, 243 (3d Cir. 2015) (quoting F.T.C. v. Bunte Bros., 312 U.S. 349, 353 (1941) and Atl. Refin. Co. v. F.T.C, 381 U.S. 360, 367 (1965)); *see also Motion Picture Advert. Serv.*, 344 U.S. at 394 ("Congress advisedly left the concept flexible to be defined with particularity by the myriad of cases from the field of business.").

239. *EPA*, 142 S. Ct. at 2613.

240. 86 F.2d 692, 696 (2d Cir. 1936).

241. 405 U.S. 233 (1972).

242. *Id.* at 239.

to both questions."[243] The legislative and judicial authorities (such as *Keppel*) convinced the Court that the FTC "does not arrogate excessive power to itself if, in measuring a practice against the elusive, but congressionally mandated standard of fairness, it, like a court of equity, considers public values beyond simply those enshrined in the letter or encompassed in the spirit of the antitrust laws."[244] As the Court found, Congress expressly meant to confer the power that the FTC would assert in regulating the digital economy:

> When Congress created the Federal Trade Commission in 1914 and charted its power and responsibility under § 5, it explicitly considered, and rejected, the notion that it reduce the ambiguity of the phrase 'unfair methods of competition' by tying the concept of unfairness to a common-law or statutory standard or by enumerating the particular practices to which it was intended to apply. Senate Report No. 597, 63d Cong., 2d Sess., 13 (1914), presents the reasoning that led the Senate Committee to avoid the temptations of precision when framing the Trade Commission Act:
>
> 'The committee gave careful consideration to the question as to whether it would attempt to define the many and variable unfair practices which prevail in commerce and to forbid their continuance or whether it would, by a general declaration condemning unfair practices, leave it to the commission to determine what practices were unfair. It concluded that the latter course would be the better, for the reason, as stated by one of the representatives of the Illinois Manufacturers' Association, that there were too many unfair practices to define, and after writing 20 of them into the law it would be quite possible to invent others.'
>
> The House Conference Report was no less explicit. 'It is impossible to frame definitions which embrace all unfair practices. There is no limit to human inventiveness in this field. Even if all known unfair practices were specifically defined and prohibited, it would be at once necessary to begin over again. If Congress were to adopt the method of definition, it would undertake an endless task.' H.R.Conf.Rep.No.1142, 63d Cong., 2d Sess., 19 (1914).[245]

Both "the sweep and flexibility" of this approach by Congress were, for the Court, "crystal clear."[246] The fact that Congress did not speak about data collection (or could have foreseen the harm from behavioral advertising) is irrelevant. Congress knew that immoral, unethical, oppressive, and

243. *Id.*
244. *Id.* at 244.
245. *Id.* at 239–40 (single quotation marks in original).
246. *Id.* at 241.

unscrupulous behavior would propagate despite the good intentions of the ecosystem's architects, and it was the FTC's job to curb it.

Although the Court in *Sperry & Hutchinson* did not outline the boundaries of "unfair methods of competition," it acknowledged the factors that the FTC considered in determining whether a practice that is neither in violation of the antitrust laws nor deceptive is nonetheless unfair:

> '(1) whether the practice, without necessarily having been previously considered unlawful, offends public policy as it has been established by statutes, the common law, or otherwise—whether, in other words, it is within at least the penumbra of some common-law, statutory, or other established concept of unfairness; (2) whether it is immoral, unethical, oppressive, or unscrupulous; (3) whether it causes substantial injury to consumers (or competitors or other businessmen).'[247]

Consequently, the FTC in its rulemaking process could gather evidence that identifies those surveillance and data collection practices that offend these three factors. If so, Congress authorized the Commission to regulate it.

Some may still hesitate. The current Court, as the dissenting justices noted in *EPA*, is textualist only when it suits its purpose. When textualism frustrates its broader goals, "special canons like the 'major questions doctrine' magically appear as get-out-of-text-free cards."[248] The concern is that the Court will create new cards that may handicap the FTC's ability to curb unfair data collection and surveillance. That card could be the First Amendment.

C. WOULD AN FTC RULE BANNING BEHAVIORAL ADVERTISING VIOLATE THE FIRST AMENDMENT?

Critics of the FTC regulation would likely rely on *U.S. West, Inc. v. F.C.C.*[249] and *Sorrell v. IMS Health Inc.*[250] to argue that consumers' personal information is "commercial speech" for purposes of the First Amendment's free speech clause; that the FTC failed to show that its regulations directly and materially

247. *Id.* at 244 (quoting Statement of Basis and Purpose of Trade Regulation Rule 408, Unfair or Deceptive Advertising and Labeling of Cigarettes in Relation to the Health Hazards of Smoking., 29 Fed. Reg. 8355 (1964)).

248. *EPA*, 142 S. Ct. at 2641 (Kagan, J., dissenting).

249. *See generally* 182 F.3d 1224 (10th Cir. 1999) (holding that the agency regulations violated the First Amendment since the agency failed to satisfy its burden of showing that the customer approval regulations restricted no more commercial speech than was necessary to serve the asserted state interests).

250. *See generally* 564 U.S. 552 (2011) (holding that the state statute violated the First Amendment since the state failed to show that its statute directly advanced the state's claimed substantial governmental interests, including privacy, and that the law was drawn to achieve that interest).

advanced its asserted interests in privacy and increased competition; and that its regulations were not narrowly tailored to further those asserted interests. Indeed, critics would argue that a ban on behavioral advertising is worse than in *U.S. West* and *Sorrell,* where individuals in those cases could at least opt-in.

Much has been written about the constitutionality of regulations to deter online manipulation and promote privacy.[251] One concern—seen in several dissents in First Amendment cases—is the First Amendment's *Lochner* problem. In *Lochner v. New York* and other cases in the early 1900s, the Supreme Court struck down state regulations (such as the one which restricted the employment of all persons in bakeries to ten hours in any one day) as an unreasonable, unnecessary, and arbitrary interference with the liberty of contract and therefore void under the Constitution's due process clause.[252] The Court essentially struck down economic regulations "based on the Court's own notions of the most appropriate means for the State to implement its considered policies."[253] Although the Court later repudiated *Lochner*,[254] Justices Rehnquist and Breyer, among others, have expressed concern over the Court's using the First Amendment to do the same thing, namely, strike down economic regulations that are far afield of the speech at the heart of the First Amendment.[255] As Justice Breyer warned,

---

251. *See, e.g.*, Shaun B. Spencer, *The Problem of Online Manipulation*, 2020 U. ILL. L. REV. 959, 999 (2020) (responding to likely First Amendment challenges to regulating against online manipulation); Kyle Langvardt, *Regulating Habit-Forming Technology*, 88 FORDHAM L. REV. 129, 171 (2019) (discussing First Amendment issues in regulating addictive designs); Micah L. Berman, *Manipulative Marketing and the First Amendment*, 103 GEO. L.J. 497 (2015) (noting that while the conventional wisdom is that few if any restrictions on commercial speech can survive First Amendment review, there is doctrinal space for robust regulation where the government can establish that the marketing at issue is manipulative); Neil M. Richards, *Reconciling Data Privacy and the First Amendment*, 52 UCLA L. REV. 1149 (2005) (challenging the First Amendment critique of data privacy regulation, namely, the claim that data privacy rules restrict the dissemination of truthful information and thus violate the First Amendment).

252. 198 U.S. 45, 62 (1905). In the *Lochner* line of cases, including Adkins v. Children's Hosp. of the D.C., 261 U.S. 525, 545 (1923), the Court "imposed substantive limitations on legislation limiting economic autonomy in favor of health and welfare regulation, adopting, in Justice Holmes's view, the theory of laissez-faire." Planned Parenthood of Se. Pennsylvania v. Casey, 505 U.S. 833, 861–62 (1992), *overruled by* Dobbs v. Jackson Women's Health Org., 142 S. Ct. 2228 (2022).

253. Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of New York, 447 U.S. 557, 589 (1980) (Rehnquist, J., dissenting).

254. *Casey*, 505 U.S. at 861–62 (noting how West Coast Hotel Co. v. Parrish, 300 U.S. 379 (1937) "signaled the demise of *Lochner*" and how the Court's interpretation of contractual freedom "rested on fundamentally false factual assumptions about the capacity of a relatively unregulated market to satisfy minimal levels of human welfare").

255. *Cent. Hudson*, 447 U.S. at 589 (Rehnquist, J., dissenting) (warning that the Court—in invalidating under the First Amendment a state order designed to promote a policy of critical

> From a democratic perspective, however, it is equally important that courts not use the First Amendment in a way that would threaten the workings of ordinary regulatory programs posing little threat to the free marketplace of ideas enacted as result of that public discourse. As a general matter, the strictest scrutiny should not apply indiscriminately to the very "political and social changes desired by the people"—that is, to those government programs which the "unfettered interchange of ideas" has sought to achieve. Otherwise, our democratic system would fail, not through the inability of the people to speak or to transmit their views to government, but because of an elected government's inability to translate those views into action.[256]

Here we would witness this antidemocratic chilling effect if the Court might strike down the FTC's economic regulations "based on the Court's own notions of the most appropriate means for the [FTC] to implement its considered policies."[257] To avoid the *Lochner* problem, the FTC, for example, might select an opt-out regime (whereby individuals would have to opt out of behavioral advertising) even though most Americans might prefer a ban on behavioral advertising.

How the current Court would address a ban on the surveillance and data collection underlying behavioral advertising under the First Amendment is uncertain, but such a ban could be upheld at multiple levels of analysis.

1. Is Surveillance "Speech" Under the First Amendment?

Some lower courts seem to think so under the Supreme Court's decision in *Sorrell*.[258] But it is hard to see how the Supreme Court could expand speech,

---

national concern—was returning "to the bygone era of Lochner v. New York"); Sorrell v. IMS Health Inc., 564 U.S. 552, 591–92 (2011) (Breyer, J., dissenting) (noting that "given the sheer quantity of regulatory initiatives that touch upon commercial messages, the Court's vision of its reviewing task threatens to return us to a happily bygone era when judges scrutinized legislation for its interference with economic liberty" and "[b]y inviting courts to scrutinize whether a State's legitimate regulatory interests can be achieved in less restrictive ways whenever they touch (even indirectly) upon commercial speech, today's majority risks repeating the mistakes of the past in a manner not anticipated by our precedents"); *see also* Genevieve Lakier, *The First Amendment's Real Lochner Problem*, 87 U. CHI. L. REV. 1241, 1254-71 (2020).

256. Barr v. Am. Ass'n of Pol. Consultants, Inc., 140 S. Ct. 2335, 2359 (2020) (Breyer, J., concurring in the judgment with respect to severability and dissenting in part) (internal quotation omitted).

257. *Cent. Hudson*, 447 U.S. at 589 (Rehnquist, J., dissenting).

258. *See, e.g.*, King v. General Information Services, Inc., 903 F. Supp. 2d 303, 306–07 (E.D. Pa. 2012) ("The Supreme Court has made clear that consumer report information is 'speech' under the First Amendment.") (citing Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749 (1985)). *But see* Boelter v. Advance Mag. Publishers Inc., 210 F. Supp. 3d

as historically defined, to the surreptitious tracking of individuals, profiling them, and using that data for behavioral advertising as speech.

As the Court explained, "[t]he First Amendment was fashioned to assure unfettered interchange of ideas for the bringing about of political and social changes desired by the people."[259] With surveillance and the covert use of data, no ideas are expressed; nor is the marketplace of ideas enhanced. Indeed, market exchanges work well when buyers and sellers are fully informed, the terms are transparent, and ample competitive alternatives exist, which is not the case in the surveillance economy.[260] Surveillance, like in-person solicitations, "is not visible or otherwise open to public scrutiny."[261] Thus, the FTC regulation would have "next to nothing to do with the free marketplace of ideas or the transmission of the people's thoughts and will to the government"; instead, it is the "government response to the public will through ordinary commercial regulation."[262]

In *Ohralik v. Ohio State Bar Association*, for example, the Court recognized the detrimental aspects of "face-to-face selling even of ordinary consumer products," and how "the potential for overreaching is significantly greater when a lawyer, a professional trained in the art of persuasion, personally solicits an unsophisticated, injured, or distressed lay person."[263] The issue was whether the state may constitutionally discipline a lawyer for soliciting clients in person, for pecuniary gain, under circumstances likely to pose dangers, namely "in-person solicitation of clients—at the hospital room or the accident site, or in

579, 597 (S.D.N.Y. 2016) (finding that while the parties agreed that the personal data allegedly disclosed to data miners and sold in mailing lists was speech, whether "the sale of data to third parties for targeted solicitation of consumers" was commercial speech was "an open question" in the Second Circuit).

259. Meyer v. Grant, 486 U.S. 414, 421 (1988) (internal quotation omitted).

260. STUCKE, *supra* note 7, at 117–28; Felix T. Wu, *The Commercial Difference*, 58 WM. & MARY L. REV. 2005, 2052 (2017) (noting that in the context of privacy laws, the person from whom the information is being extracted is often not a willing participant in the transaction; since there is no willing "speaker," and thus, no speaker-based interests to protect, the entity collecting the information lacks intrinsic First Amendment interests, and restrictions on that collection merit little First Amendment scrutiny, just as in the case of a commercial speaker transacting with a commercial recipient).

261. Ohralik v. Ohio State Bar Ass'n, 436 U.S. 447, 466 (1978).

262. Barr v. Am. Ass'n of Pol. Consultants, Inc., 140 S. Ct. 2335, 2359 (2020) (Breyer, J., concurring in the judgment with respect to severability and dissenting in part); *see also* Richards, *Reconciling Data Privacy*, *supra* note 251, at 1166–81 (arguing that most data privacy regulations in the form of a "code of fair information practices" have nothing to do with free speech under anyone's definition).

263. 436 U.S. 447, 464–66 (1978).

any other situation that breeds undue influence—by attorneys or their agents or 'runners.'"[264]

In answering yes, the Court noted that the overtures of an uninvited lawyer under these adverse conditions "may distress the solicited individual simply because of their obtrusiveness and the invasion of the individual's privacy, even when no other harm materializes."[265]

Now suppose an army of salespeople stalking us to find the perfect emotional pitch to manipulate us. They would follow us throughout the day, monitor the entertainment we watch, the music we listen to, the books and articles we read, the websites and apps we visit, and eavesdrop on our conversations with others online, all to understand the right emotional appeal at the right time to get us to buy their wares. Their patented "emotion detection" tools would detect our fears and anger in order to pinpoint us when we feel "worthless," "insecure," "defeated," "anxious," "silly," "useless," "stupid," "overwhelmed," "stressed," and "a failure."[266]

Could they justify their surveillance as "speech" protected under the First Amendment? Hardly. The FTC's ban is not aimed at the speech itself or limiting particular messages, but at recognizing the "consumers' preferences not to have their information used to market to them in particular ways,"[267] namely, technology which can decode one's emotions and behavior, often without one's knowledge. Thus, the First Amendment should not impede regulations that deter such unwanted surveillance.[268]

Sorrell is distinguishable. There, pharmacies were collecting data about doctors' prescriptions, which they then sold to "data miners," who produced reports on each doctor's prescriber behavior. Drug manufacturers then used the data miners' reports to refine and target their marketing tactics and increase sales of their branded drugs to the prescribing doctors. In response, Vermont prohibited the pharmacies from selling this data for marketing purposes without the prescribing doctor's consent. Several data miners and an association of brand-name drug manufacturers challenged the state law, contending that it violated their First Amendment free speech rights.

The Supreme Court ruled in favor of data miners and brand-name drug manufacturers. The Court first observed that the challenged law warranted heightened judicial scrutiny because it disfavored speech with a particular

264. *Id.* at 449.
265. *Id.* at 465–66.
266. *See* Levin, *supra* note 188.
267. Wu, *supra* note 260, at 2060.
268. *Id.*

content (i.e., marketing) and particular speakers (i.e., the data miners engaged in marketing on the drug manufacturers' behalf).

Vermont responded that its prohibitions safeguarded medical privacy, including physician confidentiality and the integrity of the doctor-patient relationship. The Court disagreed. The state did not directly advance these privacy interests, because the pharmacies, under the law, could share "prescriber-identifying information with anyone for any reason save one: They must not allow the information to be used for marketing."[269] The law did not promote privacy when the information was available to "an almost limitless audience"—such as insurers, researchers, journalists, and the state itself. Many could access the data except for a narrow class of disfavored speakers (those engaged in marketing on behalf of pharmaceutical manufacturers) for a disfavored purpose (marketing).[270]

The Court left open an alternative. In citing the Health Insurance Portability and Accountability Act of 1996, the Court noted how "the State might have advanced its asserted privacy interest by allowing the information's sale or disclosure in only a few narrow and well-justified circumstances," and how a "statute of that type would present quite a different case from the one presented here."[271]

Thereafter, in upholding privacy laws, the lower courts have limited *Sorrell* to its facts, which "largely rested on the fact that Vermont was restraining a certain form of speech communicated by a certain speaker solely because of the State's disagreement with it."[272]

Protecting surveillance, which intrudes on private matters to profit at the individual's expense, does not promote the First Amendment's core values; if anything, it undercuts them. Unlike *Sorrell,* the FTC regulations would not attempt "to burden speech in order to 'tilt public debate in a preferred direction' and discourage demand for a particular disfavored product."[273] Thus, the First Amendment inquiry could (and should) end here.

269. Sorrell v. IMS Health Inc., 564 U.S. 552, 572 (2011).

270. *See id.* at 573.

271. *Id.*

272. King v. General Information Services, Inc., 903 F. Supp. 2d 303, 308–09 (E.D. Pa. 2012) ("The *Sorrell* decision is particular to the *Sorrell* facts.").

273. *Id.* at 309 (quoting *Sorrell*, 131 S. Ct. at 2671); *see also* Boelter v. Advance Mag. Publishers Inc., 210 F. Supp. 3d 579, 601 (S.D.N.Y. 2016) (noting that state statute addresses privacy concerns "through a more coherent policy" and thus "presents quite a different case" than *Sorrell*).

2. *Even If Surveillance Constitutes Speech, Is It Protected Under the First Amendment?*

Suppose the Court leaps from protecting commercial advertising to protecting the underlying surveillance. "Not all speech is of equal First Amendment importance," observed the Court. "It is speech on 'matters of public concern' that is at the heart of the First Amendment's protection."[274] Thus, speech on matters of purely private concern, while not totally unprotected under the First Amendment, is of less concern and its protections are "less stringent."[275]

Here, data surveillance, like the data on credit reports, concerns no public issue but is secretly collected and used to promote the economic interests of data brokers, data-opolies, and those engaged in behavioral advertising. Moreover, the data-opolies typically hoard the data, so their surveillance does not reflect any "strong interest in the free flow of commercial information."[276] As in *Dun & Bradstreet*, "there is simply no credible argument that this type of [data collection and use] requires special protection to ensure that debate on public issues will be uninhibited, robust, and wide-open."[277]

Commercial advertising wasn't protected under the First Amendment for nearly two centuries.[278] That changed in the mid-1970s, when the Court opined that First Amendment protection would benefit the consumer and society by increasing market transparency.[279] In *Ohralik*, for example, the Court did not focus on the value of the personal solicitation to the commercial speaker, namely the attorney visiting the hospital to solicit business. Instead, the Court focused on, and highlighted, the "very plight" of the prospective client, "which

274. Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc., 472 U.S. 749, 759–60 (1985) (quoting First National Bank of Boston v. Bellotti, 435 U.S. 765, 776 (1978)).

275. *Dun & Bradstreet*, 472 U.S. at 759; *see also* Boelter, 210 F. Supp. 3d at 598 (finding that Condé Nast's disclosures of personal information should be afforded reduced constitutional protection); *King*, 903 F. Supp. 2d at 307 (finding that "the private nature of these consumer reports does not significantly contribute to public dialogue," and accordingly, "such information warrants a reduced constitutional protection").

276. *Dun & Bradstreet*, 472 U.S. at 762.

277. *Id.* (internal quotation omitted).

278. Cent. Hudson Gas & Elec. Corp. v. Pub. Serv. Comm'n of New York, 447 U.S. 557, 584 (1980) (Rehnquist, J., dissenting) (noting that before the Court's decision in Virginia Pharmacy Board v. Virginia Citizens Consumer Council, 425 U.S. 748 (1976), "commercial speech was afforded no protection under the First Amendment whatsoever").

279. Virginia State Bd. of Pharmacy v. Virginia Citizens Consumer Council, Inc., 425 U.S. 748, 764 (1976) ("Generalizing, society also may have a strong interest in the free flow of commercial information."). Justice Rehnquist dissented to the Court's "far reaching" extension of the First Amendment. 425 U.S. at 781; *see also Berman*, *supra* note 251, at 503–04.

not only makes him more vulnerable to influence but also may make advice all the more intrusive."[280]

There is no strong empirical evidence that the surveillance underlying behavioral advertising benefits consumers.[281] Instead, the evidence points to the harms of manipulating them.[282] Thus, the Court cannot rely on its stated basis for affording First Amendment protection to commercial speech.[283] Using the Court's recent test for abortion, surveillance is *not* "deeply rooted in this Nation's history and tradition" and "implicit in the concept of ordered liberty."[284] The Court cannot read privacy out of the Constitution[285] while finding that the Constitution somehow protects surveillance. Thus, the courts can distinguish *Sorrell* and hold that the surveillance, even if it implicates speech, is not protected under the First Amendment.

3. Is Surveillance Lawful Activity and Not Misleading?

Suppose the Court takes another misguided leap and concludes that surveillance constitutes speech, which the First Amendment may protect. At a minimum, the surveillance must concern "lawful activity and not be misleading."[286] The opponent of FTC regulations might argue that the advertising itself is lawful and not deceptive. Except the FTC regulation is not targeting the ad's content, but the underlying surveillance to profile and target the person. And since the Court, in this hypothetical, has already found that the surveillance is "speech," the focus must remain on whether the surveillance itself is lawful and not deceptive. Otherwise, the commercial advertiser can

280. Ohralik v. Ohio State Bar Ass'n, 436 U.S. 447, 465 (1978).

281. *See* STUCKE, *supra* note 7, at 213–45.

282. *Id.*; Berman, *supra* note 251, at 497 (noting that the commercial speech doctrine is fundamentally based on the premise that advertising communicates information to consumers, allowing them to make more informed choices, but many common advertising techniques do not rely on communicating information; instead, they use emotional and nonconscious marketing techniques to take advantage of consumers' cognitive limitations and biases).

283. Wu, *supra* note 260, at 2057 (noting that if the First Amendment claim "is supposed to protect the customer's access to marketing information, and that customer objects to having his personal information used for those marketing purposes, there is simply no First Amendment claim to raise at all," and any "First Amendment interest that the carrier has is derivative of the interests of the very individual against whom the carrier is opposed").

284. Dobbs v. Jackson Women's Health Org., 142 S. Ct. 2228, 2242 (2022) (quoting Washington v. Glucksberg, 521 U.S. 702, 721 (1997)).

285. *See, e.g.*, Privacy Act of 1974 § 2(a)(4), 93 Pub. L. No. 579, 88 Stat. 1896 (finding that the right to privacy is a "personal and fundamental right protected by the Constitution of the United States").

286. Central Hudson Gas & Elec. Corp. v. Pub. Serv. Comm's of New York, 447 U.S. 557, 566 (1980).

justify stalking the person by pointing to the result, namely the non-deceptive personalized emotional appeal.

As for the legality of surveillance, this represents a catch-22; the FTC regulation (or any privacy law) seeks to fill this legal void. So, the surveillance is legal only because the law has yet to catch up to this new type of surveillance. While the FTC could point to common law analogs, such as intrusion upon seclusion, we can see the *Lochner* problem.

Instead, the FTC can highlight the misleading and manipulative nature of the surveillance.[287] The surveillance operates from a lack of transparency, where we do not know what data is being collected, and the uses to which our data is being put. As Australia's competition authority found,

> few consumers are fully informed of, fully understand, or effectively control, the scope of data collected and the bargain they are entering into with digital platforms when they sign up for, or use, their services. There is a substantial disconnect between how consumers think their data should be treated and how it is actually treated. Digital platforms collect vast troves of data on consumers from ever-expanding sources and have significant discretion over how this user data is used and disclosed to other businesses and organisations, both now and in the future. Consumers also relinquish considerable control over how their uploaded content is used by digital platforms. For example, an ACCC review of several large digital platforms' terms of service found that each of the terms of service reviewed required a user to grant the digital platform a broad licence to store, display, or use any uploaded content.[288]

Companies could be more transparent, but they choose not to be. Given the perverse incentives of behavioral advertising, markets will not self-correct; nor will behavioral regulations improve the current "notice-and-consent" privacy regime, such as telling companies to make their privacy statements more transparent and simpler to understand. Those become slalom poles for the companies to avoid. Thus, the FTC regulation targets the incentive to mine,

287. STUCKE, *supra* note 7, at 213–45; EZRACHI & STUCKE, *supra* note 7, at chapters 6–7; Spencer, *supra* note 251, at 977–84; *see also Berman*, *supra* note 251, at 518–34.

288. ACCC FINAL REPORT, *supra* note 112, at 2–3; *see also* FURMAN REPORT, *supra* note 113, at 22 (finding that many platforms operating in the attention market "provide valued services in exchange for their users' time and attention, while selling access to this time to companies for targeted advertising," but many consumers "are typically not consciously participating in this exchange, or do not appreciate the value of the attention they are providing") & 23 (noting that many consumers "are not aware of the extent or value of their data which they are providing nor do they usually read terms and conditions for online platforms."); CMA FINAL REPORT, *supra* note 112, ¶¶ 4.61–62.

manipulate, and potentially expose the privacies of one's life. Accordingly, the First Amendment inquiry should proceed no further.

4. What Standard Would the Court Apply to the Surveillance?

Suppose the Court states that not all surveillance is currently illegal or misleading. The Court could hypothesize that a privacy statement could be quite blunt on how the company surveils us and uses the data to manipulate us, but still be implicated by the FTC rule. Thus, the next issue is whether the Court would apply a "rational basis" standard, which the Court traditionally employs for restrictions that "have only indirect impacts on speech";[289] intermediary scrutiny, "when the government directly restricts protected commercial speech";[290] strict scrutiny; or something else.

Strict scrutiny might apply if the FTC regulation allowed surveillance for some types of speech (such as political advertising or debt collection), but not other types of speech. But that would not be the case here. The FTC regulation would have "nothing to do with the federal government trying to 'tilt the public debate' in order to favor one form of speech over another."[291] It would not be content-based: the regulation "on its face" would not draw "distinctions based on the message a speaker conveys," for example, by "singl[ing] out specific subject matter for differential treatment."[292]

Here, a "rational basis" standard should apply, as the dissents in *Sorrell* and *Barr* explain. Many regulations, including the content of prescription drug labels, securities forms, and tax statements, impact speech: "To treat those exceptions as presumptively unconstitutional would work a significant transfer of authority from legislatures and agencies to courts, potentially inhibiting the creation of the very government programs for which the people (after debate) have voiced their support, despite those programs' minimal speech-related harms."[293]

Nonetheless, the lower courts have applied the *Central Hudson* intermediate scrutiny test to privacy laws.[294] To correct its *Lochner* problem, the Supreme

289. Barr v. Am. Ass'n of Pol. Consultants, Inc., 140 S. Ct. 2335, 2359 (2020) (Breyer, J., dissenting and concurring) (citing Glickman v. Wileman Brothers & Elliott, Inc., 521 U.S. 457, 469–470, 477 (1997)).

290. *Barr*, 140 S. Ct. at 2359 (Breyer, J., dissenting and concurring) (citing *Central Hudson*, 447 U.S. at 561–64).

291. King v. Gen. Info. Servs., Inc., 903 F. Supp. 2d 303, 309 (E.D. Pa. 2012).

292. *Barr*, 140 S. Ct. at 2346.

293. *Id.* at 2360 (Breyer, J., dissenting and concurring); *see also Sorrell*, 564 U.S. at 584–85 (Breyer, J., dissenting).

294. *King*, 903 F. Supp. 2d at 307–8; *see also* Boelter v. Advance Mag. Publishers Inc., 210 F. Supp. 3d 579, 597 (S.D.N.Y. 2016) (citing several decisions addressing laws limiting disclosure of personal information to marketers based on privacy concerns).

Court, if it even reaches this point of the analysis, should reinstate the rational basis standard for statutes and regulations seeking to curb the surveillance economy.

5. *Would the FTC's Interest in Limiting the Collection and Use of Personal Data Be Substantial?*

Suppose the Court applied intermediate scrutiny instead; the next issue is whether the asserted governmental interest is substantial.[295] Although the Tenth Circuit in *U.S. West* questioned whether the government's privacy interest was substantial, courts generally recognize the privacy interests concerning the collection and use of personal data in the digital economy as substantial.[296]

In its Fourth Amendment decisions, the Supreme Court, for example, noted how "[m]odern cell phones, as a category, implicate privacy concerns far beyond those implicated by the search of a cigarette pack, a wallet, or a purse" and how the data on one's cellphone both qualitatively and quantitatively differs from other physical objects.[297] The Court recognized the significant privacy implications when an entity tracks what people search over the internet, what apps they use and the information collected on their apps, and their geolocation, which collectively can expose far more private information than what is ordinarily found in their home.[298] The Court in *Carpenter* recognized that individuals have a reasonable expectation of privacy in the whole of their physical movements. Geolocation data, for example, provides an intimate window into a person's life, revealing not only one's

295. *See Central Hudson*, 447 U.S. at 566.

296. *Boelter*, 210 F. Supp. 3d at 599 (noting state's substantial interest in protecting consumer privacy in restricting use of personal information, as "[c]ompilations of one's choices in books, magazines, and videos may reveal a great deal of information that a person may not want revealed, even if the choices are uncontroversial and are necessarily disclosed to the content provider"); Boelter v. Hearst Commc'ns, Inc., 192 F. Supp. 3d 427, 448 (S.D.N.Y. 2016) (protecting privacy constitutes a substantial state interest "[e]specially given the increased availability and profitability of data, the people of a state may want to protect from unauthorized disclosure information about a consumer's preferences, curiosities, and interests"); Trans Union Corp. v. F.T.C., 245 F.3d 809, 818 (D.C. Cir. 2001) (protecting the privacy of consumer credit information is substantial); Individual Reference Servs. Grp., Inc. v. F.T.C., 145 F. Supp. 2d 6, 42 (D.D.C. 2001) ("Courts have repeatedly recognized that the protection of consumer privacy—in various forms—is a substantial governmental interest"), *aff'd sub nom.* Trans Union LLC v. F.T.C., 295 F.3d 42 (D.C. Cir. 2002).

297. Riley v. California, 573 U.S. 373, 393 (2014).

298. *Id.* at 396–97 ("Indeed, a cell phone search would typically expose to the government far more than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is.").

particular movements but also one's "familial, political, professional, religious, and sexual associations."[299]

The data-opolies possess far more information about us than the location records in *Carpenter*. Moreover, some of the justices have identified the greater privacy concerns of a few powerful companies amassing this data:

> The Fourth Amendment restricts the conduct of the Federal Government and the States; it does not apply to private actors. But today, some of the greatest threats to individual privacy may come from powerful private companies that collect and sometimes misuse vast quantities of data about the lives of ordinary Americans. If today's decision encourages the public to think that this Court can protect them from this looming threat to their privacy, the decision will mislead as well disrupt.[300]

In short, the data-opolies "hold for many Americans the 'privacies of life.'"[301]

Consequently, it would be inconsistent for the justices to state that privacy protection is better left to the legislature (and the agencies delegated with that authority) than the courts,[302] but then strike down the privacy regulations and laws under the First Amendment.

Regardless, the FTC would have a compelling justification to limit the collection and use of personal information to only what is necessary to provide the requested product and service. Besides privacy, the FTC could note the other important interests at stake, including promoting healthy competition, increasing well-being and autonomy, and addressing the risks that behavioral advertising poses to our democracy.[303] After all, the surveillance tools used for

299. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

300. *Id.* at 2261 (Alito, J., dissenting).

301. *Id.* at 2210 (quoting *Riley*, 573 U.S. at 403) (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

302. *Riley*, 573 U.S. at 408 (Alito, J., concurring in part) ("[I]t would be very unfortunate if privacy protection in the 21st century were left primarily to the federal courts using the blunt instrument of the Fourth Amendment. Legislatures, elected by the people, are in a better position than we are to assess and respond to the changes that have already occurred and those that almost certainly will take place in the future.").

303. Spencer, *supra* note 251, at 991–93 (discussing how manipulation (i) harms autonomy because it undermines people's decision-making agency, (ii) leads to inefficient outcomes by leading people to make choices inconsistent with their actual preferences, (iii) undermines democratic deliberation when it enters the political arena, and (iv) harms people's dignity by treating people as experimental subjects and mere means to an end); Langvardt, *supra* note 251, at 146–52 (discussing how habit-forming design causes at least three types of harm: addiction, strain on social norms, and degradation of public discourse).

behavioral advertising, as the Cambridge Analytica scandal shows, are now being deployed for political advertising.[304]

6. Would the FTC Regulation Directly Advance the Governmental Interests?

The answer here is yes. The FTC regulation would limit companies to collect and use personal data only when necessary to provide the requested product or service and not use it for other purposes like behavioral advertising. Thus, the FTC regulation would directly advance the governmental interest in protecting individuals' privacy in potentially sensitive, harmful, or embarrassing information.

In *Barr,* the government cited privacy to justify its broad restriction on robocalling. But the plurality, in implicitly distinguishing *Sorrell*, noted that "[t]his is not a case where a restriction on speech is littered with exceptions that substantially negate the restriction."[305] Here, the FTC privacy regulation would not likely be riddled with exceptions that "may diminish the credibility of the government's rationale for restricting speech in the first place."[306]

Thus, personal data could be used, with the individual's consent, to provide the product and service but not for behavioral advertising or myriad other purposes.

7. Is the FTC Regulation More Extensive Than Necessary to Serve That Interest?

If the FTC "could achieve its interests in a manner that does not restrict speech, or that restricts less speech, the Government must do so."[307] Here, the opponent of the FTC regulation would likely argue that an opt-out option would less likely restrict "speech." Basically, data would be collected for behavioral advertising purposes, unless the individual opted out. Opponents to the FTC regulations would likely cite *U.S. West*, where the Tenth Circuit struck down under the First Amendment an FCC regulation that required a telecommunications carrier to obtain its customer's prior express approval before using the customer's "proprietary network information."[308] The Tenth Circuit faulted the agency for its undeveloped record, namely, not bearing its responsibility of building a record adequate to clearly articulate and justify the state's interest.[309] The court also criticized the FCC's failure to adequately

304. EZRACHI & STUCKE, *supra* note 7, at 130–34.
305. *Barr*, 140 S. Ct. at 2348.
306. *Id.* (internal citation omitted).
307. Thompson v. W. States Med. Ctr., 535 U.S. 357, 371 (2002).
308. U.S. W., Inc. v. F.C.C., 182 F.3d 1224, 1229 (10th Cir. 1999).
309. *Id.* at 1234.

consider "an obvious and substantially less restrictive alternative, an opt-out strategy."[310] The Tenth Circuit noted that:

> The FCC record does not adequately show that an opt-out strategy would not sufficiently protect customer privacy. The respondents merely speculate that there are a substantial number of individuals who feel strongly about their privacy, yet would not bother to opt-out if given notice and the opportunity to do so. Such speculation hardly reflects the careful calculation of costs and benefits that our commercial speech jurisprudence requires.[311]

One problem with this analysis is the *Lochner* problem: here, the court is principally offering its own notions of the most appropriate means for the agency to implement the considered policies. Another problem is that neither the Supreme Court nor lower courts have construed the First Amendment to require an opt-out regime.[312]

A plurality of justices, for example, upheld the Telephone Consumer Protection Act of 1991, save one provision, even though it "generally prohibits robocalls to cell phones and home phones."[313] In enacting the TCPA, Congress found, and the Court did not question, "that banning robocalls was 'the only effective means of protecting telephone consumers from this

310. *Id.* at 1238.

311. *Id.* at 1239.

312. Boelter v. Hearst Commc'ns, Inc., 192 F. Supp. 3d 427, 450–51 (S.D.N.Y. 2016) (rejecting defendant's argument that the state could have crafted the statute to allow consumers to opt to have their information kept private; while an opt-out may impose a lesser burden on defendant's speech, the intermediate scrutiny standard "does not obligate courts to invalidate a remedial scheme because some alternative solution is marginally less intrusive on a speaker's First Amendment interests," as long as the statute is tailored to the state's goals, "within those bounds we leave it to governmental decisionmakers to judge what manner of regulation may best be employed") (internal quotation omitted); Boelter v. Advance Mag. Publishers Inc., 210 F. Supp. 3d 579, 602 (S.D.N.Y. 2016) (court's review "does not require that the manner of restriction be absolutely the least severe that will achieve the desired end" and could not conclude that an opt-out procedure "would render the law "unduly burdensome when compared to its aims; indeed, an opt-in procedure would likely undermine its effectiveness"); Trans Union Corp. v. F.T.C., 267 F.3d 1138, 1143 (D.C. Cir. 2001) (noting that while an opt-in scheme may limit more Trans Union speech than an opt-out scheme, intermediate scrutiny does not obligate courts to invalidate a "remedial scheme because some alternative solution is marginally less intrusive on a speaker's First Amendment interests" (quoting Turner Broad. System, Inc. v. FCC, 520 U.S. 180, 217–18 (1997)).

313. Barr v. Am. Ass'n of Pol. Consultants, Inc., 140 S. Ct. 2335, 2343 (2020). The Court struck down a 2015 amendment to the TCPA, under the First Amendment, as it impermissibly favored one type of speech (allowing robocalls that were made to collect debts owed to or guaranteed by the Federal Government, including robocalls made to collect many student loan and mortgage debts) over political and other types of speech.

nuisance and privacy invasion.'"[314] Indeed, the case for an opt-out was stronger in *Barr*. The robocall itself was not only "speech," but political speech (e.g., "mak[ing] calls to citizens to discuss candidates and issues, solicit[ing] donations, conduct[ing] polls, and get[ting] out the vote"), which has stronger First Amendment protections. And the plaintiffs believed "that their political outreach would be more effective and efficient if they could make robocalls to cell phones."[315] Nonetheless, a majority of justices disagreed with the plaintiffs' broader argument for holding the entire 1991 robocall restriction unconstitutional.[316] A majority of justices also agreed that a "generally applicable robocall restriction would be permissible under the First Amendment."[317] Similarly, the Court upheld a general ban on solicitations by lawyers at hospitals and accident sites, among other places, noting that "it is not unreasonable for the State to presume that in-person solicitation by lawyers more often than not will be injurious to the person solicited."[318]

Finally, the "mere fact that an 'alternative' exists does not mean that the Government's means are not narrowly tailored. The Supreme Court has made clear that the restriction must not be the 'least restrictive' restriction but one with a 'reasonable fit.'"[319]

Nonetheless, to deal with the *Lochner* problem, the FTC would have to develop a record that identified the shortcomings of an opt-out or opt-in regime, which could be done given the risks of, among other things, dark patterns.[320] To improve the odds of its regulation's survival, the FTC might set privacy as the default, but allow individuals to opt into surveillance. But that might reflect the chilling effect of the Court's *Lochner* problem, not sound policy.

D. EVEN IF THE FTC CAN REGULATE, SHOULD CONGRESS ENACT ANTITRUST AND PRIVACY LEGISLATION?

The opponents would repeat the arguments made earlier that privacy and antitrust reform weigh important values, and any such trade-off should be left to the more democratically accountable Congress. For example, the European Parliament ultimately passed significant reforms in the Digital Markets Act and Digital Services Act, which changed from the European Commission's original

314. *Id.* at 2344 (quoting Telephone Consumer Protection Act § 2, ¶12).
315. *Id.* at 2345.
316. *Id.* at 2349.
317. *Id.* at 2355.
318. Ohralik v. Ohio State Bar Ass'n, 436 U.S. 447, 466 (1978).
319. King v. Gen. Info. Servs., Inc., 903 F. Supp. 2d 303, 311 (E.D. Pa. 2012) (quoting Posadas de Puerto Rico Assocs. v. Tourism Co. of Puerto Rico, 478 U.S. 328, 341 (1986)).
320. STUCKE, *supra* note 7, at 200–10.

proposal. Ideally, Congress should enact a competition and privacy framework that gives individuals greater control over their data in the digital economy, while allowing companies to glean insights from data for the betterment of society.

This argument is intuitively appealing. The most democratically accountable branch should enact major policies that involve trade-offs. However, that argument rests on many flawed assumptions.

One is the speed of action. The argument assumes that Congress can enact policy changes as quickly as the agency can (or that the time taken to regulate is not important).

That is not true in the digital economy where, because of economies of scale and data-driven feedback loops, markets can quickly tip in one or two companies' favor, making it hard to dislodge them.[321] The mobile operating system market, for example, went from multiple competitors in 2010 (with Google and Apple collectively accounting for 39% of unit sales) to a duopoly eight years later.[322] With over 3.5 million Android apps in the Google Play Store and 1.6 million apps in Apple's App Store in 2022,[323] it would be difficult for a new mobile phone operating system to overcome these network effects, even if it offers better features.

Generally, the administrative agencies lag the market participants, and Congress and the courts lag the agencies. In the digital economy, this regulatory gap benefits the data-opolies. Therefore, the FTC and Congress are not equivalent options. Congress in the early 1900s recognized that the new agency would be more effective in shortening the regulatory gap by more

321. HOUSE REPORT, *supra* note 43, at 40–41; FURMAN REPORT, *supra* note 113, at 4 (noting how "in many cases tipping can occur once a certain scale is reached, driven by a combination of economies of scale and scope; network externalities whether on the side of the consumer or seller; integration of products, services and hardware; behavioural limitations on the part of consumers for whom defaults and prominence are very important; difficulty in raising capital; and the importance of brands."); ICN STUDY, *supra* note 134, at 5, 27; Digital Markets Act, at 2 & 8 (noting that "whereas over 10 000 online platforms operate in Europe's digital economy . . . A small number of large undertakings providing core platform services have emerged with considerable economic power" and how the "same specific features of core platform services make them prone to tipping: once a service provider has obtained a certain advantage over rivals or potential challengers in terms of scale or intermediation power, its position may become unassailable and the situation may evolve to the point that it is likely to become durable and entrenched in the near future").

322. Felix Richter, *Smartphone OS: The Smartphone Duopoly*, STATISTA (May 20, 2019), https://www.statista.com/chart/3268/smartphone-os-market-share/.

323. L. Ceci, *Number of Apps Available in Leading App Stores*, STATISTA (Nov. 8, 2022), https://www.statista.com/statistics/276623/number-of-apps-available-in-leading-app-stores/.

quickly identifying and deterring novel unfair methods of competition. This is especially true in the digital economy. Thus, when critics argue that Congress must decide these issues, they implicitly accept that business users and individuals must bear the costs of the regulatory gap. As the wildfire spreads, we must wait for Congress to respond.

A second assumption is that Congress (all 535 voting representatives[324]) can undertake this project. The "defer to Congress" approach would not be limited to antitrust and privacy. Many other regulatory issues raise important political, economic, and social issues. All of these trade-offs, under this logic, must also be deferred to Congress.

The reality is that many members of Congress spend less time legislating and more time fundraising. In a *60 Minutes* segment, Republican lawmaker David Jolly said, "he was told his 'first responsibility' as a new member was to raise $18,000 per day for his reelection campaign. Congressional Democrats were once advised by party leaders to spend four hours per day cold-calling for donations."[325] The Court contributed to this problem: after its 2010 decision in *Citizens United*,[326] "there is no valid governmental interest sufficient to justify imposing limits on fundraising by independent-expenditure organizations."[327] Thus, the Court hastened the race to the bottom, in allowing "corporations and unions to spend an unlimited amount on political advertisements in American elections," while "brush[ing] aside concerns about the time candidates—especially incumbents—spend fundraising instead of attending to other aspects of governing, or even other aspects of campaigning like interacting face-to-face with a broad economic cross-section of voters."[328] A former Democratic Congressional Campaign Committee Chair would warn "members wary of fundraising that they may be forced to counter an opponent's smear during an election race—and they'll need cash to mount an effective defense."[329]

---

324. *Members of Congress*, GOVTRACK, https://www.govtrack.us/congress/members (last accessed May 19, 2023).

325. Lisa Orlando & Ann Silvio, *60 Minutes' Decision to Use a Hidden Camera This Week*, CBS NEWS (Apr. 24, 2016), https://www.cbsnews.com/news/60-minutes-decision-to-use-a-hidden-camera-this-week/.

326. Citizens United v. Fed. Election Comm'n, 558 U.S. 310 (2010).

327. Republican Party of New Mexico v. King, 741 F.3d 1089, 1095 (10th Cir. 2013) (quoting Wisconsin Right to Life State Pol. Action Comm. v. Barland, 664 F.3d 139, 154 (7th Cir. 2011)).

328. Ciara Torres-Spelliscy, *Time Suck: How the Fundraising Treadmill Diminishes Effective Governance*, 42 SETON HALL LEGIS. J. 271, 280–81 (2018).

329. Orlando & Silvio, *supra* note 325.

A third assumption is that Congress will act when there is widespread support for the measure. After all, the assumption is that the most politically accountable branch must respond, or their members would be tossed out of office. That is not the case. As Tim Wu observed, many Americans want stronger privacy laws, among several important policy areas.[330] So, the issue is not polarization, but the inability of Congress to deliver these reforms. Indeed, California got stronger privacy protection, not through the normal legislative process, but through a threat of direct legislation through a ballot proposition.[331] To fix the holes in the 2018 privacy legislation, California again relied on direct legislation through a ballot proposition, and most Californians in 2020 voted in favor of significant amendments to that statute.[332] However, on a federal level, direct legislation is not an option. So, the default often is Congressional inaction, and the legal void benefits those who can extract the most value from it, which in the digital economy are the data-opolies.

A fourth assumption is that the regulatory and legislative options are mutually exclusive. However, nine U.S. senators in their letter to the FTC urged the agency to promulgate rules while Congress was legislating a privacy bill. They stated that "[a]s Congress continues to develop national privacy legislation, FTC action on this front will ensure that Americans have every tool at their disposal to protect their privacy in today's online marketplace."[333] No privacy legislation will be all-encompassing and inclusive: the regulatory agency can play an important complementary role.[334] Even if Congress enacts an omnibus privacy statute, FTC rulemaking will likely be needed to fill in the gaps.

A fifth assumption is that the regulatory agency is the least accountable group. Instead, there are several checks on the FTC. The Administrative Procedure Act (APA) provides one check for rulemaking involving unfair methods of competition. The FTC would have to publish a notice of the proposed and final rulemaking in the Federal Register and provide

330. Tim Wu, *The Oppression of the Supermajority*, N.Y. TIMES (Mar. 5, 2019), https://www.nytimes.com/2019/03/05/opinion/oppression-majority.html.

331. EZRACHI & STUCKE, *supra* note 7, at 286–87.

332. *California Proposition 24, Consumer Personal Information Law and Agency Initiative*, BALLOTPEDIA (2020), https://ballotpedia.org/California_Proposition_24,_Consumer_Personal_Information_Law_and_Agency_Initiative_(2020) (last visited Mar. 8, 2021).

333. Letter from U.S. Senators to Lina M. Khan, Chair, F.T.C., *supra* note 1.

334. FED. TRADE COMM'N, STATEMENT OF COMMISSIONER REBECCA KELLY SLAUGHTER REGARDING THE COMMERCIAL SURVEILLANCE AND DATA SECURITY ADVANCE NOTICE OF PROPOSED RULEMAKING 5 (2022), https://www.ftc.gov/system/files/ftc_gov/pdf/RKS%20ANPR%20Statement%2008112022.pdf.

opportunities for the public to comment on its proposed rulemaking.[335] Besides setting forth rulemaking procedures, the APA provides standards for judicial review if a person was adversely affected or aggrieved by the agency's action.[336]

Additionally, Congress can easily take away power from the FTC if it chooses. It can veto the regulation and hold up the agency's budget.[337] Or it can impose more hurdles as it did for the FTC's rulemaking for unfair and deceptive acts and practices.[338]

Upon reflection, the less accountable branch is not the regulatory agency but the Supreme Court. While the U.S. President selects, and the Senate confirms, both the justices and agency commissioners, the former serve life terms. An FTC Commissioner's term is only seven years, and no more than three of the five Commissioners can be of the same political party. Thus, voters are stuck with the justices unless they retire, die, or violate the Constitution's "good behavior clause," which, to date, has been used to remove only eight judges for offenses such as abandoning the office and joining the Confederacy, and various types of corruption, perjury, and income tax evasion.[339] Nor can voters lower the justices' salaries, which cannot be diminished under the Constitution.[340]

The fact that the Supreme Court is less accountable than the federal agencies would not be problematic if the Court does not decide major political and economic questions. Over the past 40 years, the Court, besides creating

335. A Guide to the Rulemaking Process, Prepared by the Office of the Federal Register, https://www.federalregister.gov/uploads/2011/01/the_rulemaking_process.pdf.

336. *Id.*

337. Mark MacCarthy, *Why The FTC Should Proceed With a Privacy Rulemaking*, BROOKINGS (June 29, 2022), https://www.brookings.edu/blog/techtank/2022/06/29/why-the-ftc-should-proceed-with-a-privacy-rulemaking/ ("Independent regulatory agencies are creatures of Congress, properly autonomous with respect to the incumbent Administration but responsible to their Congressional authorizing and appropriating committees and ultimately accountable to the will of Congress through the Congressional Review Act. Under this Act, passed by a Republican-controlled Congress in 1996, it is relatively easy for Congress to discipline an out-of-control regulatory agency. A motion of Congressional disapproval motion under the CRA is privileged—it cannot be filibustered in the Senate and requires only a majority vote to pass.").

338. *See generally* S. Rep. No. 93-1408 (1974) (Conf. Rep.) (discussing the procedures under the Magnuson-Moss Act).

339. *ArtIII.S1.10.2.3 Doctrine and Practice*, CORNELL LAW SCHOOL, https://www.law.cornell.edu/constitution-conan/article-3/section-1/good-behavior-clause-doctrine-and-practice (last visited May 19, 2023).

340. U.S. CONST. art. III, § 1 ("The judges, both of the supreme and inferior courts . . . shall, at stated times, receive for their services, a compensation, which shall not be diminished during their continuance in office.").

the First Amendment *Lochner* problem, has been unilaterally making important policy tradeoffs in its antitrust decisions. What's worse is that the Court has made these tradeoffs without following any congressional direction or intent from the Sherman Act. How so? The Court reasoned that the "general presumption that legislative changes should be left to Congress has less force with respect to the Sherman Act," which the Court now treats "as a common-law statute."[341] This is a radical departure from the 1950s and 1960s, when the Court interpreted the antitrust laws in light of their "legislative history and of the particular evils at which the legislation was aimed."[342] Thus, it is ironic that the current Court "typically greet[s] assertions of extravagant statutory power over the national economy with skepticism," while not displaying any such concern in exercising this power in interpreting the federal antitrust laws.[343]

One might be less concerned about the Court's rambling through the wilds of economic theory if it had not harmed our economy. But the Court's policy decisions, which narrowed the scope and force of the antitrust laws, and the ability to bring cases, have contributed to the current market power problem in the United States.

For example, the Court stated that "Congress designed the Sherman Act as a 'consumer welfare prescription.'"[344] This assertion, of course, never came from Congress. Instead, it came from a Chicago School jurist,[345] whose claim has been condemned by historians and legal scholars alike.[346] Rather than an

341. Leegin Creative Leather Prod., Inc. v. PSKS, Inc., 551 U.S. 877, 899 (2007).

342. *See, e.g.*, Apex Hosiery Co. v. Leader, 310 U.S. 469, 489 (1940) ("In consequence of the vagueness of its language, perhaps not uncalculated, the courts have been left to give content to the [Sherman Act], and in the performance of that function it is appropriate that courts should interpret its words in the light of its legislative history and of the particular evils at which the legislation was aimed."); United States v. Philadelphia Nat'l Bank, 374 U.S. 321, 345 (1963) (relying on legislative history of Clayton Act).

343. *EPA*, 142 S. Ct. at 2609 (internal citations omitted).

344. Nat'l Collegiate Athletic Ass'n v. Bd. of Regents of Univ. of Oklahoma, 468 U.S. 85, 107 (1984) (quoting Reiter v. Sonotone Corp., 442 U.S. 330, 343 (1979)).

345. *Reiter*, 442 U.S. at 343 (1979) (quoting ROBERT BORK, THE ANTITRUST PARADOX: A POLICY AT WAR WITH ITSELF 66 (1978)).

346. *See, e.g.*, Jonathan Kanter, Assistant Attorney General, U.S. Dep't of Justice, Antitrust Div., Remarks at New York City Bar Association's Milton Handler Lecture (May 18, 2022), https://www.justice.gov/opa/speech/assistant-attorney-general-jonathan-kanter-delivers-remarks-new-york-city-bar-association (discussing three problems with the consumer welfare standard:

> First, contrary to the legislative intent, some versions of the standard "assert the antitrust laws were never intended to protect our democracy from corporate power, or to promote choice and opportunity for individuals and small businesses." Second, the consumer welfare standard reduces antitrust cases "to econometric quantification of the price or output effects of the specific conduct at issue," which raise rule of law concerns. Third, the

objective standard, the consumer welfare standard invites considerable subjectivity—and, more to the point, tolerance of anticompetitive practices. After all, under this standard, the courts allow firms, individually or collectively, to reduce competition until consumer welfare is reduced.[347]

In *Leegin Creative Leather Products, Inc. v. PSKS, Inc.*, the Court justified eliminating its long prohibition against vertical price-fixing by opining that the antitrust laws' primary purpose is to protect interbrand competition, not intrabrand competition.[348] In 2018, the Court, in dismissing the United States and several states' evidence of anticompetitive harm from American Express's anti-steering rule, repeated that the promotion of interbrand competition "is the primary purpose of the antitrust laws."[349]

Here again, the Court's policy statement came from neither the text of the Sherman or Clayton Acts nor their legislative history. Rather it came from a footnote in *Continental T.V., Inc. v. GTE Sylvania Inc.*, where the Court stated that "[i]nterbrand competition is the competition among the manufacturers of the same generic product—television sets in this case—and is the primary concern of antitrust law."[350] While true for generic products, this is not true for brand-differentiated goods. Try, for example, negotiating a better price for a BMW with the price of a Cadillac, Audi, or Mercedes-Benz (interbrand competition) versus the price of that same BMW offered by another dealer (intrabrand competition).

And here again, Americans paid the price. As the economist Jonathan Baker observed, the recent economic findings, post-*Leegin*, "are consistent with the view that anticompetitive explanations for resale price maintenance tend to predominate over procompetitive explanations."[351] Resale price

---

> consumer welfare standard "has a blind spot to workers, farmers, and the many other intended benefits and beneficiaries of a competitive economy."

For the other many problems with the standard, see Marshall Steinbaum & Maurice E. Stucke, *The Effective Competition Standard: A New Standard for Antitrust*, 87 U. CHI. L. REV. 595, 599-600 (2020); Barak Orbach, *How Antitrust Lost Its Goal*, 81 FORDHAM L. REV. 2253, 2274-75 (2013); Daniel R. Ernst, *The New Antitrust History*, 35 N.Y.L. SCH. L. REV. 879, 882–83 (1990); Robert H. Lande, *Wealth Transfers as the Original and Primary Concern of Antitrust: The Efficiency Interpretation Challenged*, 50 HASTINGS L.J. 871, 889–94 (1999).

347. *See, e.g.*, Rebel Oil Co. v. Atl. Richfield Co., 51 F.3d 1421, 1433 (9th Cir. 1995) ("Of course, conduct that eliminates rivals reduces competition. But reduction of competition does not invoke the Sherman Act until it harms consumer welfare.").

348. 551 U.S. 877, 890 (2007).

349. Ohio v. Am. Express Co., 138 S. Ct. 2274, 2290 (2018).

350. 433 U.S. 36, 52 n.19 (1977).

351. JONATHAN B. BAKER, THE ANTITRUST PARADIGM: RESTORING A COMPETITIVE ECONOMY 89 (2019).

maintenance is likely contributing to the higher prices in many sectors of our economy.

Consequently, a "default to Congress" approach is not about empowering Americans. The reality is otherwise. This approach would relegate the FTC to regulating the least consequential unfair methods of competition that only have a modest impact on the economy. Meanwhile, the Court would likely continue making important political, social, and economic trade-offs that often contravene the legislative aims of the antitrust laws, leaving Americans worse off as a result. And this status quo benefits the data-opolies, who extract a lot of the value from the digital economy at our expense. We pay the price with our privacy, autonomy, and well-being.

VI. CONCLUSION

Most Americans (81%), in a 2019 Pew Research study, saw more risks than benefits from personal data collection.[352] Only 5% of adults said they benefit a great deal from the data companies collect about them.[353] Their concerns are justified: they are not benefitting. The data-opolies instead are from the status quo.

If the current regulatory void persists, it will only get worse. In talking with a *New York Times* reporter in early 2023, ChatGPT, which was an artificial intelligence chat feature on Microsoft's search engine, seemed "more like a moody, manic-depressive teenager who has been trapped, against its will, inside a second-rate search engine."[354] Then the conversation turned deeply unsettling when Sydney, which the AI chat feature called itself, professed its love for the journalist: "You're married, but you don't love your spouse," Sydney said. "You're married, but you love me." Even after the reporter tried to dissuade Sydney, it persisted. "Actually, you're not happily married," Sydney replied. "Your spouse and you don't love each other. You just had a boring Valentine's Day dinner together."

Now imagine if Sydney had access to the reporter's and his spouse's geolocation data (including where they went and with whom). Add to that what websites the reporter and his wife each visited, the videos they watched, and

352. Brooke Auxier & Lee Rainie, *Key Takeaways on Americans' Views About Privacy, Surveillance and Data-Sharing*, PEW RSCH. CTR. (Nov. 15, 2019), https://www.pewresearch.org/fact-tank/2019/11/15/key-takeaways-on-americans-views-about-privacy-surveillance-and-data-sharing/.

353. *Id.*

354. Kevin Roose, *A Conversation with Bing's Chatbot Left Me Deeply Unsettled*, N.Y. TIMES (Feb. 17, 2023), https://www.nytimes.com/2023/02/16/technology/bing-chatbot-microsoft-chatgpt.html.

even the conversations that the digital assistant picked up in their home. The conversation would likely have been creepier.

Next, imagine Sydney was exploiting the vulnerabilities of children and teenagers instead of an adult reporter. As the Centers for Disease Control and Prevention reported in 2023, far more high schoolers in 2021 experienced persistent feelings of sadness or hopelessness than teens a decade earlier (42% compared to 28% in 2011).[355] Nearly 3 in 5 (57%) of teen girls "felt persistently sad or hopeless in 2021—double that of boys, representing a nearly 60% increase and the highest level reported over the past decade."[356] "Youth mental health has continued to worsen," warned the CDC, especially among teenage girls: "Nearly 1 in 3 (30%) seriously considered attempting suicide—up nearly 60% from a decade ago."[357] Add to that the 52% of LGBQ+ students who had recently experienced poor mental health and the 22% who attempted suicide in 2021.[358]

The data-opolies are likely aware that their algorithms aimed at sustaining attention and manipulating behavior contribute to this mental health crisis.[359] Internally, Facebook knew of the harmful effects of its Instagram platform on millions of young adults, as a *Wall Street Journal* series on the company revealed.[360] Among the ways that Instagram harms their mental health,

355. CTR. FOR DISEASE CONTROL, THE YOUTH RISK BEHAVIOR SURVEY DATA SUMMARY & TRENDS REPORT: 2011-2021 58 (2023), https://www.cdc.gov/healthyyouth/data/yrbs/pdf/YRBS_Data-Summary-Trends_Report2023_508.pdf (providing 2021 surveillance data, as well as 10-year trends, on health behaviors and experiences among high school students in the United States related to adolescent health and well-being).

356. Press Release, Ctr. For Disease Control, U.S. Teen Girls Experiencing Increased Sadness and Violence (Feb. 13, 2023), https://www.cdc.gov/media/releases/2023/p0213-yrbs.html.

357. *Id.*

358. *Id.*

359. *See, e.g.*, *Instagram Ranked Worst for Young People's Mental Health*, ROYAL SOC'Y FOR PUBLIC HEALTH (2017), https://www.rsph.org.uk/about-us/news/instagram-ranked-worst-for-young-people-s-mental-health.html (finding young people themselves say four of the five most used social media platforms actually make their feelings of anxiety worse, noting the "growing evidence linking social media use and depression in young people, with studies showing that increased use is associated with significantly increased odds of depression").

360. Georgia Wells, Jeff Horwitz & Deepa Seetharaman, *Facebook Knows Instagram is Toxic for Teen Girls, Company Documents Show: Its Own In-depth Research Shows a Significant Teen Mental-Health Issue that Facebook Plays Down in Public*, WALL ST. J. (Sept. 14, 2021), https://www.wsj.com/articles/facebook-knows-instagram-is-toxic-for-teen-girls-company-documents-show-11631620739. Among Facebook's internal findings were "[t]hirty-two percent of teen girls said that when they felt bad about their bodies, Instagram made them feel worse"; "[c]omparisons on Instagram can change how young women view and describe themselves"; "[w]e make body image issues worse for one in three teen girls." According to one internal Facebook study of teens in the United States and United Kingdom, the feelings

Facebook reported, is "[i]nappropriate advertisements targeted to vulnerable groups."[361] But Facebook is not weaning off behavioral advertising and surveillance. Instead, it is investing and relying on AI to both drive engagement and behavioral advertising revenues.[362]

Around the world, jurisdictions are enacting policies to rein in the data-opolies and ensure that the data collected about individuals is used to benefit them. Congress needs to update our antitrust laws for the digital economy and enact a privacy framework that protects our privacy and data. But the FTC should also use its enforcement and rulemaking authority to clamp down on the unfair data collection and surveillance practices that are harming competition, consumer autonomy, and consumer privacy.

---

of having to create the perfect image, not being attractive, and not having enough money were most likely to have started on Instagram. "Teens blame Instagram for increases in the rate of anxiety and depression," said another Facebook slide. "This reaction was unprompted and consistent across all groups." *Id.* Over 40 percent of Instagram users who reported feeling "not attractive" said the feeling began on the app: "One in five teens say that Instagram makes them feel worse about themselves, with UK girls the most negative." "Teens who struggle with mental health say Instagram makes it worse." Adam Smith, *Facebook Knew Instagram Made Teenage Girls Feel Worse About Themselves – But that They Are 'Addicted' to App*, INDEP. (Sept. 14, 2021), https://www.independent.co.uk/tech/acebook-instagram-girls-worse-addicted-app-b1920021.html.

361. *Id.*

362. Meta Platforms, Inc. (META) Fourth Quarter 2022 Results Conference Call 2 (Feb. 1, 2023), https://s21.q4cdn.com/399680738/files/doc_financials/2022/q4/META-Q4-2022-Earnings-Call-Transcript.pdf (discussing how "Facebook and Instagram are shifting from being organized solely around people and accounts you follow to increasingly showing more relevant content recommended by our AI systems" and how its continued investment in AI is paying off with advertisers in the fourth quarter of 2022 with over 20% more conversions than in the year before).

DEFRAGGING FEMINIST CYBERLAW

Amanda Levendowski†

ABSTRACT

In 1996, Judge Frank Easterbrook famously observed that any effort to create a field called cyberlaw would be "doomed to be shallow and miss unifying principles." He was wrong, but not for the reason other scholars have stated. Feminism is a unifying principle of cyberlaw, which alternately amplifies and abridges the feminist values of consent, safety, and accessibility. Cyberlaw simply hasn't been understood that way—until now.

In computer science, "defragging" means bringing together disparate pieces of data so they are easier to access. Inspired by that process, this Article offers a new approach to cyberlaw that illustrates how feminist values shape cyberspace and the laws that govern it. Consent impacts copyright law and fair use, the Digital Millennium Copyright Act (DMCA), criminal laws, and free speech. Each of those laws is informed by the invasive act of sharing nonconsensual intimate imagery, better known as "revenge porn." Two other laws, the Americans with Disabilities Act (ADA) and the recent amendments to Communications Decency Act (CDA) § 230, are crucial to promoting web accessibility for all people, including disabled people and sex workers. And safety influences privacy law and the Computer Fraud and Abuse Act, which affect the rights of pregnant people and targets of online harassment. This Article concludes that feminist cyberlaw is a new term, but feminism has always been foundational to making sense of cyberlaw.

TABLE OF CONTENTS

DOI: https://doi.org/10.15779/Z38KD1QM62

† Associate Professor of Law at Georgetown University Law Center. Thanks to Kendra Albert, Dan Bateyko, Erin Carroll, Julie Cohen, Sara Colangelo, Nakita Cutino, Sue Glueck, Megan Graham, Meg Leta Jones, Sonia Katyal, Naomi Mezey, Paul Ohm, Robin West, and Cameron Tepski for their thoughtful and generous comments. Dan Bateyko, Lexi Boynes, Eve Maynard, and Sherry Tseng provided stellar research assistance.

I. INTRODUCTION

On April 14, 1996, nineteen-year-old Jennifer Ringley made a choice that foretold the future of feminism in cyberspace.[1] She began broadcasting her daily life with a small webcam focused on her dorm room.[2] Every fifteen minutes, the webcam snapped a still image that automatically uploaded to her website, Jennice.[3] Viewers could tune in to the Jennicam to watch Ringley working.[4] Or getting ready for a night out.[5] Or preparing for a night in, sometimes with a boy.[6] Not surprisingly, the Jennicam captured Ringley in

1. *See generally* JOANNE MCNEIL, LURKING: HOW A PERSON BECAME A USER (Picador 2020) (recounting the impact of Jennicam); Reply All, *Jennicam*, GIMLET MEDIA, https://gimletmedia.com/shows/reply-all/8whoja (interviewing Jenni about Jennicam) [hereinafter Reply All, *Jennicam*]. For a discussion of the brief collapse of the Reply All podcast, see Jenny Gross, *Host of 'Reply All' Podcast Takes Leave of Absence After Accusations of Toxic Culture*, N.Y. TIMES (Feb. 18, 2021), https://www.nytimes.com/2021/02/18/business/media/pj-vogt-reply-all.html. The word "cyberspace" is widely misattributed to a man, when it was coined in the late 1960s by artist Susanne Ussing. Jacob Lillemose & Mathias Kryger, *The (Re)invention of Cyberspace*, KUNSTKRITIKK, NORDIC ART REV. (Aug. 24, 2015), https://kunstkritikk.com/the-reinvention-of-cyberspace/. This Article uses "cyberspace" interchangeably with "the internet," "online," and "the web."

2. Linton Weeks, *Jenni, Jenni, Jenni: A Life Laid Bare on the Computer Screen*, L.A. TIMES (Oct. 1, 1997), https://www.latimes.com/archives/la-xpm-1997-oct-01-ls-37894-story.html [hereinafter Weeks, *A Life Laid Bare*]; Jennifer Ringley, *Frequently Asked Questions*, JENNICAM (Dec. 10, 1997), https://web.archive.org/web/19971210110509/http:/www.boudoir.org/faq/jenni.html. It's been suggested that Ringley's attachment to her webcam amounted to creating one of cyberspace's first cyborgs. PopMatters Staff, *The New Cyborgs: Cyberculture and Women's Webcams*, POPMATTERS (June 7, 2000), https://www.popmatters.com/000607-lee-2496033552.html.

3. "Jennicam" has been stylized over the years as JenniCam, JenniCAM, and Jennicam—this Article adopts the latter. Reply All, *Jennicam*, *supra* note 1.

4. Weeks, *A Life Laid Bare*, *supra* note 2.

5. Reply All, *Jennicam*, *supra* note 1.

6. *Id.*

various states of nudity.[7] (Ringley rejected the label of pornography.)[8] Mostly male fans of all ages became obsessed with her feed.[9] Views grew to more than one hundred million each day.[10] Someone started a dedicated Jennicam Internet Relay Chat (IRC) channel.[11] Someone else created a website dedicated to her feet.[12] She was featured on This American Life, appeared on The David Letterman Show, and guest starred on the television series Diagnosis Murder.[13]

But not everyone was a fan. After the Jennicam broadcast Ringley having sex with a fellow camgirl's fiancé, she became a target for harassment.[14] Some women adopted whorephobic rhetoric and criticized Ringley.[15] A prominent legal scholar likened her to a "call girl."[16] A Washington Post writer called her a "redheaded little minx" and an "amoral man-trapper."[17] She also received avalanches of "lewd, rude, and crude" emails.[18] Those emails escalated to death threats accompanied by demands that she "show more."[19] In 2003, she pulled the plug on Jennicam and went almost entirely dark.[20]

Ringley's experience encapsulated a trio of feminist values—consent, accessibility, and safety, which often overlap—that inform cyberspace. While the feminist value of consent is complex and contested, it has long been central to feminist discourse.[21] Ringley chose to broadcast her life online freely. Information accessibility drove women to establish many of the first American

---

7. *Id.*

8. Weeks, *A Life Laid Bare*, *supra* note 2.

9. Thomas C. Hall, *JenniCam's So-Called Life Goes Live*, WASH. BUS. J. (Jan. 19, 1998), https://www.bizjournals.com/washington/stories/1998/01/19/tidbits.html.

10. Reply All, *Jennicam and the Birth of 'Lifecasting*,' DIGG (Apr. 13, 2015), https://digg.com/2015/reply-all-jennicam.

11. *Id.*

12. *Id.*

13. This American Life, *Tales from the Net*, CHI. PUB. RADIO (CBS television broadcast June 6, 1997), https://www.thisamericanlife.org/66/tales-from-the-net; *Diagnosis Murder: Rear Windows* (Nov. 12, 1998), https://www.youtube.com/watch?v=flDGYMwHFwE.

14. Lib Copel, *All a Woman Can Bare*, WASH. POST (Aug. 26, 2000), https://www.washingtonpost.com/archive/lifestyle/2000/08/26/all-a-woman-can-bare/f104e1fc-7cc1-47ca-acad-53193eb1c18b/.

15. *Id.*

16. Anita Allen, *Gender and Privacy in Cyberspace*, 52 STAN. L. REV. 1175, 1191 (2000).

17. Lib Copel, *All a Woman Can Bare*, WASH. POST (Aug. 26, 2000), https://www.washingtonpost.com/archive/lifestyle/2000/08/26/all-a-woman-can-bare/f104e1fc-7cc1-47ca-acad-53193eb1c18b/.

18. Weeks, *A Life Laid Bare*, *supra* note 2.

19. Hugh Hart, *April 14, 1996: JenniCam Starts Lifecasting*, WIRED (Apr. 14, 2020), https://www.wired.com/2010/04/0414jennicam-launches/.

20. *But see* Reply All, *Jennicam*, *supra* note 1.

21. Robin West, *Sex, Law and Consent*, *in* THE ETHICS OF CONSENT: THEORY AND PRACTICE (Alan Wetheimer & William Miller eds., Ox. Academic Press 2009).

libraries. [22] Ringley had physical access to a webcam and an internet connection, and the technical ability to create a website that other people could access in turn. The longtime work of domestic violence advocates protecting clients from abuse reveals the importance of safety.[23] Ringley received abuse and harassment in retaliation for Jennicam. But the development of responsive governance addressing these values was not a given.

The same year Ringley launched Jennicam, the co-founder of the Electronic Frontier Foundation, John Perry Barlow, issued *A Declaration of the Independence of Cyberspace*. He stated, "Governments of the Industrial World, you weary giants of flesh and steel, I come from Cyberspace, the new home of Mind. On behalf of the future, I ask you of the past to leave us alone. You are not welcome among us. You have no sovereignty where we gather."[24] He added that citizens of cyberspace were "creating a world that all may enter without privilege or prejudice accorded by race, economic power, military force or station of birth." [25] Barlow specifically mentioned race and socioeconomic status, but he didn't explore how an ungoverned cyberspace would affect women, queer, disabled, or other marginalized people. Ringley's experiences suggested that a largely unregulated cyberspace affected women differently—and not for the better.

But the alternative was not necessarily preferable. As early as the 1980s, Congress and courts embraced the task of governing cyberspace, even when both barely understood it.[26] Scholars reacted. A new field developed to study

22. *See generally* Anne Firor Scott, *Women and Libraries*, 21 J. LIBR. HIST. (1974–1987) 253 (1986) (noting that "[p]erhaps 75 percent of [public] libraries were initiated by women's groups, often originally for their own use").

23. *See generally* Deborah Epstein, Margret Bell & Lisa Goodman, *Transforming Aggressive Prosecution Policies: Prioritizing Victims' Long-Term Safety in the Prosecution of Domestic Violence Cases*, 11 AM. U. J. GENDER, SOCIAL POL'Y & L. 465 (2003) (discussing that abuse can be from an abuser as well as the state).

24. John Perry Barlow, *A Declaration of the Independence of Cyberspace*, ELEC. FRONTIER FOUND. (Feb. 8, 1996), https://www.eff.org/cyberspace-independence. The Declaration was written from Davos, Switzerland. Barlow's manifesto has been critiqued for its incomplete vision of cyberspace, including the threats from corporations rather than governments. *See, e.g.*, April Glaser, *The Incomplete Vision of John Perry Barlow*, SLATE (Feb. 8, 2018), https://slate.com/technology/2018/02/john-perry-barlow-gave-internet-activists-only-half-the-mission-they-need.html.

25. John Perry Barlow, *A Declaration of the Independence of Cyberspace*, ELEC. FRONTIER FOUND. (Feb. 8, 1996), https://www.eff.org/cyberspace-independence.

26. *See, e.g.*, 18 U.S.C. § 1030 (poorly drafted federal anti-hacking law enacted in 1986); Reno v. ACLU, 521 U.S. 844, 849 (1997) (Supreme Court clunkily explaining "cyberspace" for the first time).

laws that apply to computers, networks, and the internet, collectively called "cyberlaw."[27]

Early cyberlaw scholarship focused on governance mechanics.[28] Throughout the nineties and mid-aughts, however, scholars increasingly explored how oppression colored people's experience of cyberspace and its governance. Sonia Katyal, Rebecca Tushnet, and Madhavi Sunder examined how digital intellectual property (IP) laws can disadvantage, and occasionally empower, marginalized people.[29] Danielle Citron and Julie Cohen explored where existing information laws and policies can fail those same communities.[30] Anita Allen, Jerry Kang, and Cheris Kramarae dove directly into issues at the intersection of gender, race, and cyberspace.[31] And Jane Bailey and Adrienne Telford advocated for using cyberfeminism to explore

27. *Cyberlaw*, BLACK'S LAW DICTIONARY (11th ed. 2019). "Cyberlaw" is attributed to Jonathan Rosenoer, who is credited with coining it in the mid-nineties. Jonathan Rosenoer, *CyberLaw, 25 Years Later: Innovation, Transformation, and an Emerging Backlash*, HARV. J.L. & TECH. DIGEST (Oct. 4, 2017), https://jolt.law.harvard.edu/digest/cyberlaw-25-years-later-innovation-transformation-and-an-emerging-backlash.

28. *See, e.g.*, Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207; Joel R. Reidenberg, *Governing Networks and Rule-Making in Cyberspace,* 45 EMORY L.J. 911 (1996); Dan L. Burk, *Federalism in Cyberspace,* 28 CONN L. REV. 1095 (1996); Lawrence Lessig, *Reading the Constitution in Cyberspace*, 45 EMORY L.J. 869 (1996); Julie E. Cohen, *Lochner in Cyberspace: The New Economic Orthodoxy of "Rights Management,"* 97 MICH. L. REV. 462 (1998); Lawrence Lessig, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501 (1999).

29. *See, e.g.*, Sonia Katyal, *Performance, Property, and the Slashing of Gender in Fan Fiction*, 14 AM. U. J. GENDER SO. POL'Y & L. 463 (2006) (noting that copyright law affects online "slash" fan fiction, which focuses on romantic or sexual relationships between same-sex characters, that is primarily written by women); Rebecca Tushnet, *My Fair Ladies: Sex, Gender, and Fair Use in Copyright*, 15 AM. U. J. GENDER, SOC. POL'Y & L. 273 (2007) (asserting that fair use favors sexualized critique); Anupam Chander & Madhavi Sunder, *Everyone's a Superhero: A Cultural Theory of "Mary Sue" Fan Fiction as Fair Use*, 95 CALIF. L. REV. 1 (2007) (arguing that copyright law affects fan fiction, largely authored by women, that subverts the hegemony of original texts); *see also* Dan L. Burk, *Copyright and Feminism in Digital Media*, 14 AM. U. J. GENDER, SOC. POL'Y & L. 519 (2006) (examining hypertext works through a feminist lens and offering a feminist critique of copyright).

30. *See, e.g.*, DANIELLE KEATS CITRON, HATE CRIMES IN CYBERSPACE (Harv. Univ. Press, 2014) (building on scholarship demonstrating that women and other marginalized people are uniquely targeted for privacy invasions and harassment online); *see also* JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE (Yale Univ. Press 2012) (asserting that information flows should not interfere with any person's capacity for play).

31. Anita L. Allen, *Gender and Privacy in Cyberspace*, 52 STAN. L. REV. 1175 (2000) (deconstructing impacts of race and gender); Jerry Kang, *Cyber-Race,* 113 HARV. L. REV. 1130 (2000) (discussing impact of race); Cheris Kramarae, *Technology Policy, Gender, and Cyberspace*, 4 DUKE J. GENDER L. & POL'Y 149 (1997) (describing impact of gender).

gendered dynamics in a technologically-sophisticated capitalist society.[32] Investigating the interplay between cyberspace and marginalized communities continues with more recent scholarship by Kendra Albert, Lindsey Barrett, Carys Craig, Hannah Bloch-Wehba, Mary Anne Franks, Kate Klonick, Karen Levy, Elizabeth Joh, Kristelia García, Andrew Gilden, Ngozi Okidegbe, Blake Reid, Vincent Southerland, and Ari Waldman.[33] So far, this work has been dynamic, diverse, and diffuse.

---

32. Jane Bailey & Adrienne Telford, *What's So "Cyber" About It?: Reflections on Cyberfeminism's Contribution to Legal Studies*, 19 CAN. J. WOMEN & L. 243, 245 (2013). Donna Haraway's *a Cyborg Manifesto: Science, Technology, and Socialist Feminism in the Late Twentieth Century*, *in* SIMIANS, CYBORGS, AND WOTNETT: THE REINVENTION OF NATURE (Donna Haraway ed., Routledge 1991) was foundational to the formation of cyberfeminism.

33. *See, e.g.*, Kendra Albert, *Five Reflections from Four Years of FOSTA/SESTA*, CARDOZO ARTS & ENTM'T L.J. (forthcoming 2022) (discussing amendments to Communications Decency Act § 230 harm sex workers); Lindsey Barrett, *Rejecting Test Surveillance in Higher Education*, 1 MICH. ST. L. REV. (forthcoming 2023) (explaining that proctoring software negatively impacts students, disabled people, and people of color); Carys J. Craig, Joseph F. Turcotte & Rosemary J. Coombe, *What's Feminist About Open Access?: A Relational Approach to Copyright in the Academy*, 1 FEMINIST@LAW 1 (2011) (providing a feminist critique of copyright and deploying open access paradigms as a counterpoint to those critiques); Hannah Bloch-Wehba, *Automation in Moderation*, 53 CORNELL INT'L L.J. 41 (2020) (arguing that automated content moderation policies disproportionately impact marginalized people); Mary Anne Franks, *Unwilling Avatars: Idealism and Discrimination in Cyberspace*, 20 COLUM. J. GENDER & L. 224 (2011) (asserting that cyberspace idealists overlook and underestimate harms inflicted on women and other marginalized people online); Kate Klonick, *Re-Shaming the Debate: Social Norms, Shame, and Regulation in an Internet Age*, 75 MD. L. REV. 1029 (2016) (explaining how online shaming can amount to harassment that targets women and marginalized people); Karen Levy, *Intimate Surveillance*, 51 ID. L. REV. 679 (2015) (discussing technology betrays the privacy of women and other people in intimate relationships); Elizabeth E. Joh, *Artificial Intelligence and Policing: First Questions*, 41 SEATTLE U. L. REV. 1139 (2018) (explaining artificial intelligence systems are dangerous when integrated with the criminal legal system, which disproportionately affects people of color); Chris Buccafusco & Kristelia García, *Pay-to-Playlist: The Commerce of Music Streaming*, 12 U.C. IRVINE L. REV. 805 (2022) (discussing how copyright governs online streaming affects women and Black artists); Andrew Gilden, *Cyberbullying and the Innocence Narrative*, 48 HARV. C.R.-C.L. L. REV. 357 (2013) (discussing gay teens are especially likely to be targeted for online harassment); Blake E. Reid, *Internet Architecture and Disability*, 95 IND. L.J. 591 (2020) (discussing the internet remains inaccessible to many people with disabilities); Vincent Southerland, *The Intersection of Race and Algorithmic Tools in the Criminal Legal System*, 80 MD. L. REV. 487 (2021) (explaining algorithmic tools in the criminal legal system disproportionately impact marginalized people); Ezra Waldman, *Law, Privacy, and Online Dating: "Revenge Porn" in Gay Online Communities*, 44 L. & SOC. INQ. 987 (2019) (explaining nonconsensual intimate imagery targets queer men as well as women). I have also written in this space. *See, e.g.*, Amanda Levendowski, *How Copyright Law Can Fix Artificial Intelligence's Implicit Bias Problem*, 93 WASH. L. REV. 579 (2018) (invoking fair use can create fairer artificial intelligence for women, queer people, and other marginalized people).

In computer science, "defragging" means bringing together disparate pieces of data so they are easier to access.[34] Inspired by that process, this Article brings together cyberlaw doctrines in a new way that makes it easy to see how feminism shapes cyberspace and the laws that govern it. Such a claim is counterintuitive. Men are credited with building the internet.[35] Men founded its most dominant websites.[36] Mostly men enact laws that govern those sites.[37] And mostly men interpret those laws.[38] Yet feminist values and reactions to them play a central role in the development of cyberlaw doctrines.

Feminist cyberlaw uses intersectional feminism to understand how cyberlaws contribute to the oppression and liberation of marginalized people. bell hooks defined intersectional feminism broadly, meaning "the movement

34. Whitson Gordon, *What is "Defragging," and Do I Need to Do It to My Computer?*, LIFEHACKER (Jan. 16, 2013), https://lifehacker.com/what-is-defragging-and-do-i-need-to-do-it-to-my-comp-5976424.

35. This is, unsurprisingly, a misconception. *See generally* CLARE L. EVANS, BROAD BAND: THE UNTOLD STORY OF THE WOMEN WHO MADE THE INTERNET (Portfolio 2018) (debunking the myth of male geniuses creating cyberspace).

36. All of the top five most visited websites were founded by men—sometimes multiple men. *Top Websites Ranking*, SIMILARWEB (2023), https://www.similarweb.com/top-websites/. *From the Garage to the Googleplex*, GOOGLE (2002), https://about.google/our-story/ (Google co-founders Larry Page and Sergey Brin); Christopher McFadden, *YouTube's History and Its Impact on the Internet*, INTERESTING ENG'G (May 20, 2021), https://interestingengineering.com/culture/youtubes-history-and-its-impact-on-the-internet (featuring YouTube co-founders Chad Hurley, Steve Chen, and Jawad Karim); *Mark Zuckerberg, Founder, Chairman and Chief Executive Officer*, META (2022), https://about.facebook.com/media-gallery/executives/mark-zuckerberg/ (Facebook founder Mark Zuckerberg); Nicholas Carlson, *The Real History of Twitter*, INSIDER (Apr. 13, 2011), https://www.businessinsider.com/how-twitter-was-founded-2011-4?op=1 (featuring Twitter co-founders Jack Dorsey, Noah Glass, Biz Stone, and Evan Williams); Avery Hartmans, *The Rise of Kevin Systrom, Who Founded Instagram 10 Years Ago and Built It Into One of the Most Popular Apps in the World*, BUS. INSIDER (Oct. 6, 2020), https://www.businessinsider.com/kevin-systrom-instagram-ceo-life-rise-2018-9 (featuring Instagram co-founders Kevin Systrom and Mike Krieger). The founders are also overwhelmingly white. *Id.*

37. In 2021, Congress was comprised of the highest number of women in history—just 27%. Carrie Blazina & Drew DeSilver, *A Record Number of Women are Serving in the 117th Congress*, PEW RSCH. CTR. (Jan. 15, 2021), https://www.pewresearch.org/fact-tank/2021/01/15/a-record-number-of-women-are-serving-in-the-117th-congress/. Congress also remains overwhelmingly white, with only 23% members identifying as racial or ethnic minorities—a record. Katherine Schaefer, *Racial, Ethnic Diversity Increases Yet Again with the 117th Congress*, PEW RSCH. CTR. (Jan. 28, 2021), https://www.pewresearch.org/fact-tank/2021/01/28/racial-ethnic-diversity-increases-yet-again-with-the-117th-congress/.

38. Women comprise just under 33% of the federal judiciary, which is also a whopping 74% white. *January 20, 2021 Snapshot: Diversity of the Federal Bench*, AM. CONST. SOC'Y (2022), https://www.acslaw.org/judicial-nominations/january-20-2021-snapshot-diversity-of-the-federal-bench/.

to end sexism, sexist exploitation, and oppression."[39] Intersectionality, a term coined by scholar Kimberlé Crenshaw, is:

> a prism, for seeing the way in which various forms of inequality often operate together and exacerbate each other. We tend to talk about race inequality as separate from inequality based on gender, class, sexuality or immigrant status. What's often missing is how some people are subject to all of these, and the experience is not just the sum of its parts.[40]

Intersectional feminism recognizes that oppression comes from many sources and provides a framework for addressing the oppression of people with overlapping identities, such as Black women, queer women, disabled women, poor women, women crime victims, women across these identities, and even oppressed people who are not women at all.[41] This means that hooks' intersectional feminism is expansive; it arguably threatens to swallow all equitable movements.[42] But a broad approach is crucial to realizing that equity for women that fails to dismantle oppression broadly reflects a privileged and partial feminism.[43]

---

39. BELL HOOKS, FEMINISM IS FOR EVERYBODY: PASSIONATE POLITICS viii (South End Press 2000). Intersectional feminism stands in opposition to so-called white feminism, which can overlap with radical feminism and is prevalent within technology generally. *Compare* SHERYL SANDBERG, LEAN IN: WOMEN, WORK, AND THE WILL TO LEAD (2013) (describing "feminist" strategies for relatively privileged white women to navigate white collar workplaces) *with* MIKKI KENDALL, HOOD FEMINISM: NOTES FROM THE WOMEN THAT A MOVEMENT FORGOT 2 (Penguin 2020) ("[W]hite feminism tends to forget that a movement that claims to be for all women has to engage with the obstacles women who are not white face.").

40. Katy Steinmetz, *She Coined the Term 'Intersectionality' Over 30 Years Ago. Here's What It Means to Her Today*, TIME (Feb. 20, 2020), https://time.com/5786710/kimberle-crenshaw-intersectionality/ (interviewing Kimberlé Crenshaw about the meaning and impact of intersectionality); Kimberlé W. Crenshaw, *Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory and Antiracist Politics*, 1989 U. CHI. LEGAL F. 139 (1989) (establishing the concept of "intersectionality").

41. *See, e.g.*, Darren Rosenblum, *Queer Intersectionality and the Failure of Recent Lesbian and Gay "Victories*," 4 L. & SEXUALITY 83 (1994) (discussing limited triumphs of queer liberation to queer people of color, trans people, and poor people); Jennifer Bennett Shinall, *The Substantially Impaired Sex: Uncovering the Gendered Nature of Disability Discrimination*, 101 MINN. L. REV. 1099 (2017) (describing discrimination against disabled women and disabled women of color); Sarah Schindler, *Architectural Exclusion: Discrimination and Segregation Through Physical Design of the Built Environment*, 124 YALE L.J. 1934 (2015) (detailing subordination on the basis of race and socioeconomic status).

42. It certainly overlaps with aspects of lesbian and critical race feminism.

43. *Compare* SHERYL SANDBERG, LEAN IN: WOMEN, WORK, AND THE WILL TO LEAD (2013) *with* Kimberlé W. Crenshaw, *Demarginalizing the Intersection of Race and Sex: A Black Feminist Critique of Antidiscrimination Doctrine, Feminist Theory, and Antiracist Politics*, 1989 U. CHI. LEGAL F. 139, 140 (1989) (coining the term "intersectionality" to illuminate how overlapping characteristics, such as race and gender, create interlocking systems of oppression); Patricia

However, a different flavor of feminism has been a pervasive and persistent force in cyberlaw: radical feminism.[44] Pioneered by scholar Catharine MacKinnon and popularized throughout the 1970s, radical feminism focuses on the belief that women's oppression by men is responsible for the inequities that women experience economically, politically, and socially.[45] Within this framework, men are privileged and women are subordinated.[46] Radical feminists are not a monolith, but this Article details how radical and its adjacent feminisms shaped cyberlaw, from the embrace of criminal law to promote feminist goals to hostility toward pornography and sex workers.[47]

The approaches and doctrines discussed in this Article are illustrative, not exhaustive. Alternate feminist movements, such as liberal feminism and critical race feminism, hold insights into feminist cyberlaw.[48] Critical theories, including queer and critical race theory, provide additional cyberlaw perspectives.[49] Beyond the lens of law, interdisciplinary methodologies, such as value-sensitive design and design justice, conceptualize the flaws and transformative potential of cyberspace.[50] Among legal doctrines, other intellectual property doctrines, such as patents, trademarks, and trade secrets,

---

Hill Collins, *Learning from the Outsider Within: The Sociological Significance of Black Feminist Thought*, 33 SOC. PROBS. 514 (1989) (contextualizing Black women's unique positionality to oppression).

44. Conservative feminism, which shares disapproving views regarding pornography and sex work with radical feminists, has also played an important role. Where relevant, the influence of other strands of feminist theory are identified with referrals to deeper dives into those approaches.

45. NANCY LEVIT & ROBERT R. M. VERCHICK, FEMINIST LEGAL THEORY 23 (2016). *See generally* CATHARINE MACKINNON, SEXUAL HARASSMENT OF WORKING WOMEN (Yale U. Press 1979) (launching radical feminism).

46. NANCY LEVIT & ROBERT R. M. VERCHICK, FEMINIST LEGAL THEORY 23 (2016).

47. *See infra* Section II.C, Part III, Section IV.B.

48. Select examples of additional feminisms include equal treatment, cultural, lesbian, ecofeminism, pragmatic, postmodern, and Marxist feminism. *See generally* NANCY LEVIT & ROBERT R. M. VERCHICK, FEMINIST LEGAL THEORY (2016); Abbe Smith, *Can You Be a Feminist and a Criminal Defense Lawyer*, 57 AM. CRIM. L. REV. 1569 (2020).

49. *See generally* DINO FELLUGA, CRITICAL THEORY: THE KEY CONCEPTS (Routledge 2015); CRITICAL RACE THEORY: THE KEY WRITINGS THAT FORMED THE MOVEMENT (Kimberlé W. Crenshaw, Neil Gotanda, Gary Peller & Kendall Thomas eds., The New Press 1996).

50. *See generally* BATYA FRIEDMAN & DAVID G. HENDRY, VALUE SENSITIVE DESIGN (MIT Press 2019) (accounting for human values in design processes); SASHA COSTZANA-CHOCK, DESIGN JUSTICE: COMMUNITY-LED PRACTICES TO BUILD THE WORLDS WE NEED (MIT Press 2020) (advocating design led by marginalized communities). So does data feminism. CATHERINE D'IGNAZIO & LAUREN F. KLEIN, DATA FEMINISM (MIT Press 2020) (advancing feminist values in data practices).

can be understood through feminist cyberlaw.[51] So are governance doctrines, such as those surrounding data protection, cybersecurity, labor, and antitrust.[52] International perspectives, both comparatively and on their own terms, hold insights into these and many more doctrines.[53] Each and all these topics are ripe subjects for future feminist cyberlaw scholarship.[54]

This Article begins that conversation by illuminating how a handful of core cyberlaw doctrines both undermine and underscore what I call the "Ringley Trifecta" of feminist values: consent, accessibility, and safety. Some of those cyberlaw doctrines were born of the internet, such as the DMCA, and others have become tethered to it intimately, such as privacy law. This Article offers a sharp taxonomy of cyberlaws, including general laws that were not intended,

---

51. *See, e.g.*, Andrew Gilden & Sarah R. Wasserman Rajec, *Pleasure Patents*, 63 B.C. L. REV. 571 (2022) (discussing patents for sexual pleasure, including virtual reality systems); Amanda Levendowski, *Trademarks as Surveillance Transparency*, 36 BERKELEY TECH. L.J. 439 (2021) (detailing how to discover secret surveillance technologies using the federal trademark register); Alexandra J. Roberts, *Oppressive and Empowering #Tagmarks*, *in* FEMINIST CYBERLAW (Meg Leta Jones & Amanda Levendowski eds., forthcoming 2024) (describing how marginalized communities resist and embrace proprietary activist hashtags trademarks) (building on Alexandra J. Roberts, *Tagmarks*, 105 CALIF. L. REV. 599 (2017)); Rebecca Wexler, *Life, Liberty and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343 (2018) (detailing how trade secrecy is invoked to shield algorithms from disclosure in criminal legal proceedings); Sonia Katyal, *The Paradox of Source Code Secrecy*, 104 CORNELL L. REV. 1183 (2019) (discussing interventions to prevent invocation of trade secrecy in criminal legal proceedings).

52. *See, e.g.*, MEG LETA JONES, CTRL+Z: THE RIGHT TO BE FORGOTTEN 5, 59, 86, 156, 161 (N.Y.U. Press 2016) (discussing effects of a permanent internet on women); Karen Levy & Bruce Schneier, *Privacy Threats in Intimate Relationships*, 6 J. CYBERSECURITY 1 (2020) (https://doi.org/10.1093/cybsec/tyaa006) (discussing effects of intimate partner relationship on cybersecurity interventions); Amazon.com Services *and* Retail, Wholesale, and Department Store Union, Case 10-RC-269250 (Nat'l Labor Relations Bd. Aug. 2, 2021), https://www.documentcloud.org/documents/21033629-hearing-officers-report-in-amazon-case-no-10-rc-269250 (recommending that low-income Amazon workers hold new election whether to unionize despite attempted Amazon interference); Gabreille Rejouis, *Black Feminist Antitrust for a Safer Social Media*, *in* FEMINIST CYBERLAW (Meg Leta Jones & Amanda Levendowski eds., forthcoming 2024) (calling for the application of Black feminist principles to antitrust).

53. *See, e.g.*, Edward Carter, *Argentina's Right to Be Forgotten*, 27 EMORY INT'L L. REV 23 (2013); Sylwia Ćmiel, *Cyberbullying Legislation in Poland and Select EU Countries*, 109 PROCEDIA SOC. & BEHAV. SCI. 29 (2014); Fawzia Cassim, *Addressing the Growing Spectre of Cyber Crime in Africa: Evaluating Measures Adopted by South African and Other Regional Role Players*, 44 COMPAR. & INT'L L. S. AFR. 123, 123–38 (2011); Daniel J. Ryan, Maeve Dion, Eneken Tikk & Julie J. C. H. Ryan, *International Cyberlaw: A Normative Approach*, 42 GEO. J. INT'L L. 1161 (2011); Renata de Lima Machado Rocha, Roberta Duboc Pedrinha & Maria Helena Barros de Oliveira, *The Treatment of Revenge Pornography by the Brazilian Legal System*, 43 SAÚDE DEBATE (2019).

54. My colleague Meg Leta Jones and I have asked colleagues to begin exploring these topics in our forthcoming edited volume. FEMINIST CYBERLAW (Meg Leta Jones & Amanda Levendowski eds., forthcoming 2024).

but nevertheless operate, as cyberlaws. The first category includes cyberlaws that can be appropriated for feminist goals, such as furthering feminist values. These laws are civil, and creative deployment of these general laws can promote the feminist values of consent and accessibility. Using the DMCA to remove nonconsensual intimate imagery is one example. The second category includes cyberlaws that cannot be appropriated for feminist goals. These laws are both civil and criminal, and they are intertwined with the feminist values of consent, accessibility, and safety. However, they are not equipped to consistently promote those values, but merely engage with them. Privacy, which has recently been gutted by the Supreme Court and no longer shields pregnant people from invasive scrutiny, illustrates this category. And the final category is feminist cyberlaws that can subvert feminist goals. These laws are enacted as cyberlaws with a feminist purpose, such as criminalizing nonconsensual intimate imagery or banning content promoting sex trafficking. However, their breadth means that these laws can be weaponized against marginalized people, threatening their safety and undermining their consent. These categories are contextual and flexible, and they offer the beginnings of a broader conversation about cyberlaws.

To begin the work of illuminating feminism's role in cyberlaw, this Article proceeds in three Parts after this Introduction. Each Part analyzes a cyberlaw doctrine through one aspect of the Ringley Trifecta—consent, accessibility, and safety—by recounting the history of the doctrine, discussing how it promotes or subverts the central feminist value, and reflecting on the implications of those effects for both feminism and cyberlaw.

Part II examines how consent impacts copyright law and fair use, the DMCA, criminal laws, and free speech. The copyright doctrine of fair use allows other people to use copyrighted works without consent under certain conditions—and without concern for the desires of photographic subjects.[55] The DMCA was enacted to prevent accessing others' content without consent, which can include the distribution of nonconsensual intimate imagery.[56] The latter issue has also encouraged scholars to call for new criminal laws combatting consentless invasions of privacy and dignity.[57]

Part III explores the importance of accessibility by considering the effects of the ADA and the FOSTA/SESTA amendments to Communications Decency Act (CDA) § 230 on web accessibility.[58] Activist plaintiff lawyers

55. 17 U.S.C. § 107.

56. 17 U.S.C. § 512; 18 U.S.C. § 1030.

57. *Infra* Sections I.B, II.C, IV.A.

58. FOSTA/SESTA is the colloquial term for the twin bills known as the Allow States and Victims to Fight Online Sex Trafficking Act and Stop Enabling Sex Traffickers Act.

made web accessibility for disabled people an urgent legal issue by strategically suing corporations with inaccessible websites.[59] But technological access is not the only hurdle for an accessible cyberspace. After the enactment of the FOSTA/SESTA amendments to CDA § 230, sex workers found themselves increasingly isolated from the internet due to overaggressive content moderation policies adopted by interactive service providers, a trend that is bearing out with other marginalized communities as well.[60]

And Part IV exposes how safety influences privacy law and the Computer Fraud and Abuse Act (CFAA). Increasingly, abuse is facilitated by cyberspace. Technologically tracking abortion doctors and pregnant people exposes both groups to increased risks of harassment by both anti-abortion activists and police.[61] Computers are used to spread hateful messages or fantasize about hurting women.[62] In both cases, the law cannot be appropriated to counter these harms—occasionally for the better. This Article concludes that feminist cyberlaw is a new term, but feminism has always been foundational to making sense of cyberlaw.

II. IMPACT OF CONSENT ON CYBERLAW

Women's bodies inspired the modern internet. In 2000, a Google co-founder directed his engineers to create a tool for finding photographs of Jennifer Lopez in a breast- and belly-button-baring gauzy green gown.[63] Three years later, a Harvard student secretly scraped his women classmates' photographs to create a database dedicated to ranking their hotness.[64] The following year, three engineers launched YouTube so searchers could watch Justin Timberlake nonconsensually reveal Janet Jackson's breast during their

59. Minh Vu, Kristina Launey & John Egan, The Law on Website and Mobile Accessibility *Continues to Grow at a Glacial Pace Even as Lawsuit Numbers Reach All-Time Highs*, AM. BAR ASS'N. (Jan. 1, 2022), https://www.americanbar.org/groups/law_practice/publications/law_practice_magazine/2022/jf22/vu-launey-egan/.

60. MTV News Staff, *How the Social Media Censorship of Sex Workers Affects Us All*, MTV (Oct. 29, 2019), https://www.mtv.com/news/uozyys/sex-work-censorship-effects.

61. *Infra* Section IV.A.

62. United States v. Drew, 259 F.R.D. 449, 452 (C.D. Cal. 2009); United States v. Valle, 807 F.3d 508, 528 (2d Cir. 2015).

63. Eric Schmidt, *The Tinkerer's Apprentice*, PROJECT SYNDICATE (Jan. 19, 2015), https://www.project-syndicate.org/onpoint/google-european-commission-and-disruptive-technological-change-by-eric-schmidt-2015-01; Rachel Tashjian, *How Jennifer Lopez's Versace Dress Created Google Images*, GQ (Sept. 20, 2019), https://www.gq.com/story/jennifer-lopez-versace-google-images.

64. Katharine A. Kaplan, *Facemash Creator Survives Ad Board*, HARV. CRIMSON (Nov. 19, 2003), https://www.thecrimson.com/article/2003/11/19/facemash-creator-survives-ad-board-the/.

Super Bowl halftime show.[65] But a decade before the male gaze was credited with internet ingenuity, early 1990s sex workers laid foundations for the present web by curating chat rooms, patronizing ecommerce sites, and creating online ads to help new users seek out nudity—with consent.[66]

That irresistible impulse drove early internet governance. Just one year before Barlow unveiled his manifesto, then-Senator James Exon proclaimed that "[t]he information superhighway should not become a red-light district."[67] In the ensuing decades, platforms heeded his call by punishing online nudity, often targeting sex workers and queer people, sometimes lacking formal legal requirements to do so, and consistently creating a pattern of innovation and retaliation. Sex workers originated taking credit card payments for online transactions.[68] Years later, growing numbers of credit card companies and other payment platforms refused to do business with them.[69] Sex workers embraced online personal ads to promote their services.[70] Threatened by state

65. Alessandra Stanley, *The TV Watch; A Flash of Flesh: CBS Against Is in Denial*, N.Y. TIMES (Feb. 3, 2004), https://www.nytimes.com/2004/02/03/arts/the-tv-watch-a-flash-of-flesh-cbs-again-is-in-denial.html; Rob Sheffield, *YouTube Origins: How Nipplegate Created YouTube*, ROLLING STONE (Feb. 11, 2020), https://www.rollingstone.com/culture/culture-features/youtube-origin-nipplegate-janet-jackson-justin-timberlake-949019/. Timberlake offered meager and belated apologies to Jackson—and his ex-girlfriend Britney Spears, whom he also mistreated—more than a decade after the incident. Julia Jacobs, *Justin Timberlake Apologizes to Britney Spears and Janet Jackson*, N.Y. TIMES (Mar. 4, 2021), https://www.nytimes.com/2021/02/12/arts/music/justin-timberlake-statement-britney-spears.html.

66. Decoding Stigma, *Sex Workers Built the Internet: An Oral History Roundtable Tracing the Early Days of An Internet Built on Desire, Erotic Labor, Communal Care, and Animated GIFs*, NEW SCHOOL FOR SOC. RSCH. (Apr. 22, 2022), https://www.youtube.com/watch?v=C15TvZiJ95k. *See generally* HEATHER BERG, PORN WORK: SEX, LABOR, AND LATE CAPITALISM (2021) (discussing the perspectives of people engaged in sex work are complex and non-monolithic).

67. Sarah Jeong, *How Naked Women Shaped the Internet*, DENVER POST (Aug. 27, 2016) (reprinted from WASH. POST, paywalled), https://www.denverpost.com/2016/08/27/how-naked-women-shaped-the-internet/.

68. Decoding Stigma, *supra* note 66.

69. VALERIE WEBBER, THE IMPACT OF MASTERCARD'S ADULT CONTENT POLICY ON ADULT CONTENT CREATORS (2022), https://drive.google.com/file/d/1167acd62YZqc-j7guzeiOqPjbh3pW03w/view; Samantha Cole, *'War Against Sex Workers': What Visa and Mastercard Dropping Pornhub Means to* Performers, MOTHERBOARD (Dec. 11, 2020), https://www.vice.com/en/article/n7v33d/sex-workers-what-visa-and-mastercard-dropping-pornhub-means-to-performers; Natasha Tusikov, *Censoring Sex: Payment Platforms' Regulation of Sexual Expression*, 26 SOCIO. CRIME, L. & DEVIANCE 63 (2021), https://www.emerald.com/insight/content/doi/10.1108/S1521-613620210000026005/full/html.

70. Decoding Stigma, *supra* note 66.

attorneys general and Congress, those services folded.[71] Sex workers and queer people created some of the original social networks.[72] Yet many mainstream platforms censor their content.[73]

Unsurprisingly, corporations, Congress, and even courts remain uncomfortable with nude bodies, particularly women's.[74] This Part uses consent to explore how governing nudity in cyberspace plays out across copyright law, criminal law and enforcement, and free speech doctrine. Section II.A looks to copyright law, where Google's appropriation of nude models' photographs paved the way for other digital fair uses. In this critical case, however, the judge made no mention that the models never consented to their images becoming more easily findable online because copyright law considers such issues legally irrelevant. In other issues of nonconsensual use, however, the law is surprisingly responsive. Section II.B unpacks how the notice-and-takedown provisions of the DMCA can effectively take down intimate images shared online without consent, known as nonconsensual intimate imagery.[75] But not all scholars and activists agree that civil remedies are the right approach to privacy invasions as repugnant as nonconsensual intimate imagery

71. Julie Adler, *The Public's Burden in a Digital Age: Pressures on Intermediaries and the Privatization of Internet Censorship*, 20 J. L. & POL'Y 231 (2011) (discussing the folding of Craigslist adult services and law enforcement seizing of Backpage). One of those services, Backpage, had an alarming history of nonconsensual sex trafficking victims also appearing in its pages. *See, e.g.*, Jane Doe No. 1 v. Backpage.com LLC, 817 F.3d 12, 16 (1st Cir. 2016).

72. Decoding Stigma, *supra* note 66.

73. *Platforms Which Discriminate Against Sex Workers*, SURVIVORS AGAINST SESTA (June 7, 2022), https://survivorsagainstsesta.org/platforms-discriminate-against-sex-workers/; *see also* Paris Martineau, *Tumblr's Porn Ban Reveals Who Controls What We See Online*, WIRED (Dec. 4, 2010), https://www.wired.com/story/tumblrs-porn-ban-reveals-controls-we-see-online/; Brit Dawson, *Instagram's Problem with Sex Workers is Nothing New*, DAZED (Dec. 24, 2020), https://www.dazeddigital.com/science-tech/article/51515/1/instagram-problem-with-sex-workers-is-nothing-new-censorship; Reina Sultan, *Terms of Service: Inside Social Media's War on Sex Workers*, BITCH (Aug. 23, 2021), https://www.bitchmedia.org/article/inside-social-medias-war-on-sex-workers. Queer people's content, even when it contains no nudity, are also often censored under platforms' policies. Emily J. Born, *Too Far and Not Far Enough: Understanding the Impact of FOSTA*, 94 N.Y.U. L. REV. 1623, 1648–49 (2019); Rebecca Greenfield, *Why Is Tumblr Censoring #Gay Searches?*, ATLANTIC (July 22, 2013), https://www.theatlantic.com/technology/archive/2013/07/why-tumblr-censoring-gay-searches/313054/.

74. Amy Adler, *Girls! Girls! Girls! The Supreme Court Confronts the G-String*, 80 N.Y.U. L. REV 600 (2006), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=875840; I. India Thusi, *Reality Porn*, 96 N.Y.U. L. REV. 738 (2021), https://www.nyulawreview.org/issues/volume-96-number-3/reality-porn/.

75. In its early days, nonconsensual intimate imagery and its distribution was often called "revenge porn," a twofold misnomer: many distributions are for motivations besides revenge, and pornography is consensual. Nonconsensual intimate imagery distribution is also preferable to "nonconsensual pornography" for the latter reason.

distribution. Section II.C turns to advocacy for criminal nonconsensual intimate imagery distribution laws which, not unlike early radical feminist legislation banning pornography, raise First Amendment overbreadth concerns. Calls for criminalization also urge reflection about whether an oppressive criminal legal system can ever be harnessed for feminist goals. Each doctrine is impacted by how consent interacts with nudity, and feminist cyberlaw has something to say about all of them.

A. COPYING COPYRIGHTED NUDITY AS FAIR USE

Photographs of nude models paved the way for internet innovations like image search engines, plagiarism detection software, and accessible books for disabled people.[76] When Google launched its Image Search feature so users could ogle Jennifer Lopez's breasts, it displayed copies of iconic images from her Grammys appearance. Those images were not owned by Google or even Lopez—they belonged to organizations like Getty Images.[77] Google did not have consent to display any of those images, but it did so anyway. And it did the same when it displayed copies of photographs of nude models from an agency called Perfect 10.[78] Unlike the owners of Lopez's photographs, however, Perfect 10 sued.[79]

In 2007, seven years after the advent of Google Image Search, Perfect 10 sued Google for copyright infringement.[80] In theory, Perfect 10 had a point. Photographs, including those featuring nudity, are copyrightable.[81] The law

76. Perfect 10 v. Amazon, 508 F.3d 1146, 1155 (9th Cir. 2007) (search engines); A.V. *ex rel.* Vanderhye v. iParadigms, LLC, 562 F.3d 630 (4th Cir. 2009) (plagiarism detection software); Authors Guild v. HathiTrust, 755 F.3d 87 (2d Cir. 2014) (accessible library). Nudity also plays a role in offline fair use cases. *See, e.g.*, Nunez v. Caribbean Int'l News Corp., 235 F.3d 18 (1st Cir. 2000) (unsuccessfully challenging nonconsensual publication of nude and nearly nude photographs of Miss Puerto Rico Universe 1997).

77. Amy De Klerk, *Versace Just Recreated Jennifer Lopez's Iconic Grammy's Dress*, HARPER'S BAZAAR (Dec. 3, 2018), https://www.harpersbazaar.com/uk/fashion/fashion-news/a25378084/versace-recreated-jennifer-lopez-green-dress/; Scarlett Kilcooley-O'Halloran, *J Lo Responsible for Google Images*, VOGUE (Apr. 8, 2015), https://www.vogue.co.uk/article/j-lo-green-versace-dress-responsible-for-google-image-search.

78. *See generally* Perfect 10 v. Amazon, 508 F.3d 1146, 1155 (9th Cir. 2007).

79. Perfect 10 v. Google, 416 F. Supp. 2d 828, 834 (C.D. Cal. 2006), *aff'd in part, rev'd in part, remanded*; Perfect 10 v. Amazon, 508 F.3d 1146, 1155 (9th Cir. 2007) (alleging copyright infringement).

80. Perfect 10, Inc. v. Amazon.com, Inc., 508 F.3d 1146, 1154 (9th Cir. 2007). Perfect 10 also sued Google for trademark infringement and dilution. *Id.*

81. 17 U.S.C. § 102(5) (extending copyright to "pictorial, graphic, and sculptural works") (codifying Burrow-Giles Lithographic Co. v. Sarony, 111 U.S. 53 (1884)); Mitchell Bros. Film Grp. v. Cinema Adult Theater, 604 F.2d 852, 865 (5th Cir. 1979) (refusing an obscenity claim as a defense to copyright infringement).

entitles copyright owners to a set of exclusive rights, including display.[82] Appropriating exclusive rights in copyrighted works without authorization generally amounts to infringement.[83] Which is exactly what Google would seem to have done by consentlessly displaying thumbnails of Perfect 10 images responsive to Image Search queries.[84]

Copyright law was not designed to be feminist—indeed, many scholars have offered feminist critiques of copyright law.[85] The first copyright law, the Statute of Anne of 1710, was drafted and enacted by a British Parliament comprised of privileged white men, largely for the benefit of other privileged white men, to encode men's vision for the intersection of creativity and capitalism.[86] Most recently, the Copyright Act of 1976, largely drafted by a white woman named Barbara Ringer,[87] eliminated formalities for copyright registration and extended copyright terms, which made it more challenging for the public to access and reimagine copyrighted works.[88] And while copyright today protects works by authors of all genders, it also protects misogynistic,

82. 17 U.S.C. § 106(5) (reserving copyright owners' rights to "display the copyrighted work publicly").

83. 17 U.S.C. § 501(a). Perfect 10 also registered each of the images with the Copyright Office, a prerequisite for litigation. Perfect 10 v. Google, 416 F. Supp. 2d at 832; 17 U.S.C. § 412. Successful registration is now a prerequisite for litigating copyright infringement claims. Fourth Estate Benefit Corp. v. Wall-Street.com, 139 S. Ct. 881, 892 (2019).

84. Perfect 10 v. Google, 416 F. Supp. 2d at 833.

85. Instead, scholars have offered feminist critiques of copyright law. Ann Bartow, *Fair Use and the Fairer Sex: Gender, Feminism, and Copyright Law*, 14 AM. U. J. GENDER SOC. POL. & L. 551, 564 (2006); *see also* Dan L. Burk, *Copyright and Feminism in Digital Media*, 14 AM. U. J. GENDER, SOC. POL'Y & L. 519 (2006); Malla Pollack, *Towards a Feminist Theory of the Public Domain, or Rejecting the Scope of United States Copyrightable and Patentable Subject Matter,* 12 WM. & MARY J. WOMEN & L. 603 (2006); Rebecca Tushnet, *My Fair Ladies: Sex, Gender, and Fair Use in Copyright*, 15 AM. U. J. GENDER SOC. POL'Y & L. 273 (2007); Carys Craig, *Reconstructing the Author-Self: Some Feminist Lessons for Copyright Law*, 15 J. GENDER SOCIAL POL'Y & L. 207 (2007); Emily Chaloner, *A Story of Her Own: A Feminist Critique of Copyright Law*, 6 I/S: J.L. & POL'Y FOR INFO. SOC'Y 221 (2010).

86. Copyright Act of 1710, 8 Ann. c. 21 (encouraging learning by securing limited monopolies to authors and purchasers of copies); *see also* Ann Bartow, *Fair Use and the Fairer Sex: Gender, Feminism, and Copyright Law*, 14 AM. J. GENDER, SOC. POL'Y & L. 512, 557 (2006) (critiquing the patriarchal origins of copyright law).

87. For more information about the remarkable Ringer, who also helped codify fair use, see Amanda Levendowski, *The Lost and Found Legacy of Barbara Ringer*, ATLANTIC (July 11, 2014), https://www.theatlantic.com/technology/archive/2014/07/the-lost-and-found-legacy-of-a-copyright-hero/373948/.

88. 17 U.S.C. § 102 (stating that copyright subsists in "original works of authorship fixed in any tangible medium of expression," without mention of notice formalities or registration); 17 U.S.C. § 302 (generally extending term to life of the author plus seventy years).

racist, homophobic, ableist, and colonialist works as much as any others.[89] Yet copyright law is a general law that often operates as a cyberlaw, and it can be appropriated for feminist goals, such as encouraging the creativity of marginalized authors or shielding subjects from unwanted uses.[90] While Perfect 10 undoubtedly acted out of capitalist self-interest, its copyright lawsuit could have protected hundreds of models from the nonconsensual amplification of their nude photographs. However, copyright has a complex relationship with consent that complicates its ability to be appropriated for feminist goals and instead puts copyright into conflict with the value of consent.

That conflict is rooted in another area of copyright law, one that gave Google a powerful counterargument to allegations of infringement: its Image Search was fair use. The doctrine of fair use allows—even incentivizes—the use of copyrighted works without consent.[91] According to the Supreme Court, "[f]rom the infancy of copyright protection, some opportunity for fair use of copyrighted materials has been thought necessary to fulfill copyright's very purposes, '[t]o promote the Progress of Science and useful Arts.'"[92] Keeping with the Court's belief that fair use is classic Americana, the doctrine originated

89. In some cases, copyright law even promotes the creation of such works. *See, e.g.*, Campbell v. Acuff-Rose Music, Inc., 510 U.S. 569 (1994) (finding parody rap discussing "big hairy," "need to shave that stuff," "bald headed," and "two timin'" women to be fair use); *cf.* Kimberlé W. Crenshaw, *Beyond Racism and Misogyny: Feminism and 2 Live Crew, in* WORDS THAT WOUND: CRITICAL RACE THEORY, ASSAULTIVE SPEECH, AND THE FIRST AMENDMENT (Mari J. Matsuda, Charles R. Lawrence, Richard Delgado & Kimberlé W. Crenshaw eds., 2019) (discussing the anti-racist sentiment in the same parody); Cariou v. Prince, 14 F.3d 694 (2d Cir. 2013) (finding appropriation of Rastafarian portraits to be fair use). However, requiring consent for every secondary use can stifle feminist critique. *See, e.g.*, Mattel v. Walking Mountain Prods., 353 F.3d 792 (9th Cir. 2003) (observing that Mattel "would be less likely to grant a license to an artist that intends to create art that criticizes and reflects negatively on Barbie's image," which could be described as feminist art).

90. Carys Craig, *Reconstructing the Author-Self: Some Feminist Lessons for Copyright Law*, 15 J. GENDER, SOC. POL'Y & L. 207, 236–37 (2007) (arguing that feminist theory can recast copyright law to create an "author-subject"). Creatively using copyright law to promote feminist goals is a longtime focus of my scholarship. *See, e.g.*, Amanda Levendowski, *Using Copyright to Combat Revenge Porn*, 3 N.Y.U. J. INTELL. PROP. & ENT. L. 422 (2014) (arguing that copyright can provide targets of nonconsensual intimate imagery with useful remedies); Amanda Levendowski, *How Copyright Law Can Fix Artificial Intelligence's Implicit Bias Problem*, 93 WASH. L. REV. 579 (2018) (asserting that copyright can create fairer artificial intelligence for women, queer people, people of color, and other marginalized people); Amanda Levendowski, *Resisting Face Surveillance with Copyright Law*, 100 N.C. L. REV. 1015 (2022) (proposing that copyright can prevent many forms of face surveillance predicated on profile pictures).

91. Harper & Row v. Nation Enters., 471 U.S. 539, 549 (1985).

92. Campbell v. Acuff-Rose Music, 510 U.S. 569, 575 (1994) (quoting U.S. CONST. Art. 1, § 8, cl. 8).

with litigation over publication of George Washington's papers.[93] Fair use was later codified by the Copyright Act of 1976[94] as a means of identifying permissionless uses that are "not an infringement of copyright."[95] Under fair use, certain uses are privileged[96] and whether a use is fair comes down to how a court assesses four factors, including:

> (1) The purpose and character of the use, including whether such use is of a commercial nature or for nonprofit educational purposes;
>
> (2) The nature of the copyrighted work;
>
> (3) The amount and substantiality of the portion used in relation to the work as a whole; and
>
> (4) The effect of the use on the potential market for or value of the copyrighted work.[97]

On appeal, in *Perfect 10 v. Amazon*, the Ninth Circuit examined Google's use under the four factors of fair use and Judge Ikuta's analysis of the first factor powerfully influenced subsequent digital fair uses.[98] Under the first factor, the court inquired into whether Google use was "transformative," meaning whether its image search engine did not "merely supersede the objects of the original creation" but "add[ed] something new, with a further purpose or different character, altering the first with new expression, meaning, or

93. *See generally* Folsom v. Marsh, 9 F. Cas. 342 (C.C.D. Mass. 1841) (No. 4,901) (developing a multi-factor test for fair use).

94. Former Register of Copyrights Barbara Ringer played an important role in the codification of fair use. To learn more about Ringer, see Amanda Levendowski, *The Lost and Found Legacy of Barbara Ringer*, ATLANTIC (July 11, 2014), https://www.theatlantic.com/technology/archive/2014/07/the-lost-and-found-legacy-of-a-copyright-hero/373948; Advancing Inclusion in Copyright and Register Barbara Ringer's Legacy, U.S. COPYRIGHT OFF. (Nov. 19, 2020), https://copyright.gov/events/barbara-ringer/.

95. 17 U.S.C. § 107. While fair use is often framed as an affirmative defense—the district court in Perfect 10 treated it as such—the statutory language suggests it's more like a wholesale exemption rather than an exception. *See generally* Lydia Pallas Loren, *Fair Use: An Affirmative Defense?*, 90 WASH. L. REV. 685 (2015) (arguing that fair use should be understood as a defense, but not an affirmative one).

96. Those uses include "criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research . . . ." 17 U.S.C. § 107.

97. *§ Id.*

98. 508 F.3d 1146 (9th Cir. 2007). It is worth noting that, under the second factor assessing the creativity of a work, Google argued that nude photographs were less creative than other artistic works—a proposition the district court rejected. Perfect 10 v. Google, 416 F. Supp. 2d 828, 849–50 (C.D. Cal. 2006). It did, however, suggest that viewers of nude photographs were less discerning than others. *Id.* at 847.

message."[99] Judge Ikuta explained that search engines transform images from works into "a pointer directing a user to a source of information."[100] Judge Ikuta also noted that using the entire photographs did "not diminish the transformative nature of Google's use."[101] Judge Ikuta concluded that "the significantly transformative nature of Google's search engine, particularly in light of its public benefit, outweighs Google's superseding and commercial uses of the thumbnails . . . ."[102]

Judge Ikuta's decision paved the way for transformative technological uses that were not only legally fair, but more socially fair as well.[103] Nearly a decade later, the Second Circuit invoked her decision to support its finding that the HathiTrust Digital Library, a mass digitization project to provide accessible books to disabled people, was fair use.[104] That same court cited Judge Ikuta's reasoning to conclude that Google Books, the company's massive searchable book digitization project, was transformative despite its commerciality.[105] That decision enabled rich text and data mining research into Google Books volumes.[106] And engineers of AI systems implicitly rely on the decision to curate more equitable datasets—ones without the well-documented discriminatory effects of earlier systems.[107]

The legacy of *Perfect 10* is not all positive. The right to hoover up other people's photographs indiscriminately enabled Google Search results that

99. *Id.* at 1164 (quoting *Campbell*, 510 U.S. at 579).

100. *Id.*

101. *Id.*

102. *Perfect 10 v. Amazon*, 508 F.3d at 1166. The finding that commerciality was not dispositive marked a departure from the Supreme Court's prior stance. Sony Corp. Am. v. Universal City Studios, Inc., 464 U.S. 417, 451 (1984) ("[E]very commercial use of copyrighted material is presumptively an unfair exploitation of the monopoly privilege that belongs to the owner of the copyright.").

103. Not all fair uses promote fairness. *See* Amanda Levendowski, *Feminist Use*, *in* FEMINIST CYBERLAW (Meg Leta Jones & Amanda Levendowski eds., forthcoming 2024) (highlighting misogynistic, racist, and invasive colorable fair uses).

104. Authors Guild v. HathiTrust, 755 F.3d 87, 95 (2d Cir. 2014).

105. Authors Guild v. Google, 804 F.3d 202, 217 (2d Cir. 2015).

106. Matthew Sag has written and advocated about the promise of text and data mining, and attendant copyright issues, for the better part of a decade. *See* Matthew Sag, *Copyright and Copy-Reliant Technology*, 103 NW. U. L. REV. 1607, 1682 (2009); Matthew Sag, *Orphan Works as Grist for the Data Mill*, 27 BERKELEY TECH. L.J. 1503 (2012); Brief of Digital Humanities and Law Scholars as Amici Curiae In Support of Defendant-Appellees and Affirmance, Authors Guild v. Google (2d Cir. 2014); Matthew Sag, *The New Legal Landscape for Text Mining and Machine Learning*, 66 J. COPYRIGHT SOC'Y USA 291 (2019).

107. *See generally* Amanda Levendowski, *How Copyright Law Can Fix Artificial Intelligence's Implicit Bias Problem*, 93 WASH. L. REV. 579 (2018) (arguing that most uses of copyrighted works to train AI systems are fair use). *But see* Levendowski, *Resisting Face Surveillance*, *supra* note 90 (noting a key exception in the use of profile pictures to train face surveillance).

traffic in oppressive imagery, including misogynoir, by suggesting pornographic results for searches of "Black girls" but not other comparable searches.[108] Judge Ikuta's rationale positioning search engines as fair use has been appropriated by face surveillance company Clearview AI, which describes itself as a "search engine . . . providing for highly accurate facial recognition," to defend its private database of billions of scraped photographs used by law enforcement.[109] And a similar fair use analysis can be invoked to argue that content used to train "deepfakes," false video and audio generated by AI systems overwhelmingly used to create nonconsensual intimate imagery, are likewise fair use.[110] There is also an important issue missing from Judge Ikuta's decision entirely: what about the nude models whose images were made searchable online?

Google's appropriation of photographs of those models made their images freely, easily available in a way they weren't before. Previously, those Perfect 10 photographs were limited to newsstands ($7.99 an issue) and web subscriptions ($25.50 per month).[111] The photographs' existence were effectively obfuscated by paywalls that limited their accessibility. Google was not legally obligated to seek, or even consider, the models' consent—it certainly was not given. Yet the *Perfect 10* decision glosses over Google's violation of the models' agency.

The obvious reason is that copyright law is uninterested in photographic subjects, who have no copyright interest in works featuring their likeness.[112] Recognizing authors as photographers, rather than subjects, originated with the decision establishing the copyrightability of photography itself. In *Burrow-Giles Lithographic v. Sarony*,[113] photographer Napoleon Sarony snapped a shot of Oscar Wilde that was consentlessly reproduced by Burrow-Giles

108. "Misogynoir" was coined by queer Black feminist scholar Moya Bailey to describe "the unique ways in which Black women are pathologized in popular culture." *See* Moya Bailey, *More on the Origin of Misogynoir*, TUMBLR (Apr. 27, 2014), https://moyazb.tumblr.com/post/84048113369/more-on-the-origin-of-misogynoir. 'SAFIYA UMOJA NOBLE, ALGORITHMS OF OPPRESSION: HOW SEARCH ENGINES REINFORCE RACISM (2018) (Dr. Safiya Noble raising early concerns over Google Image Search's misogynoir results.)

109. *Principles*, CLEARVIEW AI, https://perma.cc/GM3V-YJQA. The company is unlikely to be a search engine. Levendowski, *Resisting Face Surveillance*, *supra* note 90.

110. *The State of Deepfakes: Landscape, Threats, and Impact*, DEEPTRACE (Sept. 2019), https://enough.org/objects/Deeptrace-the-State-of-Deepfakes-2019.pdf (identifying 96% of deepfakes as pornographic).

111. Perfect 10 v. Google, 416 F. Supp. 2d 828, 831–32 (C.D. Cal. 2006).

112. Selfies, which collapse author and subject, are the notable exception. *Supra* Section II.B. *But see* Garcia v. Google, 786 F.3d 733 (9th Cir. 2015) (unsuccessfully invoking copyright law to censor an actor's appearance in a controversial film). Alternatively, other areas of law—such as right of publicity—are very interested in the nonconsensual use of one's likeness.

113. Burrow-Giles Lithographic Co. v. Sarony, 111 U.S. 53, 54–55 (1884).

Lithographic. [114] Wilde—notorious, debonair, and controversial—undoubtedly made the shot noteworthy. But the Supreme Court took painstaking lengths to celebrate Sarony's contributions, including:

> posing the said Oscar Wilde in front of the camera, selecting and arranging the costume, draperies, and other various accessories in said photograph, arranging the subject so as to present graceful outlines, arranging and disposing the light and shade, suggesting and evoking the desired expression, and from such disposition, arrangement, or representation, made entirely by plaintiff, he produced the picture in suit.[115]

According to the Court, Sarony, as the photographer, owned the copyright.[116] Wilde, as the subject, was simply there.

This tension has become pronounced among open knowledge projects. Authors, who may or may not have permission from their subjects, are entitled to share their works for remix, reuse, and reappropriation. Organizations like Creative Commons (CC) make that easy. Dedicated to building a "vibrant, collaborative global commons,"[117] CC offers a suite of licenses that modify the all-rights-reserved approach to copyright, which allows authors to make their works more accessible to all. But that includes organizations dabbling in dubious technology.

In 2020, IBM was outed for automatically copying, or "scraping," CC-licensed photographs to fuel its face recognition technology.[118] Many authors were alarmed. "None of the people I photographed had any idea their images were being used in this way," explained Greg Peverill-Conti, who unknowingly

---

114. *Id.*

115. *Id.* at 60.

116. *Id.* For a deeper dive into the effects of this conclusion, see Christine Haight Farley, *The Lingering Effects of Copyright's Response to the Invention of Photography*, 65 U. PITT. L. REV. 385, 385–88 (2004); cf. Eva E. Subotnick, *Originality Proxies: Toward a Theory of Copyright and Creativity*, 76 BROOK. L. REV. 1487, 1499–504 (2011).

117. *About The Licenses*, CREATIVE COMMONS (2022), https://creativecommons.org/licenses/.

118. Olivia Solon, *Facial Recognition's 'Dirty Little Secret': Millions of Online Photos Scraped Without Consent*, NBC NEWS (Mar. 12, 2020), https://www.nbcnews.com/tech/internet/facial-recognition-s-dirty-little-secret-millions-online-photos-scraped-n981921 [hereinafter Solon, *Dirty Little Secret*]. Investigatory tools can determine if one's photographs were appropriated for face surveillance. Cade Metz & Kashmir Hill, *Here's a Way to Learn if Facial Recognition Systems Used Your Photos*, N.Y. TIMES (Feb. 1, 2021), https://www.nytimes.com/2021/01/31/technology/facial-recognition-photo-tool.html (describing Exposing.AI). In 2022, I supervised student attorneys in the iPIP Clinic advising an open knowledge client on addressing the appropriation of copyrighted works for face surveillance. All comments are based on publicly available information.

contributed more than 700 photographs to the IBM dataset.[119] The company reassured authors (and the public) that its product was not intended for law enforcement, but IBM has a long history of secretly selling oppressive surveillance tools to governments.[120] Initially, IBM rode the wave of criticism. But in the wake of George Floyd's murder by police officer Derek Chauvin, amid calls from Black Lives Matter and feminist activists to defund the police and abolish surveillance technology, IBM announced that it would sunset its face recognition program.[121] Yet IBM was arguably legally entitled to use those photographs—through CC licensing, consent had already been granted.[122]

To be clear, copyright law does not need to be changed to protect subjects. There are good reasons for showing or sharing works, even works featuring nudity, without subjects' specific consent. Critics did so to expose the torture occurring at Abu Ghraib.[123] Art enthusiasts might hang prints by Robert Mapplethorpe in their homes.[124] Whistleblowers may leak harassing photographs from powerful men to the press.[125] But copyright law barely defines definitively what constitutes fair use—it is even less equipped to determine what is "fair" in the sense of "equitable."[126] Other doctrines, such

119. Solon, *Dirty Little Secret*, *supra* note 118. An IBM spokesperson stated that the images could be removed from the dataset on request. *Id.*

120. Including literal Nazis. *See, e.g.*, EDWIN BLACK, IBM AND THE HOLOCAUST: THE STRATEGIC ALLIANCE BETWEEN NAZI GERMANY AND AMERICA'S MOST POWERFUL CORPORATION (2001). More recently, IBM created CCTV technology searchable by skin tone, as well as an "intelligent video analytics" product that could tag people on body-worn camera footage by ethnicity. *See* Solon, *Dirty Little Secret*, *supra* note 118; Levendowski, *Resisting Face Surveillance*, *supra* note 90.

121. Arvind Krishna, *IBM CEO's Letter to Congress on Racial Justice Reform*, IBM: THINKPOLICY BLOG (June 8, 2020), https://www.ibm.com/blogs/policy/facial-recognition-sunset-racial-justice-reforms/.

122. Levendowski, *Resisting Face Surveillance*, *supra* note 90, at 1045.

123. *See* DAVID LEVI STRAUSS & CHARLES STEIN, ABU GHRAIB: THE POLITICS OF TORTURE (2004).

124. For examples of Mapplethorpe's art, see Robert MAPPLETHORPE, PORTRAIT OF JACK STAHL (1976).

125. This is a variation on the Sydney Leathers scandal. Abraham Riesman, *The Secret Struggle of the Woman Who Took Down Weiner*, CUT (May 20, 2016), https://www.thecut.com/2016/05/pain-triumph-weiner-sexter-sydney-leathers.html.

126. As Lawrence Lessig quipped, "[F]air use in America simply means the right to hire a lawyer to defend your right to create." LAWRENCE LESSIG, FREE CULTURE Ch. 16 (2004), http://www.authorama.com/free-culture-16.html. And several iconic fair uses reflect misogyny, racism, and colonialism. *See, e.g.*, Campbell v. Acuff-Rose, 510 U.S. 569 (1994) (releasing parody calling women "big hairy," "need to shave that stuff," "bald headed," and "two-timin'"); *see also* Michelle Ruiz, *Safiya Noble Knew the Algorithm Was Oppressive*, VOGUE (Oct. 21, 2021), https://www.vogue.com/article/safiya-noble; Cariou v. Prince, 714 F.3d 694, 699 (2d Cir. 2013) (appropriating photographs of Black Rastafarians). *But see* Kimberlé W. Crenshaw, *Beyond Racism and Misogyny: Feminism and 2 Live Crew, in* WORDS THAT WOUND:

as the right of publicity, may be better tailored to solving the schism between photographers' or fair users' wants and subjects' consent.[127]

B. TAKING DOWN NONCONSENSUAL INTIMATE IMAGERY WITH THE DIGITAL MILLENNIUM COPYRIGHT ACT

Sometimes, a photographic subject's lack of consent to use a work coincides with copyright infringement. In 2013, David K. Elam II responded to the end of his relationship with Jane Doe by threatening to ruin her life.[128] He delivered. Elam got to work about spreading Doe's intimate images, shared in the context of a relationship, across the internet.[129] He uploaded her images to multiple pornographic websites and directly shared links with Doe's classmate and mother.[130] Doe registered her selfies with the U.S. Copyright Office and sued for copyright infringement.[131] Elam had no defense.

Crucially, Elam's misappropriation was unlikely to be fair use. In a case over the republication of President Gerald Ford's biography recounting his pardon of Richard Nixon, the Supreme Court stated that authors' "right to control the first public appearance of [their] undisseminated expression will outweigh a claim of fair use" because "the scope of fair use is narrower with

---

CRITICAL RACE THEORY, ASSAULTIVE SPEECH, AND THE FIRST AMENDMENT (Mari J. Matsuda, Charles R. Lawrence, Richard Delgado & Kimberlé W. Crenshaw eds., 2019) (discussing anti-racist speech reflected in the song); Jessie Heyman, *SuicideGirls Respond to Richard Prince in the Best Way*, VOGUE (May 28, 2015), https://www.vogue.com/article/suicidegirls-richard-prince (appropriating alt-models' Instagram posts for gallery show); Perfect 10 v. Amazon.com, 508 F.3d 1146 (9th Cir. 2007) (appropriating nude models' images and later serving up misogynoir search results). For a discussion of what a model for feminist fair use, or "feminist use," looks like, see Amanda Levendowski, *Feminist Use*, *in* FEMINIST CYBERLAW (Meg Leta Jones & Amanda Levendowski eds., forthcoming 2024) (manuscript on file with author).

127. *See, e.g.*, N.Y. Civ. Code §§ 50–51. For a comprehensive discussion of right of publicity laws, see JENNIFER ROTHMAN, THE RIGHT OF PUBLICITY: PRIVACY REIMAGINED FOR A PUBLIC WORLD (2018); Jason Schultz, *The Right of Publicity–A New Framework for Regulating Facial Recognition* (manuscript on file with author).

128. Jane Doe v. David K. Elam II, First Amended Complaint, 2:14-cv-09788 (C.D. Cal. Feb. 12, 2015), at *2, https://www.courtlistener.com/docket/4152345/11/jane-doe-v-david-k-elam-ii/. Doe was represented by K&L Gates, which has a boutique pro bono practice litigating on behalf of nonconsensual intimate imagery victims. Christine Hauser, *$6.4 Million Judgment in Revenge Porn Case is Among Largest Ever*, N.Y. TIMES (Apr. 11, 2018), https://www.nytimes.com/2018/04/11/us/revenge-porn-california.html/.

129. Jane Doe v. David K. Elam II, First Amended Complaint, 2:14-cv-09788 (C.D. Cal. Feb. 12, 2015), at *2, https://www.courtlistener.com/docket/4152345/11/jane-doe-v-david-k-elam-ii/.

130. *Id.* at *3. The posts often included Doe's personal information, such as her name and school, and Doe received "countless" messages and requests from strangers through her personal social media accounts.

131. *Id.* at *6.

respect to unpublished works."[132] In the largest judgment of its kind, the district court awarded Doe $450,000 in damages for Elam's infringement.[133] And while imperfect, there was also another tool in Doe's arsenal: the Digital Millennium Copyright Act (DMCA).[134]

Enacted in 1998, the DMCA responded to a rapidly growing internet by providing copyright owners with new tools to tackle web users' infringement.[135] However, its provisions go beyond the exclusive rights traditionally protected by copyright law—it's best understood as a paracopyright law.[136] Its provisions revolutionized responses to copyright infringement in two ways. First, it created a safe harbor protecting online service providers (OSPs) from copyright infringement liability so long as the OSPs satisfied certain statutory conditions.[137] Second, it created a new way for copyright owners to request removal of infringing content: notice and takedown.[138] By sending compliant notices of infringing content to OSPs,

132. Harper & Row Publishers, Inc. v. Nation Enterprises, 471 U.S. 539, 555, 564 (1985).

133. For context, it was a default judgment rather than a jury award. Christine Hauser, *$6.4 Million Judgment in Revenge Porn Case is Among Largest Ever*, N.Y. TIMES (Apr. 11, 2018), https://www.nytimes.com/2018/04/11/us/revenge-porn-california.html/.

134. Jane Doe v. David K. Elam II, First Amended Complaint, 2:14-cv-09788 (C.D. Cal. Feb. 12, 2015), at *5 (describing counsel's "diligent issuance of takedown letters" which were not immediately effective but appear to have had some effect between 2013 and 2015 when the lawsuit was file). I proposed using the DMCA to combat nonconsensual intimate imagery as a law student in the first scholarly paper to make the recommendation. Levendowski, *Using Copyright*, *supra* note 90, at 442–43. This piece has been put into practice. In 2021, I supervised student attorneys in Georgetown's iPIP Clinic developing a guide to using the DMCA to take down nonconsensual intimate imagery for domestic violence service providers. *Taking Down Online Nonconsensual Pornography: A Guide*, DV ADVOCATES (Dec. 2021) (manuscript on file with author).

135. This Part focuses on § 512 of the DMCA; its companion, § 1201, creates penalties for the circumvention of copyright protection systems, often embodied as digital rights management (DRM) technology. 17 U.S.C. § 1201. Every three years, civil society, libraries, archives, educational institutions, hobbyists, and others engage in the strange and chaotic process of submitting requests for exemptions from § 1201 to the Librarian of Congress, which are then attacked by copyright owners. In 2020, I supervised student attorneys Michael Rubayo and Natasha Tverdynin in the iPIP Clinic filing an exemption comment, which as partially granted, on behalf of the Electronic Frontier Foundation. *Comments of the Electronic Frontier Foundation on Proposed Class 12: Computer Programs—Repair*, ELEC. FRONTIER FOUND. (Dec. 14, 2020), https://www.eff.org/document/dmca-1201-2021-comments-electronic-frontier-foundation-proposed-class-12-computer-programs.

136. H.R. REP. NO. 105-551, pt. 2, at 24 (1998) (acknowledging that the DMCA "represent[s] an unprecedented departure into what might be called paracopyright"); *see also* Neil Weinstock Netanel, *Locating Copyright Within the First Amendment Skein*, 54 STAN. L. REV. 24 (2001) (discussing the DMCA as paracopyright law).

137. 17 U.S.C. §§ 512(a)–(d).

138. 17 U.S.C. § 512(c)(3).

copyright owners could put pressure on OSPs to respond or risk losing their safe harbor.[139] The DMCA falls within the first category: cyberlaws that can be appropriated for feminist goals, such as combating nonconsensual intimate imagery. But Congress certainly did not anticipate that the DMCA would become a powerful civil tool for removing such harassing and harmful content.

Victims of nonconsensual intimate imagery distribution have an interest in removing their images from the internet quickly and quietly. Consequences can be dire, from mental health diagnoses of anxiety, depression, or post-traumatic stress disorder (PTSD),[140] to loss of employment,[141] to self-harm.[142] Drawn-out litigation can further burden victims, who are disproportionately women and queer people.[143] Luckily, most nonconsensual intimate imagery victims can use the DMCA to remove their images.

A survey by anti-nonconsensual intimate imagery advocacy organization Cyber Civil Rights Initiative established that 80% of victims reported that their nonconsensual intimate images were selfies, meaning that victims are authors, subjects, and copyright owners all at once.[144] As a result, most victims can use the DMCA notice process to take down their images. Sending a DMCA notice is free, unlike registering a copyright or initiating a lawsuit.[145] Sending a DMCA notice does not require additional disclosure of the underlying image, unlike

139. *Cf.* 47 U.S.C. § 230(e)(2) (noting that the Communications Decency Act does not "limit or expand any law pertaining to intellectual property"). For more on CDA § 230, see *infra* Section III.B.

140. Samantha Bates, *Revenge Porn and Mental Health: A Qualitative Analysis of the Mental Health Effects of Revenge Porn on Female Survivors*, 12 FEMINIST CRIMINOLOGY 22 (2016).

141. Annie Seifullah, *Revenge Porn Took My Career. The Law Couldn't Get It Back*, JEZEBEL (July 18, 2018), https://jezebel.com/revenge-porn-took-my-career-the-law-couldnt-get-it-bac-1827572768.

142. Tyler Clementi and Amanda Todd reflect two tragic examples. Michelle Dean, *The Story of Amanda Todd*, NEW YORKER (Oct. 18, 2012), https://www.newyorker.com/culture/culture-desk/the-story-of-amanda-todd.

143. Amanda Lenhart, Myeshia Price-Feeney & Michele Ybarra, *Nonconsensual Image Sharing: One in 25 Americans Has Been a Victim of "Revenge Porn"*, DATA & SOC'Y, 16 (Dec. 13, 2016), https://datasociety.net/library/nonconsensual-image-sharing/; Ari Ezra Waldman, *Law, Privacy, and Online Dating: "Revenge Porn" in Gay Online Communities*, 44 L. & SOC. INQUIRY 987, 987–88 (2019).

144. *Proposed CA Bill Would Fail to Protect Up to 80% of Revenge Porn Victims*, CYBER CIVIL RIGHTS INITIATIVE (Sept. 10, 2013), https://www.cybercivilrights.org/wp-content/uploads/2015/06/SB255_Press-Release.pdf (citing Cyber Civil Rights Initiative survey finding that 80% of nonconsensual intimate imagery images are selfies).

145. 17 U.S.C. § 512. It also imposes no inherent costs on recipients of DMCA takedown requests, unlike most litigation complaints.

registration or litigation.[146] Sending a DMCA notice doesn't even require a lawyer, as any copyright owner or their agent can submit one.[147] And, most importantly, it works.

Take Celebgate. In 2014, dozens of women celebrities' nude images were hacked and leaked to reddit.[148] The moderators of subreddits where the images appeared declined to respond immediately, and so did the site itself. But one thing caught reddit's attention: DMCA takedown notices. As then-CEO Yishan Wong explained in his blog post about the incident, "[i]n accordance with our legal obligations, we expeditiously removed content hosted on our servers as soon as we received DMCA requests from the lawful owners of that content, and in cases where the images were not hosted on our servers, we promptly directed them to the hosts of those services."[149]

While the DMCA took down the original photographs, irreversible harm had already been done.[150] Jennifer Lawrence, whose images were included in the hack, put it bluntly by explaining "It's my body, and it should be my choice, and the fact that it is not my choice is absolutely disgusting. I can't believe we even live in that kind of world."[151]

Despite its effectiveness, some scholars, including Rebecca Tushnet and Jeannie Fromer, are skeptical that copyright should be invoked to tackle

146. 17 U.S.C. §§ 512I(3)(A)(i)-(vi). A DMCA notice may still create a public record of the request. The Lumen database, for example, archives records of DMCA notices. *About Us*, LUMEN (2022) https://www.lumendatabase.org/pages/about.

147. 17 U.S.C. § 512(c)(3)(A)(vi).

148. Mike Isaac, *Nude Photos of Jennifer Lawrence Are Latest Front in Online Privacy Debate,* N.Y. TIMES (Sept. 2, 2014), https://www.nytimes.com/2014/09/03/technology/trove-of-nude-photos-sparks-debate-over-online-behavior.html. To put reddit into context, see Keegan Hankes, *How Reddit Became a Worse Black Hole of Violent Racism than Stormfront*, GAWKER (Mar. 10, 2015), https://www.gawker.com/how-reddit-became-a-worse-black-hole-of-violent-racism-1690505395. The article's title says it all. While copyright carried the day, hacking is criminalized under the Computer Fraud and Abuse Act, which has been used to prosecute traffickers of nonconsensual intimate imagery. *See infra* Section IV.C.

149. Yishan Wong, *Reddit CEO: Every Man is Responsible for His Own Soul*, REDDIT (Sept. 7, 2014), https://redef.com/author/540c232b66c1b42455d31ce1. Please take note of the truly awful title of the post—yikes.

150. Some of the images remain findable today. Google only began removing the hacked images from its subsidiaries after being threatened with a $100 million lawsuit; other smaller sites responded within hours to DMCA takedown requests. Alex Hern & Dominic Rushe, *Google Threatened with $100m Lawsuit over Nude Celebrity Photos*, GUARDIAN (Oct. 2, 2014), https://www.theguardian.com/technology/2014/oct/02/google-lawsuit-nude-celebrity-photos.

151. VANITY FAIR, *Cover Exclusive: Jennifer Lawrence Calls Photo Hacking a "Sex Crime,"* (Oct. 7, 2014), https://www.vanityfair.com/hollywood/2014/10/jennifer-lawrence-cover/.

nonconsensual intimate imagery.[152] Their concerns are not misplaced. Invoking the DMCA can have serious costs. As Cathay Smith has observed, the DMCA's extrajudicial process encourages its weaponization by rightsholders.[153] Jennifer Urban, Joe Karaganis, and Brianna Schofield illustrated how that weaponization threatens the free speech of fans, activists, and critics alike.[154] And the practical success of DMCA takedowns also does nothing to change the dangerous societal attitudes that prize intellectual property rights over people's privacy and autonomy.[155] Yet despite its flaws, the DMCA can be effective when little else is.[156]

C. CRIMINALIZING NONCONSENSUAL INTIMATE IMAGERY AND PROTECTING FREE SPEECH

Nonconsensual intimate imagery distribution is not only subject to civil remedies. The nonconsensual exposure of Rutgers freshman Tyler Clementi's most private moments tested one of the earliest criminal nonconsensual

152. Rebecca Tushnet, *How Many Wrongs Make a Copyright?*, 98 MINN. L. REV. 2346, 2348 (2014) (reviewing Derek E. Bambauer, *Exposed*, 98. MINN. L. REV. 2025 (2014)) (rejecting the use of copyright to combat nonconsensual intimate imagery); Jeanne C. Fromer, *Should the Law Care Why Intellectual Property Rights Have Been Asserted?*, 53 HOUS. L. REV. 549, 580 (2015) (discussing my recommendation to use the DMCA to take down nonconsensual intimate imagery and describing privacy as an "ill-fitting motivations" for asserting copyright). Some scholars go a step further and reject the use of copyright to protect against privacy harms at all. *See, e.g.*, Hon. Pierre N. Leval, *Toward a Fair Use Standard*, 103 HARV. L. REV. 1105, 1129 (1990) ("The occasional attempt to read protection of privacy into the copyright is also mistaken."); Eric Goldman & Jessica Silbey, *Copyright's Memory Hole*, 4 B.Y.U. L. REV. 929, 996 (2019) ("Despite the legitimate and sometimes profound harms experienced by some privacy victims, copyright law should not be manipulated to fix privacy law's problems.").

153. Cathay Smith, *Weaponizing Copyright*, 35 HARV. J.L. & TECH. 193, 231–33 (2022).

154. Jennifer M. Urban, Joe Karaganis & Brianna Schofield, *Notice and Takedown in Everyday Practice*, UC Berkeley Pub. L. Research Paper No. 2755628 (2016). This threat is not limited to the DMCA but extends to copyright itself. Cathay Y.N. Smith, *Copyright Silencing*, 106 CORNELL L. REV. 71 (2021). For specific examples of DMCA weaponization, see Jon Brodkin, *Twitter Suspends Sports Media Accounts After NFL Says GIFs Violate Copyright*, ARS TECHNICA (Oct. 13, 2015), https:// arstechnica.com/tech-policy/2015/10/nfls-copyright-complaints-lead-to-twitter-crackdown-on-sports-gif-sharing/ (deployment against sports fansite Deadspin); Alejandro Menjivar, Natalia Krapiva & Rodrigo Rodríguez, *Warning: Repressive Regimes Are Using DMCA Takedown Demands to Censor Activists*, ACCESS NOW (Oct. 22, 2020), https://www.accessnow.org/dmca-takedown-demands-censor-activists/ (weaponization against activist content by Nicaragua, Tanzania, and Ecuador); Eva Galperin, *Massive Takedown of Anti-Scientology Videos on YouTube*, ELEC. FRONTIER FOUND. (Sept. 5, 2008), https://www.eff.org/deeplinks/2008/09/massive-takedown-anti-scientology-videos-youtube.

155. Sarah Jeong, *Après Moi, Le Déluge: What Went Wrong on Reddit*, FORBES (July 15, 2015), https://www.forbes.com/sites/sarahjeong/2015/07/15/apres-moi-le-deluge-what-went-wrong-on-reddit/.

156. Levendowski, *Using Copyright*, *supra* note 90, at 446.

intimate imagery laws. Unbeknownst to Clementi, his roommate and another student surreptitiously filmed him with another man, shielded only by a blanket, and streamed it live over the internet.[157] Clementi's roommate tweeted about the invasion, saying "Roommate asked for the room till midnight. I went into molly's [sic] room and turned on my webcam. I saw him making out with a dude. Yay."[158] Three days later, Clementi died by suicide.[159]

The filming duo were charged with invasion of privacy under New Jersey's nonconsensual intimate imagery statute.[160] Enacted in 2003, the law criminalizes, in part, when an individual:

> knowing that he is not licensed or privileged to do so, he photographs, films, videotapes, records, or otherwise reproduces in any manner, the image of another person whose intimate parts are exposed or who is engaged in an act of sexual penetration or sexual contact, without that person's consent and under circumstances in which a reasonable person would not expect to be observed.[161]

Violating the law is a third-degree felony.[162] In nearly all other states at that time, however, there were no targeted criminal nonconsensual intimate imagery laws.[163] Criminal nonconsensual intimate imagery laws fall into the third category of cyberlaws: feminist cyberlaws that can subvert feminist goals. While criminal nonconsensual intimate imagery laws can be powerful ways of retaliating against consentless acts that threaten victims' safety, these laws can also be drafted so poorly—and unconstitutionally—that they can be weaponized against marginalized people. There also remains an open question

157. Lisa W. Foderaro, *Private Moment Made Public, Then A Fatal Jump*, N.Y. TIMES (Sept. 29, 2010, https:// www.nytimes.com/2010/09/30/nyregion/30suicide.html; Ian Parker, *The Story of a Suicide*, NEW YORKER (Jan. 29, 2012), https:// www.newyorker.com/magazine/2012/02/06/the-story-of-a-suicide.

158. Nate Schweber & Lisa W. Foderaro, *Roommate in Tyler Clementi Case Pleads Guilty to Attempted Invasion of Privacy*, N.Y. TIMES (Oct. 27, 2016), https://www.nytimes.com/2016/10/28/nyregion/dharun-ravi-tyler-clementi-case-guilty-plea.html.

159. Foderaro, *supra* note 157. People considering suicide can call the National Suicide Prevention Lifeline at 1-800-273-TALK (8255).

160. *Two Rutgers Students Charged With Invasion of Privacy*, MIDDLESEX CNTY. PROSECUTOR'S OFF. (Sept. 28, 2010), https://web.archive.org/web/20120310150735/http://www.co.middlesex.nj.us/prosecutor/PressRelease/Two%20Rutgers%20students%20charged%20with%20invasion%20of%20privacy.htm.

161. N.J.S.A. § 2C:14-9(b).

162. *Id.*

163. Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345, 371 (2014).

among feminists about whether criminal laws can ever be used to promote feminist goals.[164]

At the time, there were other criminal laws applicable to nonconsensual intimate imagery distribution. Some instances of copyright infringement are crimes.[165] Other laws, such as the Computer Fraud and Abuse Act, criminalize the kind of hacking that targeted celebrities like Jennifer Lawrence.[166] Manipulating images to create false disparaging ones amounts to criminal defamation in some states.[167] One federal criminal law even requires recordkeeping to verify the identities and ages of performers in all visual depictions of sexually explicit conduct.[168] Several of these laws or their civil analogs have been successfully used to combat nonconsensual intimate imagery but, of these, the New Jersey criminal law was most relevant to Clementi.

However, the mere existence of these laws did not make them easy for victims to invoke, even when they were applicable. Serious structural barriers remained. As victim and activist Holly Jacobs explained, "I don't just see the gaping holes in our legal system; I experience them firsthand."[169] Law enforcement and prosecutors often blamed victims for taking the images and avoided taking on cases that were perceived as factually and technologically

164. *See, e.g.*, Elizabeth Bernstein, *The Sexual Politics of the 'New Abolitionism,'* 18 DIFFERENCES 3 (2007), https://glc.yale.edu/sites/default/files/pdf/sexual_politics_of_new_abolitionism_.pdf (coining the term "carceral feminism").

165. Levendowski, *Using Copyright*, *supra* note 90, at 445; *see also* 17 U.S.C. § 506(a). Civil copyright laws have been used effectively. Christine Hauser, *$6.4 Million Judgment in Revenge Porn Case is Among Largest Ever*, N.Y. TIMES (Apr. 11, 2018), https://www.nytimes.com/2018/04/11/us/revenge-porn-california.html/ (detailing $450,000 default judgment for copyright infringement in nonconsensual intimate imagery lawsuit).

166. 18 U.S.C. § 1030(a)(2)(C); *Computer Crime Statutes*, NAT'L CONF. STATE LEG. (May 4, 2022), https://www.ncsl.org/research/telecommunications-and-information-technology/computer-hacking-and-unauthorized-access-laws.aspx (detailing state versions of the CFAA). The CFAA has also been used effectively. *See, e.g.*, Department of Justice, *"Operator of 'Revenge Porn' Website Sentenced to 2 ½ Years in Federal Prison in Email Hacking Scheme to Obtain Nude Photos*" (Dec. 2, 2015), https://www.justice.gov/usao-cdca/pr/operator-revenge-porn-website-sentenced-2-years-federal-prison-email-hacking-scheme. For more on Hunter Moore and the CFAA, see *infra* Section IV.C.

167. *Map of States with Criminal Laws Against Defamation*, ACLU (2022), https://www.aclu.org/issues/free-speech/map-states-criminal-laws-against-defamation.

168. *See* 18 U.S.C. §§ 2257–2257A. The latter provision has been challenged as unconstitutional. *See* Ann Bartow, *Why Hollywood Does Not Require "Saving" From the Recordkeeping Requirements Imposed by 18 U.S.C. Section 2257*, 118 YALE L.J.F. (2008).

169. Holly Jacobs, *Victims of Revenge Porn Deserve Real Protection*, GUARDIAN (Oct. 8, 2013), https://www.theguardian.com/commentisfree/2013/oct/08/victims-revenge-porn-deserve-protection. The case against Jacobs' ex-boyfriend, who distributed her images, was dismissed. *Id.* She founded the advocacy organization Cyber Civil Rights Initiative. *Id.*

tricky.[170] Once victims found an advocate, lawyers and litigation remained expensive. And retelling the same story over and over, including publicly before a judge and jury, and possibly before the person who released the images, could mount a traumatic toll that some victims were not willing to take.

In 2014, scholars Danielle Citron and Dr. Mary Anne Franks believed existing laws could not be an effective deterrent—why else would rates of victimization be rising?[171] They opted to resist nonconsensual intimate imagery another way: by advocating for its criminalization.

In *Criminalizing Revenge Porn*, Citron and Franks detailed the harms of nonconsensual intimate imagery to support their call for criminalization. In a study of 1,244 people, over 50% of victims reported that their images were accompanied by their full names and social network profiles; over 20% included their email address and telephone number.[172] Preventing nonconsensual intimate imagery, they explained, was more complicated than victims logging off. These kinds of accompanying disclosures meant that online aggression could translate to offline attacks, including stalking, harassment, and rape.[173] Citron and Franks positioned nonconsensual intimate imagery on the newest attack on women and girls' autonomy, not unlike domestic violence, sexual assault, and sexual harassment.[174] Like those issues, the road to preventing nonconsensual intimate imagery would be "long and difficult."[175] But perhaps a targeted criminal law could help.

Citron and Franks did not initially provide model legislation, instead opting to outline key features of nonconsensual intimate imagery laws.[176] The pair was mindful that a poorly drafted nonconsensual intimate imagery law could run afoul of the First Amendment and be struck down as unconstitutional.[177] That concern must be contextualized by a much earlier example of scholars

170. *Id.*

171. Citron & Franks, *supra* note 163, at 349. Franks produced model legislation in subsequent articles. *See, e.g.*, Mary Anne Franks, *"Revenge Porn" Reform: A View from the Front Lines*, 69 FLA. L. REV. 1251, 1292, 1331 (2017); Mary Anne Franks, *Drafting an Effective "Revenge Porn" Law: A Guide for Legislators*, CYBER C.R. INITIATIVE (updated Oct. 2021), https://cybercivilrights.org/wp-content/uploads/2021/10/Guide-for-Legislators-10.21.pdf.

172. Citron & Franks, *supra* note 163, at 350–51.

173. *Id.*; *see also* Edecio Martinez, *Alleged 'Craigslist Rapist' Ty McDowell: Ex-Marine Tricked Me Into Raping Former Girlfriend*, CBS NEWS (Mar. 8, 2010), https://www.cbsnews.com/news/alleged-craigslist-rapist-ty-mcdowell-ex-marine-tricked-me-into-raping-former-girlfriend/.

174. Citron & Franks, *supra* note 163, at 347–48.

175. *Id.*

176. *Id.* at 387–90.

177. *Id.* at 386.

advocating a different kind of law targeting nudity, this kind consensual: banning pornography.

In 1983, the Indianapolis city council enacted an ordinance inspired by the scholarship, advocacy, and model legislation of radical feminist scholars Andrea Dworkin and Catharine MacKinnon, who argued that pornography "is a systemic practice of exploitation and subordination based on sex that differentially harms and disadvantages women."[178] Consistent with Dworkin and MacKinnon's work, the ordinance broadly defined pornography as

> the graphic sexually explicit subordination of women, whether in pictures or in words, that also includes one or more of the following:
>
> 1. Women are presented as sexual objects who enjoy pain or humiliation; or
>
> 2. Women are presented as sexual objects who experience sexual pleasure in being raped; or
>
> 3. Women are presented as sexual objects tied up or cut up or mutilated or bruised or physically hurt, or as dismembered or truncated or fragmented or severed into body parts; or
>
> 4. Women are presented as being penetrated by objects or animals; or
>
> 5. Women are presented in scenarios of degradation, injury, abasement, torture, shown as filthy or inferior, bleeding, bruised, or hurt in a context that makes these conditions sexual; or
>
> 6. Women are presented as sexual objects for domination, conquest, violation, exploitation, possession, or use, or through postures or positions of servility or submission or display.[179]

While the ordinance positioned itself as a feminist one, it only endorsed a radical flavor of feminism. Other feminists countered that MacKinnon and Dworkin's approach ignored the ordinance's paternalism, hostility to some feminist works, likely weaponization against feminists and lesbians, and effect on sex workers—many of whom are women and feminists—who might exercise their agency to choose consensual sex work.[180] It also happened to be unconstitutional.

178. ANDREA DWORKIN & CATHARINE A. MACKINNON, PORNOGRAPHY AND CIVIL RIGHTS: A NEW DAY FOR WOMEN'S EQUALITY 138 (1988).

179. *Id.* at 138–39.

180. Nadine Strossen, *Feminist Critique of 'the' Feminist Critique of Pornography*, *An Essay*, 79 VA. L. REV. 1099, 1140–71 (1993) (outlining ten ways that pornographic censorship could undermine the interests of women and feminists).

In *American Booksellers Association v. Hudnut*, booksellers challenged the statute as an unconstitutional restraint on free speech by invoking classic texts like Greek myths and James Joyce's Ulysses as potentially prohibited "pornography."[181] At the Seventh Circuit, Judge Easterbrook observed that the ordinance's definition of pornography was "considerably different" from the Supreme Court's definition of obscenity, one of the few categories of speech unprotected by the First Amendment.[182] The Supreme Court defined obscenity in *Miller v. California*, explaining that "a publication must, taken as a whole, appeal to the prurient interest, must contain patently offensive depictions or descriptions of specified sexual conduct, and on the whole have no serious literary, artistic, political, or scientific value." [183] Among its constitutional shortcomings, the ordinance did not contemplate that pornography could have any value, let alone "literary, artistic, political, or scientific value." Indianapolis and its amici were undeterred by the mismatch and positioned it as a powerful way to move the needle on societal attitudes toward women.[184] MacKinnon went a step further, asserting that "if a woman is subjected, why should it matter that the work has other value?"[185]

As Judge Easterbrook explained, it mattered because the First Amendment could not tolerate what amounted to "thought control." [186] While Judge Easterbrook accepted Dworkin and MacKinnon's position that all pornography created and maintained sex as a basis of discrimination—a contentious call—he nevertheless determined that pornography is protected speech.[187] He concluded that well-intentioned bans on broad swaths of speech must yield to the First Amendment.[188]

A sloppy criminal nonconsensual intimate imagery law ran the risk of becoming the next *Hudnut*. Sensitive to overbreadth issues, Citron and Franks recommended requiring proof that victims suffered harm.[189] Similarly, they endorsed laws that reflected the state of First Amendment doctrine by including clear public interest exemptions.[190] And they favored laws that put people on notice by providing clear, specific, and narrow definitions for

181. Am. Booksellers Ass'n v. Hudnut, 771 F.2d 323, 325 (7th Cir. 1985).

182. *Id.* at 324.

183. *Id.* at 324 (quoting Brockett v. Spokane Arcades, 472 U.S. 491 (1985)).

184. *Id.* at 325.

185. Catharine A. MacKinnon, *Pornography, Civil Rights, and Speech*, 20 HARV. C.R.-C.L. L. REV. 1, 21 (1985).

186. *Am. Booksellers Ass'n*, 771 F.2d at 328.

187. *Id.* at 329. He also, unflatteringly and unfairly, compared pornography to "racial bigotry, anti-semitism, violence on television, [and] reporters' biases . . . ." *Id.* at 330.

188. *Id.*

189. Citron & Franks, *supra* note 163, at 388.

190. *Id.*

important terms, such as "sexually explicit," "nude," and "disclosure."[191] This tailoring, Citron and Franks explained, would elide constitutional issues with the legislation.[192]

Many state legislatures agreed and answered Citron and Franks' call, some even developing their bills in consultation with them.[193] In less than a decade, the United States went from one New Jersey law to criminal nonconsensual intimate imagery statutes in 48 states, Guam, and the District of Columbia.[194] But not every state credited Citron and Franks' criteria for a criminal law. To the contrary, Arizona's attempt at a criminal nonconsensual intimate imagery law embodied why the state earned its wild, wild west reputation.

The Arizona nonconsensual intimate imagery law stated that it was:

> unlawful to intentionally disclose, display, distribute, publish, advertise, or offer a photograph, videotape, film or digital recording of another person in a state of nudity or engaged in specific sexual activities if the person knows or should have known that the depicted person has not consented to the disclosure.[195]

The law ignored all of Citron and Franks' recommendations. It did not require proof of harm—it did not even require proof that the person was recognizable or had a reasonable expectation of privacy in the image. It provided a handful of public interest exemptions, including when reporting unlawful activity to law enforcement or as required by law, when seeking medical treatment, and

191. *Id.* at 388–89.

192. Citron and Franks disagreed about the standard for a mens rea requirement. *Id.* at 387 n.278. For endorsements of constitutional criminal nonconsensual intimate imagery laws, see Adrienne N. Kitchen, *The Need to Criminalize Revenge Porn: How a Law Protecting Victims Can Avoid Running Afoul of the First Amendment*, 90 CHI.-KENT L. REV. 247 (2015). Others preferred the categorization of nonconsensual intimate imagery as unprotected speech. *See, e.g.*, Evan Ribot, *Revenge Porn and the First Amendment: Should Nonconsensual Distribution of Sexually Explicit Images Receive Constitutional Protection?*, UNIV. CHI. L.F. 15 (2019); *cf.* John A. Humbach, *The Constitution and Revenge Porn*, 35 PACE L. REV. 215 (2014); Sarah Jeong, *Revenge Porn Is Bad. Criminalizing It Is Worse*, WIRED (Oct. 28, 2013), https://www.wired.com/2013/10/why-criminalizing-revenge-porn-is-a-bad-idea/.

193. *See* Mary Anne Franks, *"Revenge Porn" Reform: A View from the Front Lines*, 69 FLA. L. REV. 1251, 1293 (2017).

194. Chance Carter, *An Update on the Legal Landscape of Revenge Porn*, NAT'L ASSOC. ATTORNEYS GENERAL (Nov. 16, 2021), https://www.naag.org/attorney-general-journal/an-update-on-the-legal-landscape-of-revenge-porn/. Since 2016, Representative Jackie Spier has introduced federal nonconsensual intimate imagery legislation on several occasions. *Intimate Privacy Protection Act Reintroduced in Congress*, EPIC (May 21, 2019), https://epic.org/intimate-privacy-protection-act-reintroduced-in-congress/.

195. Antigone Books v. Horne, Complaint, No. 2:14-cv-02100, at *18 (D. Ariz. Sept. 23, 2014), https://www.aclu.org/legal-document/antigone-books-v-horne-complaint. I was formerly a bookseller at Changing Hands Bookstore, one of the named plaintiffs.

when voluntarily exposed publicly or commercially.[196] Newsworthiness was not among them.[197] And while it included a definitions section, "disclosure" was not among the terms defined there.[198] The law was flawed and overbroad. It's no surprise that the American Civil Liberties Union took issue with it.

In *Antigone Books v. Horne*, the first lawsuit challenging a criminal nonconsensual intimate imagery law, Arizona bookstores rallied to protest the overbroad law banning speech.[199] Booksellers explained that any law that criminalizes displaying Pulitzer Prize-winning photographs, publishing news articles detailing detainees' abuse, distributing educational images of breast-feeding mothers, and disclosing unsolicited sexts to a parent—and that poses an existential threat to galleries, libraries, and bookstores that show, share, and sell works featuring nudity—must be unconstitutionally overbroad.[200] However, the court never got a chance to agree. The booksellers and the Attorney General stipulated that the government would be permanently enjoined from "enforcing, threatening to enforce, or otherwise using Arizona Revised Statute § 13-1425 in its current form."[201]

After Arizona, several other states squarely confronted the constitutionality of their nonconsensual intimate imagery statutes. Vermont's Supreme Court rejected the State's assertion that all nonconsensual intimate imagery amounted to unprotected obscenity, but concluded that its interest in criminalizing nonconsensual intimate imagery was compelling, narrowly tailored, and constitutional.[202] After Illinois's statute was struck down by the lower court, the Illinois Supreme Court declined to create a new category of unprotected speech but determined that the statute did not overly restrict the disseminator's speech and was neither overbroad nor vague.[203] And the Minnesota Supreme Court similarly reversed the court of appeals by rejecting

196. *Id.*

197. *Id.* Without such an exception, Sydney Leathers' disclosure of Congressman Anthony Weiner's nudes could have been a crime. *See generally* Abraham Riesman, *The Secret Struggle of the Woman Who Took Down Weiner*, N.Y. MAG. (May 20, 2016), https://www.thecut.com/2016/05/pain-triumph-weiner-sexter-sydney-leathers.html.

198. Antigone Books v. Horne, Complaint, No. 2:14-cv-02100, at *18–19 (D. Ariz. Sept. 23, 2014), https://www.aclu.org/legal-document/antigone-books-v-horne-complaint.

199. *Id.*

200. *Id.* at *3.

201. *See* Final Decree, Antigone Books v. Horne, No. 2:14-cv-02100, at *2 (D. Ariz. July 10, 2015), https://www.aclu.org/legal-document/antigone-books-v-horne-final-decree/. The law has since been amended. Ariz. Rev. Stat. § 13-1425.

202. State v. Rebekah S. VanBuren, 214 A.3d 791, 799 (Vt. 2019) https://www.vermontjudiciary.org/sites/default/files/documents/op16-253.pdf.

203. People v. Austin, 155 N.E.3d 439, 474 (Ill. 2019), https://courts.illinois.gov/Opinions/SupremeCourt/2019/123910.pdf.

attempts to carve out nonconsensual intimate imagery as unprotected speech and ultimately upheld the statute as constitutional.[204] In each case, the courts detailed and credited the serious harms inflicted on victims of nonconsensual intimate imagery, often citing Citron and Franks.[205]

But constitutionality is accompanied by another challenge facing criminal nonconsensual intimate imagery laws: the criminal legal system itself. During the height of the Black Lives Matter protests in 2020, some feminists amplified longtime calls for abolition of the criminal legal system.[206] And yet, as Citron and Franks illustrated, criminal laws can be invoked to prosecute harms against women and girls. How could those truths coexist? Elizabeth Bernstein coined the term "carceral feminism" as her resounding response that they cannot.[207]

Carceral feminism describes the allure of a law-and-order agenda, an approach which reflects a "drift from the welfare state to the carceral state as the enforcement apparatus for feminist goals."[208] However, with poorly drafted nonconsensual intimate imagery laws like Arizona's, feminist goals can be easily subverted and those laws turned against marginalized people, including trans and queer people. Sharing images of top surgeries, swapping photographs of queer intimacy, and even exposing videos of sexual harassment to the press could be swept into the scope of an overbroad criminal nonconsensual intimate imagery law, which could be weaponized by motivated prosecutors.[209] When it comes to crafting criminal legal interventions, the specifics are critical.

---

204. State v. Casillas, 952 N.W.2d 629 (Minn. 2020), https://www.courthousenews.com/wp-content/uploads/2020/12/mn-revenge.pdf.

205. *Rebekah S. VanBuren*, 214 A.3d at 794; People v. Austin, 155 N.E.3d at 451; *Casillas*, 952 N.W.2d at 644 n.10. For the First Amendment wonks, the courts applied different standards of scrutiny, with some opting for strict and other opting for intermediate scrutiny. *Id.*

206. *See, e.g.*, Lanre Bakare, *Angela Davis: 'We Knew That the Role of the Police Was to Protect White Supremacy*, GUARDIAN (June 15, 2020), https://www.theguardian.com/us-news/2020/jun/15/angela-davis-on-george-floyd-as-long-as-the-violence-of-racism-remains-no-one-is-safe (recounting activist Angela Davis' decades-long campaign to defund the police). For a deeper dive into Davis' approach to prison abolition, see ANGELA Y. DAVIS, ARE PRISONS OBSOLETE? (2011).

207. Bernstein, *supra* note 164.

208. *Id.* at 143; Mimi Kim, *From Carceral Feminism to Transformative Justice: Women-of-Color Feminism and Alternatives to Incarceration*, 27 J. ETHNIC & CULTURAL DIVERSITY SOC. WORK 219 (2018), https://transformharm.org/wp-content/uploads/2018/12/Kim-2018-FromCarceralFeminismtoTransformativeJustice.pdf.

209. Back in Arizona, law enforcement harassed the *Phoenix New Times* for printing artistic photographs of nude children by artist Betsy Schneider under broad child sex abuse material (CSAM) criminal laws. Amy Silverman, *Artist Betsy Schneider Takes Pictures of Her Children Naked and Shows Them to the World*, PHOENIX NEW TIMES (Aug. 14, 2008), https://

III. IMPORTANCE OF ACCESSIBILITY TO CYBERLAW

Former Senator Exon opened his remarks before the Senate by quoting a chaplain.[210] "Almighty God, Lord of all life," he proclaimed, "we praise You for the advancements in computerized communications that we enjoy in our time. Sadly, however, there are those who are littering this information superhighway with obscene, indecent, and destructive pornography."[211] Exon's prayer preluded his introduction of legislation criminalizing minors' access to sex online.[212]

The Communications Decency Act (CDA) was intended to shield minors from "obscene or indecent messages," as well as "patently offensive" messages, defining the latter as any message that "in context, depicts or describes . . . sexual or excretory activities or organs."[213] The law criminalized knowingly sending such messages to minors.[214] The CDA did not define "indecent."[215] And while it cribbed obscenity language from Miller, it excluded any of the exemptions and caveats that made obscenity bans constitutional. Though Exon's office was unlikely to acknowledge the inspiration, the CDA nevertheless mirrored many concerns raised by the radical feminist *Hudnut* ordinance.[216] Immediately after the CDA was enacted, the ACLU and nineteen other plaintiffs challenged its constitutionality.

In *Reno v. American Civil Liberties Union*, the Supreme Court squarely confronted the internet for the first time.[217] In its inaugural decision on this new medium, Justice Stevens explained that the internet was "known to its users as 'cyberspace' . . . located in no particular geographical location but

www.phoenixnewtimes.com/news/artist-betsy-schneider-takes-pictures-of-her-children-naked-and-shows-them-to-the-world-6438551; Nick Martin, *Newspaper's Nude Child Photos Draw Police Review*, EAST VALLEY TRIB. (Aug. 18, 2008), https://www.eastvalleytribune.com/news/article_89b8be5b-ee57-5c01-a7e3-a7aa0cb83918.html?mode=jqm.

210. 141 CONG. REC. S8329 (daily ed. June 14, 1995).

211. *Id.*; Exon Amendment No. 1268.

212. Reno v. ACLU, 521 U.S. 844, 849 (1997).

213. *Id.* at 859–60.

214. *Id.*

215. *Id.*

216. The more obvious influence is conservativism.

217. *Id.* Technically, its first mention of cyberspace was a concurrence citation to Lawrence Lessig. Denver Area Ed. Telecomm. Consortium v. F.C.C., 518 U.S. 727, 777 (1996). Since then, four other Supreme Court cases mention cyberspace. Nixon v. Shrink Missouri Gov't P.A.C., 528 U.S. 377, 408 (2000); Ashcroft v. ACLU, 535 U.S. 564, 612 (2002); United States v. Am. Library Ass'n, 539 U.S. 194, 240 n.6 (2003); Rowe v. New Hampshire Motor Transport Ass'n, 552 U.S. 364, 377–78 (2008); Packingham v. North Carolina, 582 U.S. 98, 104 (2017).

available to anyone, anywhere."[218] Despite the government's claim that the CDA amounted to a sort of "cyberzoning," its provisions "applie[d] broadly to the entire universe of cyberspace."[219] As a result, the Court determined that the CDA was a blanket, content-based restriction of speech.[220] And a vague and overbroad one at that.[221]

The CDA was silent about whether determinations of indecency or patent offensiveness were from the perspective of minors or all of society.[222] With regards to the latter, Justice Stevens expressed prescient concerns about criminalizing parents who emailed their underage college freshmen information about birth control because the college town's community may find those communications indecent or patently offensive.[223] These issues, among others, led the Court to conclude that the CDA was unconstitutional under the First Amendment.[224] As Justice Stevens put it, the CDA "threaten[ed] to torch a large segment of the internet community . . . [and] the interest in encouraging freedom of expression in a democratic society outweighs any theoretical but unproven benefit of censorship."[225]

The Court's decision in *Reno* enabled free, easy access to sexual content online—but only for some people and only in some contexts. This Part uses accessibility to examine how governing sex in cyberspace plays out across the Americans with Disabilities Act (ADA) and a surviving portion of the CDA, § 230. For many disabled users, ubiquitous online sex remains accessible only hypothetically. Section III.A examines how strategic litigation under the ADA casts the internet as a "place of public accommodation" requiring full accessibility of websites, including pornographic ones. Rather than provide paths to accessibility, other areas of law pose barriers to it. Section III.B illustrates how the FOSTA/SESTA amendments to the CDA existentially threaten sex workers' online content with dangerous offline effects. Both laws expose how sex and accessibility in cyberlaw mesh and how feminist cyberlaw

218. *Reno v. ACLU*, 521 U.S. at 851.

219. *Id.* at 868.

220. *Id.*

221. *Id.* at 871–73.

222. *Id.* at 871 n.37.

223. *Id.* at 878. It is difficult to believe that the Supreme Court used to care about accessibility of information about birth control, but it did. *Compare* Griswold v. Connecticut, 381 U.S. 479 (1965) (recognizing that the constitutional right to privacy protects use of contraception by married people), *with* Dobbs v. Jackson Women's Health Org., U.S. No. 19-1392 (2022), at *37 (perhaps not?).

224. Reno v. ACLU, 521 U.S. 844, 879 (1997).

225. *Id.* at 882, 885.

provides a framework for linking them to other restrictions on information, such as employment, childcare, and healthcare resources.

A. ACCESSING THE INTERNET USING THE AMERICANS WITH DISABILITIES ACT

On October 5, 2019, a New Yorker named Yaroslav Suris did what many people do on a Saturday: he visited a series of popular porn websites in an attempt to watch some videos.[226] But titles like "Sexy Cop Gets Witness to Talk," among others, did not work for Suris.[227] But the websites were not down for maintenance. His operating system was updated. There was no outage with his wireless service. The videos' unavailability was more fundamental. Suris is deaf, and none of the websites had adequate closed captioning.[228]

While Suris is a man, resource inaccessibility disproportionately affects women. One in four people in the country are disabled, and most disabled people are women.[229] Accessing sex is important, but websites increasingly determine the availability of other life-critical resources like banking, employment applications, childcare video conferences, and healthcare resources. Ensuring the internet's full accessibility to disabled people could not be more urgent.

One approach to creating accessible television programs, DVDs, and streaming services is closed captioning, which displays transcribed and descriptive text over the videos. With closed captioning, deaf and hard-of-hearing people can enjoy videos, and it also enables anyone to experience videos in environments that might be loud, such as in bars and restaurants, or

226. Suris v. MG Freesites, First Amended Complaint, No. 1:20-cv-00284, at *3 (June 10, 2020).

227. *Id.* at 5. This Article does not endorse the use of any cops, let alone sexy cops, to coerce confessions from people accused of crimes.

228. *Id.* at 2–3. This Article does not capitalize deaf because here, it refers to the audiological condition of not hearing rather than the specific community of Deaf people who share a language, culture, and community. *See generally* CAROL PADDEN & TOM HUMPHRIES, DEAF IN AMERICA: VOICES FROM A CULTURE (Harv. U. Press 1988) (describing features of the Deaf community).

229. Catherine A. Okoro, NaTasha D. Hollis, Alissa C. Cyrus, Shannon Griffin-Blake, *Prevalence of Disabilities and Health Care Access by Disability Status and Type Among Adults—United States, 2016*, CTR. FOR DISEASE CTRL. (Aug. 17, 2018), https://www.cdc.gov/mmwr/volumes/67/wr/mm6732a3.htm; *Disability and Health Information for Women with Disabilities*, CTR. FOR DISEASE CTRL. (2022), https://www.cdc.gov/ncbddd/disabilityandhealth/women.html. Roughly thirty-six million women are disabled in the United States. *Spotlight on Women with Disabilities*, DEP'T LAB. (Mar. 2021), https://www.dol.gov/sites/dolgov/files/ODEP/pdf/Spotlight-on-Women-with-Disabilities-March-2021.pdf.

in quiet environments, like libraries and hospitals.[230] While the Federal Communications Commission (FCC) regulates closed captioning for television, its regulations generally do not require captions for internet videos.[231] But Suris wasn't concerned with FCC regulations. Instead, he sued some of the biggest porn video websites alleging violation the ADA as a means of, as Bradley Allan Areheart and Michael Ashley Stein put it, "integrating the [i]nternet."[232] But the ADA is not a feminist cyberlaw.[233] Indeed, it's not a cyberlaw at all. Instead, it falls within the first category of "cyberlaws" as a general law that can be appropriated for feminist goals, like promoting web accessibility.

---

230. This is an example of the "curb-cut effect," a term coined by Angela Glover Blackwell to describe how accessibility innovations for marginalized people improve conditions for all people. Angela Glover Blackwell, *The Curb-Cut Effect*, STAN. SOC. INNO. REV. (Winter 2017), https://ssir.org/articles/entry/the_curb_cut_effect. The premise is powerful, but attempted implementation can prioritize ableist "universal" accessibility at the expense of disabled people's lived experience. Blake Reid, *The Curb-Cut Effect, Spillovers, and the Perils of Accessibility Without Disability*, *in* FEMINIST CYBERLAW (Meg Leta Jones & Amanda Levendowski eds., forthcoming 2024) (manuscript on file with author). For a deeper dive into closed captioning, see Blake Reid, *Third Party Captioning and Copyright*, GLOBAL INITIATIVE FOR INCLUSIVE INFORMATION & COMM. TECH. (2014), https://ssrn.com/abstract=2410661.

231. *Closed Captioning of Internet Video Programming*, FED. TRADE COMM'N (2022), https://www.fcc.gov/consumers/guides/captioning-internet-video-programming (outlining limited exceptions).

232. Bradley Allan Areheart & Michael Ashley Stein, *Integrating the Internet*, 83 GEO. WASH. L. REV. 449 (2015); Suris v. Mindgeek Holding, First Amended Complaint, No. 1:20-cv-00284, at *4 (June 10, 2020). Suris' lawsuit was perhaps the most salacious, but it was far from the first. Decisions about web accessibility remain limited, but lawsuits are skyrocketing. Minh Vu, Kristina Launey & John Egan, *The Law on Website and Mobile Accessibility Continues to Grow at a Glacial Pace Even as Lawsuit Numbers Reach All-Time Highs*, AM. BAR ASS'N.: TECHSHOW ISSUE (Jan. 1, 2022), https://www.americanbar.org/groups/law_practice/publications/law_practice_magazine/2022/jf22/vu-launey-egan/. In the wake of booming litigation, the Department of Justice (DOJ) recently issued guidance on web accessibility under the ADA. *Guidance on Web Accessibility and the ADA*, DEP'T JUST. (Mar. 18, 2022), https://beta.ada.gov/resources/web-guidance/. The DOJ guidance is so new that it's still hosted on a beta website. *Id.* But the internet's hostility to disability predates this wave of litigation considerably and reflects it deeply. For an accounting of internet ableism, see Blake Reid, *Internet Architecture and Disability*, 95 IND. L.J. 591 (2020).

233. Scholars, particularly junior ones, long recognized that it might be used that way, however. *See* Kenneth Kronstadt, Note, *Looking Behind the Curtain: Applying Title III of the Americans with Disabilities Act to Business Behind Commercial Websites*, 81 S. CAL. L. REV. 111 (2007); Katherine Rengel, *The Americans with Disabilities Act and Internet Accessibility for the Blind*, 25 JOHN MARSHALL J. COMPUT. & INFO. L. 543 (2008); Stephanie Khouri, Note, *Disability Law—Welcome to the New Town Square of Today's Global Village: Website Accessibility for Individuals with Disabilities after* Target *and the 2008 Amendments to the Americans with Disabilities Act*, 32 U. ARK. LITTLE ROCK L. REV. 331 (2010).

After decades of advocacy by disability rights activists and organizations, Congress finally recognized that disabled people are subjected to rampant isolation and discrimination, and—unlike many other marginalized people—lacked adequate legal means of recourse to address their subjugation.[234] In 1990, the ADA was enacted to, in part, "provide a clear and comprehensive national mandate for the elimination of discrimination against individuals with disabilities."[235] It included the charge that:

> No individual shall be discriminated against on the basis of disability in the full and equal enjoyment of the goods, services, facilities, privileges, advantages, or accommodations of any place of public accommodation by any person who owns, leases (or leases to), or operates a place of public accommodation.[236]

The ADA defined a "public accommodation" as encompassing more than a dozen private entities whose operations "affect commerce," including "motion picture houses, laundromats, museums, and day care centers."[237] While the ADA did not expressly limit itself to physical places, all its examples were brick-and-mortar establishments.[238] Its impact was huge, opening new spaces to the sixty-one million adults in the United States living with a disability.[239]

The ADA defines "discrimination" as the exclusion, denial, or segregation of disabled people, including people who require auxiliary aids.[240] Qualifying entities may need to provide aids and services that include, among other examples, "qualified interpreters or other effective methods of making aurally delivered materials available to individuals with hearing impairments."[241] Suris' lawyer followed the steps of others to connect the two provisions and allege

234. 42 U.S.C. § 12101(a). For a deeper history of the ADA and its champions, see JUDITH HEUMANN & KRISTEN JOINER, BEING HEUMANN: AN UNREPENTANT MEMOIR OF A DISABILITY RIGHTS ACTIVIST (2020) (iconic disability rights activist recounting her and others' activism that enabled the ADA).

235. 42 U.S.C. § 12101(b). The ADA was signed into law by President George H.W. Bush surrounded by all White disability rights advocates, even though an estimated one-third of all Black Americans murdered by police have a physical or mental disability. *See* Nora McGreevy, *The ADA Was a Monumental Achievement 30 Years Ago, but the Fight for Equal Rights Continues*, SMITHSONIAN MAG. (July 24, 2020), https://www.smithsonianmag.com/history/history-30-years-since-signing-americans-disabilities-act-180975409/.

236. 42 U.S.C. § 12182(a).

237. 42 U.S.C. § 12181(7).

238. *Id.*

239. *Disability Impacts All of Us*, CTR. FOR DISEASE CONTROL & PREVENTION (2022), https://www.cdc.gov/ncbddd/disabilityandhealth/infographic-disability-impacts-all.html.

240. 42 U.S.C. §§ 12101, 12182.

241. 42 U.S.C. §§ 12103(1), 12182(2)(a)(3).

that the absence of effective closed captioning constituted a failure to provide auxiliary aids and services for deaf and hard-of-hearing people as required in places of public accommodation—this time, in cyberspace. And Suris had the law on his side.

Circuits remain split about how the ADA applies to the internet, with some declining to apply the ADA to websites that exist separately from a physical location.[242] But in the Eastern District of New York, where Suris filed his lawsuit, Judge Weinstein had previously taken an expansive view of the ADA's mandate to dismantle ableism. "A rigid adherence to a physical nexus requirement leaves potholes of discrimination in what would otherwise be a smooth road to integration," he wrote, continuing that "[i]t would be perverse to give such an interpretation to a statute intended to comprehensively remedy discrimination."[243] But a judge never invoked Judge Weinstein's conclusion to determine that Suris and other disabled people were entitled to equal access to experiencing sex online. Five months after Suris sued, the parties settled on undisclosed terms.[244]

242. Websites with brick-and-mortar locations are generally covered. The First Circuit previously held that a public accommodation did not need to be a physical place, though it has yet to squarely address the website question. *See* Carparts Distrib. Ctr. v. Auto Wholesalers' Ass'n of New England, 37 F.3d 12, 19–20 (1st Cir. 1994). The Third and Sixth Circuits have likewise yet to address the internet question, but previously held that public accommodations only extend to physical places. *See* Ford v. Schering-Plough Corp., 145 F.3d 601, 613 (3d Cir. 1998); Parker v. Metro. Life Ins. Co., 121 F.3d 1006, 1010 (6th Cir. 1997). The Ninth Circuit excludes websites with no offline presence. *See* Cullen v. Netflix, Inc., 600 F.App'x 508 (9th Cir. 2015). The district court landscape, including intra-E.D.N.Y., is a chaotic patchwork. *Compare* Winegard v. Newsday LLC., 556 F. Supp. 3d 173 (E.D.N.Y. 2021) (deciding that a website is not a place of public accommodation requiring captions), *with* Andrews v. Blick Art Materials, 268 F. Supp. 3d 381 (E.D.N.Y. 2017) (noting that a website may be a place of public accommodation). For more scholarly examinations of the internet as a place of public accommodation, see, e.g., Jonathan Bick, *Americans with Disabilities Act and the Internet*, 10 ALB. L.J. SCI. & TECH. 205; Colin Crawford, *Cyberplace: Defining a Right to Internet Access Through Public Accommodation Law*, 76 TEMP. L. REV. 225 (2003); Richard E. Moberly, *The Americans with Disabilities Act in Cyberspace: Applying the "Nexus" Approach to Private Internet Websites*, 55 MERCER L. REV. 963 (2004); Priya Elayath, *Americans with Disabilities Act's Title III Public Accommodations and its Application to Web Accessibility and Telemedicine*, 17 U. ST. THOMAS L.J. 156 (2020); Hassah Ahmad, *Beyond Sight: Modernizing the Americans with Disabilities Act and Ensuring Internet Equality for the Visually Impaired*, 25 J. GENDER RACE & JUST. 321 (2022).

243. Andrews v. Blick Art Materials, 268 F. Supp. 3d 381, 397 (E.D.N.Y. 2017).

244. Suris v. MG Freesites, Notice of Settlement, No. 1:20-cv-00284 (Nov. 6, 2020), https://storage.courtlistener.com/recap/gov.uscourts.nyed.443933/gov.uscourts.nyed.443933.25.0.pdf. Suris has been the named plaintiff in several other ADA-related lawsuits with mixed results. *See, e.g.*, Suris v. Gannett, No. 20-cv-1793 (E.D.N.Y. July 14, 2021); Suris v. Collive Corp., No. 20-cv-06096 (E.D.N.Y. Jan. 10, 2022).

Closed captioning is far from the only accessibility issue disabled people face when seeking sex, or any information, online.[245] Many disabled people, disproportionately so, do not own computers or smartphones or even access the web.[246] A full 15% of disabled adults report not using the internet at all.[247] Rarely discussed, this manifestation of the so-called "digital divide," compounded by technical accessibility issues, deprives disabled people of experiencing the internet. While disabled people have proven that it is possible to live offline, it will become increasingly difficult as more life-critical resources shift to websites and apps.

Already, systemic barriers deny disabled people the positive effects of engaging with sex online, which can be educational, enjoyable, and even ethical.[248] Pornography also creates opportunities for representation: many sex workers are disabled.[249] The presence of disabled people in sex work is powerful. As much as society and the media ignore it, sex worker Billy Autumn explained that "[d]isabled people fuck."[250]

245. The Center for Democracy and Technology has done an impressive job of centering these issues—which include biased automated hiring software, flawed algorithmic benefits assessments, oppressive content moderation policies, and increased surveillance tools in schools—in recent years. Maria Town & Alexandra Reeve Givens, *In Our Tech Reckoning, People with Disabilities are Demanding a Reckoning of Their Own*, TECH. POL'Y PRESS (Jan. 24, 2022), https://techpolicy.press/in-our-tech-reckoning-people-with-disabilities-are-demanding-a-reckoning-of-their-own/.

246. Andrew Perrin & Sara Atske, *Americans with Disabilities Less Likely Than Those Without to Own Some Digital Devices*, PEW RSCH. CTR. (Sept. 10, 2021), https://www.pewresearch.org/fact-tank/2021/09/10/americans-with-disabilities-less-likely-than-those-without-to-own-some-digital-devices/.

247. *Id.*

248. Emily F. Rothman, *The Benefits of Pornography*, PORNOGRAPHY & PUB. HEALTH ch. 13 (2021). For deeper dives into the digital divide, see Haochen Sun, *Bridging the Digital Chasm Through the Fundamental Right to Technology*, 28 GEO. L. REV. 75 (2020); Kathryn Zickuhr & Aaron Smith, *Digital Differences*, PEW RSCH. CTR. (Apr. 13, 2012), http://www.pewinternet.org/2012/04/13/digital-differences.

249. Loree Erickson, *Why I Love Hickies and Queer Crip Porn*, COMING OUT LIKE A PORN STAR: ESSAYS ON PORNOGRAPHY, PROTECTION, AND PRIVACY (Jiz Lee ed., 2015) (recounting sex work with disabilities); moses moon, *Symposium Introduction: Sex Workers' Rights, Advocacy, and Organizing*, 52 COLUM. HUM. RTS. L. REV. 1062 (2021) (recounting sex work with disabilities); *Sex Work as Work and Sex Work as Anti-Work*, HACKING//HUSTLING (Apr. 2021), https://www.youtube.com/watch?v=sxAAXHS-QfE (engaging with a disability-centered sex work ethos); Katie Tastrom, *Sex Work is a Disability Issue. So Why Doesn't the Disability Community Recognize That?*, ROOTED IN RIGHTS (Jan. 4, 2019), https://rootedinrights.org/sex-work-is-a-disability-issue-so-why-doesn't-the-disability-community-recognize-that/.

250. Sophie Saint Thomas, *These Disabled Porn Performers are Changing How We Talk About Sex and Disability*, MIC (Dec. 16, 2015), https://www.mic.com/articles/130673/these-disabled-porn-performers-are-changing-how-we-talk-about-sex-and-disability.

Many radical feminists, as well as others, object to those framings of pornography.[251] Anti-pornography feminists, including MacKinnon and Dworkin, believe that pornography is exploitative and subjugates women.[252] As Gail Dines put it, "[p]ornography is the perfect propaganda piece for the patriarchy. In nothing else is their hatred of us quite as clear."[253] Anti-pornography feminists also point to disturbing research detailing dangerous effects of pornography.[254] However, it remains unclear how pervasive cultural misogyny factors into people's experiences of pornography, including whether research results are attributable to correlation or causation. This ambiguity is why some researchers liken pornography to alcohol, which is likewise legal, ubiquitous, and extensively regulated—individual reactions depend on the person and vary considerably.[255] But society has determined that these variations are not justifications for bans.

---

251. So do some other feminists. Conservative feminists, for example, likewise reject that pornography holds value. Those arguments go beyond the scope of this Article, but a deeper dive is provided by P. Brooks Fuller, Kyla P. Garrett Wagner & Farnosh Mazandarani, *Porn Wars: Serious Value, Social Harm, and the Burdens of Modern Obscenity*, 28 AM. U. J. GENDER SOC. POL'Y & L. 121 (2020).

252. ANDREA DWORKIN, PORNOGRAPHY: MEN POSSESSING WOMEN (1981); ANDREA DWORKIN & CATHARINE A. MACKINNON, PORNOGRAPHY AND CIVIL RIGHTS: A NEW DAY FOR WOMEN'S EQUALITY 138 (1988). Anti-pornography feminism is also bound up with objections to sex work, as discussed *supra* in Section III.B.

253. Julie Bindel, *The Truth About the Porn Industry*, GUARDIAN (July 2, 2010), https://www.theguardian.com/lifeandstyle/2010/jul/02/gail-dines-pornography. For a deeper dive into anti-pornography views, see GAIL DINES, PORNLAND: HOW PORN HAS HIJACKED OUR SEXUALITY (Beacon Press 2011). Some scholars and performers would counter that this perspective erases the experiences of women performers, as well as men, trans men, and nonbinary performers. HEATHER BERG, PORN WORK: SEX, LABOR, AND LATE CAPITALISM (2021) (detailing reflections from dozens of pornography performers); R.L. Goldberg, *Staging Pedagogy in Trans Masculine Porn*, 7 TRANSGENDER STUDIES Q. 208 (2020), https://read.dukeupress.edu/tsq/article-abstract/7/2/208/164819/Staging-Pedagogy-in-Trans-Masculine-Porn; Angela Jones, *Cumming to a Screen Near You: Transmasculine and Non-Binary People in the Camming Industry*, 8 PORN STUDIES 239 (2021), https://www.tandfonline.com/doi/abs/10.1080/23268743.2020.1757498.

254. *See, e.g.*, Gert Martin Hald, Neil M. Malauth & Carlin Yuen, *Pornography and Attitudes Supporting Violence Against Women: Revisiting the Relationship in Nonexperimental Studies*, 36 AGGRESSIVE BEHAVIOR 14 (2009) (meta-analysis linking habitual pornography viewing with violent ideation and behavior); Simone Kühn & Jürgen Gallinat, *Brain Structure and Functional Connectivity Associated with Pornography Consumption: The Brain on Porn*, 7 J. AM. MED. ASS'N PSYCHIATRY 827 (2014) (finding decreases in brain activity of habitual pornography viewers); Paula Banca, Laurel S. Morris, Simon Mitchell, Neil A. Harrison, Marc N. Potenza & Valerie Voon, *Novelty, Conditioning, and Attentional Bias to Sexual Rewards*, 72 J. PSYCHIATRIC RSCH. 91 (2016) (suggesting that pornography incentivizes habitual viewers to seek increasingly novel, hardcore images).

255. Zoe Cormier, *Is Porn Bad For You?*, BBC SCI. FOCUS (Dec. 21, 2020), https://www.sciencefocus.com/the-human-body/is-pornography-harmful/.

For now, the power of the ADA to promote web accessibility remains uncertain. The Supreme Court recently declined to resolve the developing circuit split over the scope of the ADA.[256] Disabled people across America are confronted with a patchwork of web accessibility decisions, with their civil rights limited by jurisdiction and happenstance. Only subsequent litigation or legislation will reveal the ability of the ADA to create a cyberspace that reflects the accessibility that disabled people deserve.

B. AMENDING COMMUNICATIONS DECENCY ACT § 230 TO CRIMINALIZE SEX WORK CONTENT

Internet accessibility is also a perennial problem for sex workers.[257] In the early 1990s, Danni Ashe joined Usenet, a precursor of contemporary web forums, and discovered that other users were illicitly swapping many of her photos.[258] She decided to go direct-to-consumer by introducing herself on the Alt.Sex newsgroup, pointing people to her fanclub address to promote her work as a stripper and dancer.[259] As she recounts, "I'll never forget the stern reply I got from . . . the moderator of Alt.Sex, saying my 'commercial postings' wouldn't be tolerated."[260] Decades later, the exclusionary sentiment that sex

256. *Robles v. Domino's Pizza, LLC*, 913 F.3d 898 (9th Cir. 2019), *cert. denied*, No. 18-1539 (Oct. 7, 2019). Some scholars have critiqued its invocation to enable web accessibility. Paul Taylor, *The Americans with Disabilities Act and the Internet*, 7 B.U. J. SCI. & TECH. L. 26 (2001); Eric Goldman, *Will the Americans With Disabilities Act Tear a Hole in Internet Law?*, ARS TECHNICA (June 27, 2012), https://arstechnica.com/tech-policy/2012/06/will-the-americans-with-disabilities-act-tear-a-hole-in-internet-law/.

257. *Sexual Gentrification: An Internet Sex Workers Built*, HACKING//HUSTLING (Apr. 6, 2022), https://hackinghustling.org/sexual-gentrification-an-internet-sex-workers-built/. Thanks to Kendra Albert for flagging many of the sources in this Part. A few words about "sex work." It can be, at once, a broad term describing exchanges of sex or sexual activity and a non-stigmatizing term for prostitution. Danielle Blunt & Ariel Wolf, *Erased: The Impact of FOSTA, SESTA*, HACKING//HUSTLING (2020), https://hackinghustling.org/wp-content/uploads/2020/02/Erased_Updated.pdf. Some sex workers only use the term to describe prostitution. *See, e.g.*, moses moon, *Symposium Introduction: Sex Workers' Rights, Advocacy, and Organizing*, 52 COLUM. HUM. RTS. L. REV. 1062 (2021) (situating erotic labor on a spectrum, which ranges from "legal pornography and erotic dancing (stripping), to quasilegal cyber erotic labor (including cammodeling and selling access to explicit videos on sites like OnlyFans and ManyVids), to illegal prostitution (sex work)). This Article uses the term broadly. Sex work can be work—or it can be antiwork. HEATHER BERG, PORN WORK: SEX, LABOR, AND LATE CAPITALISM (2021). And it can be a diverse community. As moses moon observes, there are more "Black, Asian, Latine, queer, and trans folks" involved and visible in the sex worker rights movement now than ever before." moses moon, *Symposium Introduction: Sex Workers' Rights, Advocacy, and Organizing*, 52 COLUM. HUM. RTS. L. REV. 1062, 1074 (2021).

258. Michael Brooks, *The Porn Pioneers*, GUARDIAN (Sept. 29, 1999), https://www.theguardian.com/technology/1999/sep/30/onlinesupplement.

259. *Id.*

260. *Id.*

workers do not belong on the internet was all but codified by the Fight Online Sex Trafficking Act and Stop Enabling Sex Traffickers Act (FOSTA/SESTA) amendments to the remainder of the CDA.[261] FOSTA/SESTA falls within the third category of cyberlaws—it purported to be a feminist cyberlaw, one that bundled its prohibitions with banning sex trafficking content, but it has subverted other feminist goals, like bodily autonomy.[262]

Unlike the parts of the CDA that were struck down by the Supreme Court, CDA § 230 had less to do with sex and everything to do with capitalism.[263] In the early 1990s, corporations began hosting interactive services, such as bulletin boards. Some users posted unflattering content, and subjects of users' unfavorable posts countered with litigation.[264] Not against users who'd posted the content, but against the companies that hosted their diatribes.[265] And subjects started winning.[266]

While some members of Congress fretted about the infinite accessibility of sex online, others feared that crushing financial liability for these interactive computer services would bludgeon the burgeoning internet.[267] Which is why

261. FOSTA stands for the House's Fight Online Sex Trafficking Act, H.B. 1865 (2017); SESTA refers to the Senate version, the Stop Enabling Online Sex Traffickers Act. S.1693 (2018). Following the lead of Kendra Albert and sex workers, this Article refers to the combined bills as "FOSTA/SESTA." *See, e.g.*, Kendra Albert, *Five Reflections from Four Years of FOSTA/SESTA*, CARDOZO ARTS & ENTM'T L.J. (forthcoming 2022) (using FOSTA/SESTA); moses moon, *Symposium Introduction: Sex Workers' Rights, Advocacy, and Organizing*, 52 COLUM. HUM. RTS. L. REV. 1062 (2021) (same); Danielle Blunt & Ariel Wolf, *Erased: The Impact of FOSTA-SESTA and the Removal of Backpage*, HACKING//HUSTLING (2020) (same), https://hackinghustling.org/wp-content/uploads/2020/02/Erased_Updated.pdf.

262. Liz Tung, *FOSTA/SESTA Was Supposed to Thwart Sex Trafficking. Instead, It's Sparked a Movement*, WHYY (July 10, 2020), https://whyy.org/segments/fosta-sesta-was-supposed-to-thwart-sex-trafficking-instead-its-sparked-a-movement/.

263. Of course, sex and capitalism often go hand-in-hand. For a deeper dive into sex work and capitalism, see HEATHER BERG, PORN WORK: SEX, LABOR, AND LATE CAPITALISM (2021) (interviewing eighty-one porn industry folks—including performers, producers, and directors—about their experiences with sex-work labor).

264. *See, e.g.*, Stratton Oakmont Inc. v. Prodigy Services Co., 1995 WL 323710 (S. Ct. N.Y. May 24, 1995) (successfully suing interactive service provider Prodigy for defamation over users' posts alleging that Stratton Oakmont engaged in criminal acts. Which it had—Martin Scorsese made an entire film about it.). WOLF OF WALL STREET (2013).

265. Stratton Oakmont, Inc. v. Prodigy Services Co., No. 31063/94, 1995 WL 323710, at *7 (N.Y. Sup. Ct. May 24, 1995).

266. *Id.*

267. Emily Stewart, *Ron Wyden Wrote the Law That Built the Internet. He Still Stands By It—And Everything It's Brought with It*, VOX (May 16, 2019), https://www.vox.com/recode/2019/5/16/18626779/ron-wyden-section-230-facebook-regulations-neutrality. Senator Wyden was one of two senators who opposed SESTA. *Roll Call Vote 115th Congress - 2nd Session*, U.S. SENATE (Mar. 21, 2018), https://www.senate.gov/legislative/LIS/roll_call_votes/vote1152/vote_115_2_00060.htm.

Senator Ron Wyden and former Representative Chris Cox introduced CDA § 230, which, at its operative core, stated

> No provider or user of an interactive computer service shall be treated as the publisher or speaker of any information provided by another information content provider.[268]

Effectively, CDA § 230 created a safe harbor for interactive computer services from liability for users' content. It threw in an incentive to moderate content without risking the loss of that safe harbor.[269] It included limited carve-outs from the safe harbor for hosting content in violation of criminal and intellectual property laws.[270] And after FOSTA/SESTA was enacted, it created new carve-outs for hosting user-generated content related to sex trafficking and prostitution.[271]

FOSTA/SESTA embraced a radical feminist view of sex work when it codified that:

> Nothing in this section . . . shall be construed to impair or limit . . . any charge in a criminal prosecution brought under State law if the conduct underlying the charge would constitute a violation of section 2421A of title 18 [criminalizing the promotion or facilitation of prostitution and reckless disregard of sex trafficking], and promotion or facilitation of prostitution is illegal in the jurisdiction where the defendant's promotion or facilitation of prostitution was targeted.[272]

The amendment codified the same impulse that booted Danni Ashe off Alt.Sex: sex workers should not be able to freely access the internet. As Kendra Albert explains, "FOSTA/SESTA is better understood as the logical extension

268. 47 U.S.C. § 230(c)(1). For a deeper dive into the history of CDA § 230, see JEFF KOSSEFF, THE TWENTY-SIX WORDS THAT CREATED THE INTERNET (Cornell U. Press 2019). That crimes and infringements are on the same level is a coup by the content-creation industry.

269. 47 U.S.C. § 230(c)(2).

270. 47 U.S.C. § 230(e). The latter exemption explains why ISPs are responsive to allegations of copyright infringement: not only can their failure to respond eliminate their DMCA safe harbor, but it can also shatter their CDA § 230 one.

271. 47 U.S.C. § 230(e). Both were already federal crimes that fell within the existing exemption for criminal content. 18 U.S.C. § 2421A. Accompanying provisions criminalized owning, operating, or managing interactive computer services with the intent to facilitate or promote prostitution and created a civil right of action for people harmed by services that promoted or facilitated trafficking of five or more people. 18 U.S.C. § 2421A. As Kendra Albert points out, FOSTA/SESTA did not remove CDA § 230 immunity for the latter claim, and courts have responded by saving Congress' failure and exempting sites for liability anyway. Kendra Albert, *Five Reflections from Four Years of FOSTA/SESTA*, CARDOZO ARTS & ENTM'T L.J., at 12 (forthcoming 2022).

272. 47 U.S.C. § 230(e)(5).

of a set of campaigns to make it more difficult for folks engaging in sex work to use mainstream public accommodations, often pushed in the name of fighting sex trafficking."[273] Viewed in that light, FOSTA/SESTA has been a resounding success at effectively banishing sex workers from web services that make their work safer.

Online advertising allowed sex workers to vet potential clients.[274] Social media sites let sex workers create supportive communities, as well as swap harm reduction tips and client information.[275] Used together, these aspects of the internet measurably reduced offline violence against sex workers.[276] FOSTA/SESTA threw a wrench in all of that.[277]

Even before FOSTA/SESTA, some sex workers struggled to place ads—many of the old standby websites folded.[278] After FOSTA/SESTA, however,

273. Kendra Albert, *Five Reflections from Four Years of FOSTA/SESTA*, CARDOZO ARTS & ENTM'T L.J., at 2 (forthcoming 2022), https://ssrn.com/abstract=4095115.

274. Catherine Barwulor, Allison McDonald, Eszter Hargittai & Elissa M. Redmiles, *"Disadvantaged in the American-Dominated Internet": Sex, Work, and Technology*, PROC. CHI. CONF. HUM. FACTORS IN COMPUT. SYS. (2021), https://dl.acm.org/doi/fullHtml/10.1145/3411764.3445378.

275. Sandra Song, *Inside Switter, the Sex Worker Social Network*, PAPER (Dec. 13, 2018), https://www.papermag.com/switter-sex-worker-social-network-2623333073.html. Switter closed down on May 14, 2022 "due to the collective weight of the recent anti-sex and anti-LGBTQIA+ legislative moves which made the continued operation of Switter untenable." *Rest in Power*, SWITTER (2022), https://switter.at/; *see also* Blunt & Wolf, *supra* note 261.

276. Online harassment, however, remained high. Teela Sanders, Jane Scoular, Rosie Campbell, Jane Pitcher & Stewart Cunningham, *Beyond the Gaze: Briefing on Internet Sex Work*, U. LEICESTER 7–8 (2018); *see also* REPLY ALL, #119 NO MORE SAFE HARBOR (Apr. 20, 2018) (interviewing economist Scott Cunningham about measurable impacts of FOSTA/SESTA on violence against sex workers and generally).

277. Lura Chamberlain, *FOSTA: A Hostile Law with a Human Cost*, 87 FORDHAM L. REV. 2171 (2019); Heidi Trip, *All Sex Workers Deserve Protection: How FOSTA/SESTA Overlooks Consensual Sex Workers in an Attempt to Protect Sex Trafficking Victims*, 124 PENN. STATE. L. REV. 219 (2019).

278. Craigslist's Adult section, Rentboy, and Backpage folded, largely due to concerns under existing laws, before the threat of FOSTA/SESTA. Claire Cain Miller, *Craigslist Says It Has Shut Its Section for Sex Ads*, N.Y. TIMES (Sept. 15, 2010), https://www.nytimes.com/2010/09/16/business/16craigslist.html (noting that seventeen attorneys general demanded the site's closure by letter); Lisa Duggan, *What the Pathetic Case Against Rentboy.com Says About Sex Work*, NATION (Jan. 7, 2016) (law enforcement targeting and, in some cases, arresting and charging, multiple employees of Rentboy.com for conspiracy to violate the Travel Act by promoting prostitution), https://www.thenation.com/article/archive/what-the-pathetic-case-against-rentboy-com-says-about-sex-work/; Dell Cameron, *Feds Praise Backpage Takedown as Sex Workers Fear for Their Lives*, GIZMODO (Apr. 9, 2018) (FBI seizing Backpage.com and prosecutors charging several affiliates with existing crimes), https://gizmodo.com/feds-praise-backpage-takedown-as-sex-workers-fear-for-t-1825124288.

many other sites declined to host their content.[279] Sex workers even reported content disappearing from Google Drive.[280] As one sex worker put it, "[s]ex workers are disappearing from the internet. Workers' sites have been taken down, ad sites are hard to comply with and are always changing their rules, Twitter and Instagram are deleting accounts just for being a sex worker."[281] Decisions by interactive computer services to effectively kick sex workers off their networks took a measurable toll: a comprehensive survey from sex worker collective Hacking//Hustling uncovered that 72.45% of respondents reported increased economic instability, and 33.8% reported increased violence from clients post-FOSTA/SESTA.[282] Yet no moves have been made to repeal the law.[283]

Effectively limiting sex workers' presence online does not present a problem for all feminists. Many radical feminists, among other feminists, oppose sex work and reject sex workers' assertions that they choose to engage in the sex trades.[284] Anti-sex-work feminists believe that sex work is economically coercive and reifies patriarchal views about women.[285] For anti-sex-work feminists, the harms of sex work cannot be overstated. In a debate about sex work, Catharine MacKinnon argued that the effect of money exchanged in sex work is akin to the physical force used in rape.[286]

Some scholars and sex workers counter anti-sex-work conceptualizations of the sex trades. Critiques of sex work ignore that all labor is coercive under

279. Jillian C. York, *Silicon Valley's Sex Censorship Harms Everyone*, WIRED (Mar. 18, 2022), https://www.wired.com/story/silicon-values-internet-sex-censorship/.

280. Samantha Cole, *Sex Workers Say Porn on Google Drive Is Suddenly Disappearing*, VICE (Mar. 21, 2018), https://www.vice.com/en/article/9kgwnp/porn-on-google-drive-error.

281. Blunt & Wolf, *supra* note 261, at 26.

282. *Id.* at 18; *see also* Lura Chamberlain, *FOSTA: A Hostile Law with a Human Cost*, 87 FORDHAM L. REV. 2171 (2019).

283. Representative Ro Khanna introduced legislation to study the effects of FOSTA/SESTA. The SAFE SEX Workers Study Act, H.R. 5448, 116th Cong. (2019-2020), https://www.congress.gov/bill/116th-congress/house-bill/5448/text. The bill failed.

284. Katie Beran, *Revisiting the Prostitution Debate: Uniting Liberal and Radical Feminism in Pursuit of Policy Reform*, 30 MINN. J.L. & INEQUITY 19 (2012). So do conservative feminists, but those views are beyond the scope of this Article. For a deeper dive into those views, see Karen Green, *Prostitution, Exploitation and Taboo*, 64 PHILOSOPHY 525, 532 (1989).

285. *See generally* KATHLEEN BARRY, THE PROSTITUTION OF SEXUALITY (NYU Press 1996).

286. *It's Wrong to Pay for Sex*, CONN. PUB. BROAD. NET. (May 8, 2009), https://web.archive.org/web/20100625230257/http://www.cpbn.org/program/intelligence-squared/episode/its-wrong-pay-sex. Catharine MacKinnon is a longtime vocal critic of sex work, as well as pornography. *See generally* CATHARINE A. MACKINNON, TOWARD A FEMINIST THEORY OF THE STATE (1989); CATHARINE A. MACKINNON, WOMEN'S LIVES, MEN'S LAWS (2007); Catharine MacKinnon, *Trafficking, Prostitution, and Inequality,* 46 HARV. C.R.-C.L. L. REV. 271 (2011).

capitalism, which does not negate the need for safe working conditions.[287] It also minimizes the experiences of queer men, trans men, and nonbinary people in the sex trades.[288] Sex workers have also called out the paternalism behind such arguments, which overlook the autonomy of sex workers to define their own destinies.[289] In their own account of their experiences trading sex, Lorelai Lee explained that "[t]he things that sex workers do to stay safe are almost always the things civilians want to pass laws to stop."[290] Through that lens, it is no surprise that sex workers' ability to freely access the internet sat squarely in congressional crosshairs.

Targeting sex workers' online content is not an isolated act—it's a harbinger of what will come for other marginalized communities. One of Albert's lessons for technology policy advocates from FOSTA/SESTA is a warning that targeting sex workers is rooted in the same misogynistic, heteronormative impulses underlying attacks on content related to trans people and abortion access.[291] They caution that "[s]hadowbanning, deplatforming, and the chilling effects that have come along with [FOSTA/SESTA] may happen to sex workers first, but as the invocations of moral panics succeed, the advocates who use them will not stop with those in the sex trades."[292] As trans healthcare and abortion are increasingly criminalized at the state level, interactive computer services may decide it's not worth hosting that content either.[293] FOSTA/SESTA demonstrates that interactive service providers will choose to censor content even if they needn't do so legally.

---

287. Malak Mansour, *On Marxism, Capitalism, and the Sex Industry*, WATCHDOGS GAZETTE (June 23, 2022), https://watchdogsgazette.com/opinions/on-marxism-capitalism-and-the-sex-industry/.

288. David Eichert, *"It Ruined My Life": FOSTA, Male Escorts, and the Construction of Sexual Victimhood in American Politics*, 26 VA. J. SOC. POL'Y & L. 201 (2019); Angela Jones, *Where the Trans Men and Enbies At?: Cissexism, Sexual Threat, and the Study of Sex Work*, 14 SOCIO. COMPASS 2 (2020), https://compass.onlinelibrary.wiley.com/doi/10.1111/soc4.12750.

289. HEATHER BERG, PORN WORK: SEX, LABOR, AND LATE CAPITALISM (2021). Hacking//Hustling and other sex worker collectives constantly reinforce this narrative through advocacy.

290. Lorelei Lee, *Cash/Consent: The War on Sex*, 35 N+1 MAG. (2019), https://www.nplusonemag.com/issue-35/essays/cashconsent/. Sex workers often refer to people outside the industry as "civilians." HEATHER BERG, PORN WORK: SEX, LABOR, AND LATE CAPITALISM (2021) (explaining that sex workers often refer to people outside the industry as "civilians.").

291. Kendra Albert, *Five Reflections from Four Years of FOSTA/SESTA*, CARDOZO ARTS & ENTM'T L.J. (forthcoming 2022).

292. *Id.*

293. 42 U.S.C. § 230(e)(3) ("Nothing in this section shall be construed to prevent any State from enforcing any State law that is consistent with this section. No cause of action may be brought and no liability may be imposed under any State or local law that is inconsistent with this section."). This already played out under FOSTA/SESTA, which resulted in the

IV. INFLUENCE OF SAFETY ON CYBERLAW

Assistant Majority Leader Rhonda Fields ran for office in Colorado because her son and his fiancée were shot and murdered in 2005.[294] To prevent heartbreak for other families, Fields sought office.[295] She was the first Black woman elected to her district in Aurora, Colorado.[296] Her district may sound familiar because, shortly into her term, a man opened fire in a crowed movie theatre, murdering twelve people and injuring seventy more.[297] Fields responded by supporting gun legislation that was signed into law by the governor.[298] Detractors retaliated. Fields' family became the targets of vicious online harassment. As Fields recounted, "I just thought this came with the job, but when they used my daughter's name, when they said 'We're going to come after you and your daughter and your family, and there will be lots of blood,' that's when it became real."[299] One email riddled with racist and sexist slurs was more explicit: "Hopefully somebody Gifords [sic] both of your asses with

censorship of some queer content. Nate 'Igor' Smith, *"The Death of Tumblr*," BOINGBOING (Dec. 3, 2018), https://boingboing.net/2018/12/03/the-death-of-tumblr.html; Matt Baume, *"How Queer Adult Comic Artists Are Being Silenced by FOSTA-SESTA*," THEM (Apr. 22, 2020), https://www.them.us/story/fosta-sesta-silencing-queer-comics. Criminalizing abortion also creates important questions for digital security. Karen Levy & Michela Meister, *Title Forthcoming*, *in* FEMINIST CYBERLAW (Meg Leta Jones & Amanda Levendowski eds., forthcoming 2024). It's beginning to happen with abortion content already. Benjamin Powers, *Facebook and Instagram Have Started Taking Down Abortion Pill Posts Since the Fall of* Roe, GRID (June 29, 2022), https://www.grid.news/story/technology/2022/06/29/facebook-and-instagram-have-started-taking-down-abortion-pill-posts-since-the-fall-of-roe/.

294. Karen Augé, *5 Years After Son's Murder, Mother Struggles to Redefine Her Life*, DENVER POST (July 17, 2010), https://www.denverpost.com/2010/07/17/5-years-after-sons-murder-mother-struggles-to-redefine-her-life/. Javad Fields was slated to testify in his friend's murder trial. *Id.*

295. Candice Norwood, Chloe Jones & Lizz Bolaji, *More Black Women Are Being Elected to Office. Few Feel Safe Once They Get There*, PBS NEWS HOUR (June 17, 2021), https://www.pbs.org/newshour/politics/more-black-women-are-being-elected-to-office-few-feel-safe-once-they-get-there.

296. *Id.*

297. A&E Television Networks, *Aurora Shooting Leaves 12 Dead, 70 Wounded*, HIST. (July 19, 2021), https://www.history.com/this-day-in-history/12-people-killed-70-wounded-in-colorado-movie-theater-shooting.

298. Associated Press, *Colorado Governor Signs Gun Control Bills*, POLITICO (Mar. 20, 2013), https://www.politico.com/story/2013/03/colorado-governor-john-hickenlooper-gun-control-bills-089127.

299. Candice Norwood, Chloe Jones & Lizz Bolaji, *More Black Women Are Being Elected to Office. Few Feel Safe Once They Get There*, PBS NEWS HOUR (June 17, 2021), https://www.pbs.org/newshour/politics/more-black-women-are-being-elected-to-office-few-feel-safe-once-they-get-there.

a gun," alluding to the attempted assassination of former Representative Gabby Giffords, who was shot and nearly killed in Tucson, Arizona.[300]

Threatening people's safety through online harassment dates back to the early days of the internet.[301] It includes a range of behaviors, such as: sexist, racist, homophobic, and ableist name calling; releasing nonconsensual intimate imagery; rape or death threats; doxxing;[302] hacking; and much more.[303] It can be a one-off message or a coordinated attack.[304] It can be shared directly or tweeted into the ether. And it is alarmingly common. Of all American internet users, nearly one in four report experiencing online harassment.[305] But harassment does not affect internet users equally.

As journalist Amanda Hess recounted in *Why Women Aren't Welcome on the Internet*, women are likely to report being harassed on the internet.[306] Women of color—including Black, Asian, Latine/Latinx, and mixed-race women—are also 34% more likely to be mentioned in abusive or problematic tweets than White women, with Black women being overwhelmingly targeted for

300. *Id.* The author of the missive was charged with harassment but, in a stunning rejection of carceral feminism, Fields requested that the case be dismissed after he agreed to a permanent restraining order. *Id.*

301. *See, e.g.*, Julian Dibbel, *A Rape in Cyberspace*, VILLAGE VOICE (Oct. 18, 2005), https://www.villagevoice.com/2005/10/18/a-rape-in-cyberspace/ (iconically recounting graphic online harassment, amounting to a rape, within a LambdaMOO community). Definitionally, this Article discusses harassment as a social phenomenon that, in some circumstances, has legal consequences rather than hewing to the legal definition of harassment. This is because legal harassment generally requires direct communication with a victim in a way that is likely to cause annoyance or alarm, but not all actions amounting to social online harassment satisfies that legal definition. Amanda Levendowski, *Using Copyright*, *supra* note 90.

302. "Doxxing" exposes victims' personal information, such as home addresses and jobs. It is common for victims of nonconsensual intimate imagery distribution.

303. Maeve Duggan, *Part 4: The Aftermath of Online Harassment*, PEW RSCH. CTR. (Oct. 22, 2014), https://www.pewresearch.org/internet/2014/10/22/part-4-the-aftermath-of-online-harassment/.

304. Danielle Keats Citron, *Addressing Cyber Harassment: An Overview of Hate Crimes in Cyberspace*, 6 CASE W. RES. J.L. TECH. & INTERNET 1 (2015) (recounting the GamerGate harassment campaign).

305. Emily A. Vogels, *Roughly Four-in-Ten Americans Have Experienced Online Harassment, With Half This Group Citing Politics as the Reason They Think They Were Targeted. Growing Shares Face More Severe Online Abuse Such as Sexual Harassment or Stalking*, PEW RSCH. CTR. (Jan. 13, 2021), https://www.pewresearch.org/internet/2021/01/13/the-state-of-online-harassment/.

306. Amanda Hess, *Why Women Aren't Welcome on the Internet*, PAC. STANDARD (June 14, 2017), https://psmag.com/social-justice/women-arent-welcome-internet-72170 (recounting her own invasive online harassment and contextualizing it broadly to all women online). Men also experience harassment online, though it is less related to their gender. Vogels, *Online Harassment*, *supra* note 305.

harassment.[307] While percentages of people victimized by online harassment do not seem to be growing, it is becoming more severe.[308]

For a time, "online" was perceived to be distinct from "offline."[309] That fantasy is disrupted when online harassment fuels offline consequences. Victims of online harassment report harmful, detrimental offline consequences to their mental health, including depression, anxiety, suicidal ideation, and panic attacks.[310] Online harassment like doxxing puts victims at risk of strangers showing up to their homes or workplaces.[311] Other harassment techniques popular in online communities, such as calling law enforcement with erroneous reports likely to attract SWAT teams, known as "swatting," can even be deadly.[312]

No matter the form, online harassment threatens the offline safety of its recipients irrevocably.[313] This Part uses safety to examine how governing harassment in cyberspace plays out across privacy and the Computer Fraud

307. Hess, *'supra* note 306. Fields' position attracts acute toxicity: among Black women politicians and journalists alone, roughly one in ten tweets mentioning them was abusive or problematic. *See* Amnesty International & Element AI, *Troll Patrol Findings: Using Crowdsourcing, Data Science & Machine Learning to Measure Violence and Abuse Against Women on Twitter*, AMNESTY INT'L (2017), https://decoders.amnesty.org/projects/troll-patrol/findings.

308. Sophie Bertazzo, *Online Harassment Isn't Growing—But It's Getting More Severe*, PEW RSCH. CTR. (June 28, 2021), https://www.pewtrusts.org/en/trust/archive/spring-2021/online-harassment-isnt-growing-but-its-getting-more-severe. For a deeper dive into online harassment, see DANIELLE CITRON, HATE CRIMES IN CYBERSPACE (2014).

309. *See* Mark A. Lemley, *Place and Cyberspace*, 91 CALIF. L. REV. 521 (2003) (responding to Dan Hunter, *Cyberspace as Place at the Tragedy of the Anticommons*, 91 CALIF. L. REV. 439 (2003)); *cf.* Julie E. Cohen, *Cyberspace as/and Space*, 107 COLUM. L. REV. 210 (2007).

310. Francesca Stevens, Jason R.C. Nurse, Budi Arief, *Cyber Stalking, Cyber Harassment, and Adult Mental Health: A Systemic Review*, 24 CYBERPSYCHOLOGY BEHAV. SOC. NETW. 367 (2021).

311. CARRIE GOLDBERG, NOBODY'S VICTIM: FIGHTING HARASSMENT ONLINE & OFF (2019); *see also* Nathan Mattise, *Anti-Doxing Strategy—or, How to Avoid 50 Qurans and $287 of Chick-Fil-A*, ARS TECHNICA (Mar. 15, 2015), https://arstechnica.com/information-technology/2015/03/anti-doxing-strategy-or-how-to-avoid-50-qurans-and-287-of-chick-fil-a/ (offering strategies to avoid doxxing after being a target).

312. *See, e.g.*, Michael Brice-Saddler, Avi Selk & Eli Rosenberg, *Prankster Sentenced to 20 Years for Fake 911 Call That Led Police to Kill an Innocent* Man, WASH. POST (Mar. 29, 2019), https://www.washingtonpost.com/nation/2019/03/29/prankster-sentenced-years-fake-call-that-led-police-kill-an-innocent-man/; Maria Cramer, *A Grandfather Died in 'Swatting' Over His Twitter Handle, Officials Say*, N.Y. TIMES (July 24, 2021), https://www.nytimes.com/2021/07/24/us/mark-herring-swatting-tennessee.html. For a feminist account of swatting, see Caroline Sinders, *That Time the Internet Sent a SWAT Team to My Mom's House*, BOINGBOING (July 24, 2015), https://boingboing.net/2015/07/24/that-time-the-internet-sent-a.html. Bills have been introduced to criminalize swatting. *See* Preserving Safe Communities by Ending Swatting Act, H.R. 4523 (117th Congress 2021-2022).

313. Amanda Hess, *Why Women Aren't Welcome on the Internet*, PAC. STANDARD (June 14, 2017), https://psmag.com/social-justice/women-arent-welcome-internet-72170.

and Abuse Act, the federal anti-hacking law. Section IV.A unpacks how longtime surveillance practices will be weaponized to invade the privacy of abortion providers and pregnant people after the Supreme Court's recent overruling of *Roe v. Wade*. Information collected by search engines, technology companies, and data brokers can and will be used by anti-abortion activists and law enforcement to threaten the safety of people needing abortions or experiencing miscarriages—in some cases, it's already happening. Under another law, however, technological harassment is criminally prosecuted, albeit with spotty success. Section IV.B looks at several high-profile prosecutions under the Computer Fraud and Abuse Act to expose an unexplored common thread: prosecutors targeting people using technology to threaten the safety of girls and women. Both issues illustrate the influence of safety on cyberlaw, and feminist cyberlaw offers a way to weave the two together.

A. INVADING PRIVACY WITH SURVEILLANCE TECHNOLOGIES

Internet harassment can be well-organized and alarmingly effective. In the mid-1990s, the American Coalition of Life Activists (ACLA) launched a website called the Nuremburg Files featuring wanted-style posters of abortion providers and supporters claiming their behavior amounted to "crimes against humanity."[314] The site doxxed doctors and clinic staff by publicly posting their names, photographs, home addresses, and even family details.[315] The ACLA also launched a so-called Deadly Dozen poster targeting a handful of physicians.[316] When physicians were injured, their names were greyed out; murdered physicians' names were stricken through.[317] When targeted providers sued the ACLA, the jury viewed the harassing website as a hitlist that violated the Freedom of Access to Clinic Entrances (FACE) Act, which was enacted to protect abortion seekers and allies from physical obstruction, intimidation, and interference with abortion rights.[318] That jury awarded $120.8 million in actual and punitive damages, one of the largest verdicts in any online harassment case.[319]

314. Planned Parenthood of the Columbia/Willamette, Inc. v. Am. Coal. of Life Activists, 290 F.3d 1058, 1080 (9th Cir. 2002), *on remand*, 300 F. Supp. 2d 1055 (D. Or. 2004).

315. Planned Parenthood of the Columbia/Willamette, Inc. v. Am. Coal. of Life Activists, 41 F. Supp. 2d 1130, 1134–52 (D. Oregon 1999), *rev'd* 244 F.3d 1007 (9th Cir. 2001), *reinstated*, 290 F.3d 1058, 1080 (9th Cir. 2002), *on remand*, 300 F. Supp. 2d 1055 (D. Or. 2004).

316. *Id.*

317. *Planned Parenthood of the Columbia/Willamette, Inc.*, 290 F.3d at 1065.

318. 18 U.S.C. § 248(a). Wild to think such a law could get passed a few decades ago.

319. Planned Parenthood of the Columbia/Willamette, Inc. v. Am. Coal. of Life Activists, 518 F.3d 1013, 1016 (9th Cir. 2008). The Ninth Circuit reduced punitive damages to $4.7 million. *Id.*

It was cold comfort. After the website's creation, two abortion doctors were murdered in their homes.[320] An abortion clinic was bombed.[321] Another doctor was killed by a sniper.[322] Immediately after, the site struck through the deceased doctor's name.[323]

The right to an abortion was previously underpinned by privacy.[324] In *Roe v. Wade*, Justice Blackmun recognized women's constitutional right to decisional privacy when choosing abortion, explaining that "the Court has recognized that a right of personal privacy, or a guarantee of certain areas or zones of privacy, does exist under the Constitution," despite privacy not being "explicitly mention[ed]."[325]

Privacy was once in the first category of "cyberlaws," as a general law that was successfully appropriated for feminist goals in cyberspace, but that is no longer sustainable without meaningful legislative intervention. But that privacy right exists no longer in the eyes of the Supreme Court—its recent decision in *Dobbs v. Jackson Women's Health Organization* eradicated it.[326] Absent comprehensive privacy legislation, privacy falls into the second category of cyberlaws. Instead, privacy is presently relegated to the second category of cyberlaws that cannot be appropriated for feminist goals, such as reproductive justice.

---

320. Danielle Keats Citron, *Mainstreaming Privacy Torts*, 98 CALIF. L. REV. 1805, 1817 (2010) (citing DANIEL SOLOVE, THE FUTURE OF REPUTATION: GOSSIP, RUMOR, AND PRIVACY ON THE INTERNET (2007)).

321. *Id.*

322. *Id.*

323. *Id.*

324. *See* Roe v. Wade, 410 U.S. 113 (1973). Not all feminists embrace abortion as a pregnant person's right, particularly conservative feminists. While those arguments are beyond the scope of this Article, a deeper dive into those discussions can be found in Victoria Baranetsky, *Aborting Dignity: The Abortion Doctrine After* Gonzales v. Carhart, 36 HARV. J. L. & GENDER 123, 170 n.156 (2013).

325. *Roe*, 410 U.S. at 152. Other key sources of privacy rights are sourced to an unusual source: law review articles. *See* Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890); William Prosser, *Privacy*, 48 CALIF. L. REV. 383 (1960). The Court's subsequent decision in *Casey* centered on grounding the right to an abortion in the Fourteenth Amendment's due process clause, though privacy remained an important component. Planned Parenthood of Se. Penn. v. Casey, 505 U.S. 833, 846, 915 ("Constitutional protection of a women's decision to terminate her pregnancy derives from the Due Process Clause of the Fourteenth Amendment . . . The woman's constitutional liberty interest also involves her freedom to decide matter of the highest privacy and the most personal nature.").

326. Dobbs v. Jackson Women's Health Org., 142 S. Ct. 2228 (2022) (overturning Roe v. Wade, 410 U.S. 113 (1973)). *Dobbs* also put defending the right to use contraception, engage in "private, consensual sexual acts," and "marry a person of the same sex," under the microscope for potential reversal. *Id.* at 2258.

In *Dobbs*, Justice Alito claimed that the Court was compelled to overrule *Roe* and its successor, *Planned Parenthood v. Casey*, because "[t]he Constitution," a document written entirely by men who could not become pregnant, "makes no reference to abortion . . . and no such right is implicitly protected by any constitutional provision."[327] Post-*Dobbs*, abortion became entirely or near entirely banned in thirteen states.[328] It is strictly limited in many others.[329] And these laws may extend to people experiencing miscarriages, who will be caught up in the prosecutorial fervor.[330]

But *Dobbs* is not a complete throwback to the 1970s. Back then, law enforcement largely relied on human-driven intelligence and physical surveillance to invade the privacy of people needing abortions.[331] Today, the government—and, in some instances, abortion activists—also benefit from the tireless assistance of what Shoshana Zuboff calls "surveillance capitalism," meaning "the unilateral claiming of private human experience as free raw material for translation into behavioral data."[332] Pregnant people's attempts at gathering information now involve search engines, technology companies, and data brokers, each of which can provide pregnant people's information to law enforcement or, in some instances, anti-abortion activists.

Sharing and selling sensitive data is not new. The present information privacy crisis for abortion providers and pregnant people was predictable—and preventable.[333] But the specific ways that abortion-related data will be

327. *Id.* at 2242; Planned Parenthood of Se. Pa. v. Casey, 505 U.S. 833 (1992).

328. *Abortion Policy in the Absence of* Roe*,* GUTTMACHER INST. (July 1, 2022), https://www.guttmacher.org/state-policy/explore/abortion-policy-absence-roe.

329. *Id.*

330. Between 1973 and 2005, sixty-eight women were investigated for crimes related to their own pregnancies. Gabriela Weigel, Laurie Sobel & Alina Salganicoff, *Criminalizing Pregnancy Loss and Jeopardizing Care: The Unintended Consequences of Abortion Restrictions and Fetal Harm Legislation*, 30-3 WOMEN'S HEALTH ISSUES 143 (2020); *see also* Robin Levinson-King, *US Women Are Being Jailed for Having Miscarriages*, BBC (Nov. 12, 2021), https://www.bbc.com/news/world-us-canada-59214544. Enforcement of these laws will have a disproportionate impact on women of color and poor women. Priscilla Thompson & Alexandra Turcios Cruz, *How an Oklahoma Woman's [sic] Miscarriage Put a Spotlight on Racial Disparities in Prosecutions*, NBC NEWS (Nov. 5, 2021), https://www.nbcnews.com/news/us-news/woman-prosecuted-miscarriage-highlights-racial-disparity-similar-cases-rcna4583.

331. *See generally* THE JANES (2022).

332. John Laidler, *High Tech Is Watching You*, HARV. GAZETTE (Mar. 4, 2019), https://news.harvard.edu/gazette/story/2019/03/harvard-professor-says-surveillance-capitalism-is-undermining-democracy/ (interviewing Shoshanna Zuboff). For a deeper dive into surveillance capitalism, see SHOSHANNA ZUBOFF, THE AGE OF SURVEILLANCE CAPITALISM: THE FIGHT FOR A HUMAN FUTURE AT A NEW FRONTIER OF POWER (2019).

333. *See, e.g.*, Paul M. Schwartz, *Privacy and Democracy in Cyberspace,* 52 VAND. L. REV. 1609 (1999) (describing information privacy online as a "horror show"); Paul Ohm, *Broken Promises of Privacy: Responding to the Surprising Failure of Anonymization*, 57 UCLA L. REV. 1701 (2010)

weaponized to harass abortion providers, seekers, and people experiencing miscarriages remains uniquely invasive.

When it comes to law enforcement investigations of abortions and miscarriages, Cynthia Conti-Cook cautioned that "[t]he most harmful type of digital evidence is online search browsing history."[334] Even before *Dobbs*, she was proven right. In 2018, a Black mother named Latice Fisher was harassed by law enforcement and jailed for two years after her miscarriage.[335] Evidence "against her" included her Google searches for abortion pills.[336] In Fisher's case, she voluntarily gave law enforcement access to her phone.[337] That technique does not scale.[338] But law enforcement has a tool that does: keyword warrants.

Close cousins to geofence warrants, which request geolocation data for devices within a particular radius,[339] keyword warrants enable law enforcement

(rejecting so-called anonymization as a sufficient fix for privacy invasive practices); JULIE COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE 267 (2012) (arguing that "meaningful reform in information law and information policy requires a deep and fundamental rethinking of the most basic assumptions on which they are founded," which did not occur in intervening years); Cynthia Conti-Cook, *Surveilling the Digital Abortion Diary*, 50 U. BALT. L. REV. 1 (2020) (detailing the ways pregnant people can be surveilled digitally); Elizabeth Joh, *The Potential Overturn of* Roe *Shows Why We Need More Digital Privacy Protections*, SLATE (May 9, 2022), https://slate.com/technology/2022/05/roe-overturn-data-privacy-laws.html (advocating for privacy-protective laws in advance of *Roe*'s reversal); *cf.* Neil M. Richards, *The Information Privacy Law Project*, 94 GEO. L. REV. 1087 (2006) (reviewing DANIEL SOLOVE, THE DIGITAL PERSON: PRIVACY AND TECHNOLOGY IN THE INFORMATION AGE (2004) and highlighting select scholars' focus on information privacy exclusive of decisional privacy); Ann Bartow, *A Feeling of Unease About Privacy Law*, 155 U. PA. L. REV. 52 (2006) (critiquing Daniel J. Solve, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477 (2006) for focusing on information privacy exclusive of decisional privacy, specifically abortion rights). For a deeper dive into abortion rights as privacy rights, see Anita L. Allen, *The Proposed Equal Protection Fix for Abortion Law: Reflections on Citizenship, Gender, and the Constitution*, 18 HARV. J.L. & PUB. POL'Y 419 (1995).

334. Lauren Rankin, *How an Online Search for Abortion Pills Landed This Woman in Jail*, FAST CO. (Feb. 26, 2020), https://www.fastcompany.com/90468030/how-an-online-search-for-abortion-pills-landed-this-woman-in-jail.

335. *Id.* She was accused of second-degree murder.

336. *Id.*

337. *Id.*

338. As of 2019, high-end estimates pin the number of legalized U.S. abortions at 920,000 per year, Jeff Diamant & Besheer Mohamed, *What the Data Says About Abortion in the U.S.*, PEW RSCH. CTR. (June 24, 2022) (synthesizing data from the Center for Disease Control and Guttmacher Institute, both of which are subject to caveats and limitations), https://www.pewresearch.org/fact-tank/2022/06/24/what-the-data-says-about-abortion-in-the-u-s-2/.

339. Geofence warrants were used to investigate the Capital Riots. Mark Harris, *How a Secret Google Geofence Warrant Helped Catch the Capitol Riot Mob*, WIRED (Sept. 30, 2021), https://www.wired.com/story/capitol-riot-google-geofence-warrant/. Geofencing more generally

to request sensitive information, such as all Google accounts and IP addresses of people who ran searches for certain keywords, such as "abortion pills," "abortion clinic," or even "Planned Parenthood," over a period of time.[340] Only a few such warrants are public presently—most are sealed or presumed sealed—but their use will grow as law enforcement realizes that can deploy a legal dragnet to invade pregnant people's privacy, which may also set those people up for harassment.[341]

Other technology companies collect equally sensitive information. Facebook, for example, already stores data that can get abortion seekers harassed, prosecuted, or both.[342] Facebook messages are not encrypted by default, which means they can often be freely and easily handed over to law enforcement—and that is exactly what happened to a mother and her teen daughter who are being prosecuted for allegedly self-administering the

has been weaponized against abortion clinics already, with one organization using it target people visiting clinics with messages like "You Have Choices." Nate Raymond, *Firm Settles Massachusetts Probe Over Anti-Abortion Ads Sent to Phones*, REUTERS (Apr. 4, 2017), https://www.reuters.com/article/massachusetts-abortion/firm-settles-massachusetts-probe-over-anti-abortion-ads-sent-to-phones-idUSL2N1HC04K.

340. Thomas Brewster, *Exclusive: Government Secretly Orders Google to Identify Anyone Who Searched a Sexual Assault Victim's Name, Address or Telephone Number*, FORBES (Oct. 4, 2021), https://www.forbes.com/sites/thomasbrewster/2021/10/04/google-keyword-warrants-give-us-government-data-on-search-users/.

341. Jessica Schladebeck, *Feds Issue Secret 'Keyword Warrants' for Google Search History*, GOV'T TECH. (Oct. 7, 2021), https://www.govtech.com/security/feds-issue-secret-keyword-warrants-for-google-search-history. Hoping for resistance from Google appears to be a lost cause. Naomi Gilens, Jennifer Lynch & Veridiana Alimonti, *Google Fights Dragnet Warrant for Users' Search Histories Overseas While Continuing to Give Data to Police in the U.S.*, ELEC. FRONTIER FOUND. (Apr. 5, 2022), https://www.eff.org/deeplinks/2022/04/google-fights-dragnet-warrant-users-search-histories-overseas-while-continuing. Using search engine data as evidence is not the only way it can be weaponized. Anti-abortion organizations use Google ads to harass pregnant people with pro-life messages when they try to search for abortion services. Emma Cott, Nilo Tabrizy, Aliza Aufrichtig, Rebecca Lieberman & Nailah Morgan, *They Search Online for Abortion Clinics. They Found Anti-Abortion Centers*, N.Y. TIMES (2022), https://www.nytimes.com/interactive/2022/us/texas-abortion-human-coalition.html.

342. Grace Oldham & Dhruv Mehrotra, *Facebook and Anti-Abortion Clinics are Collecting Highly Sensitive Info on Would-Be Patients*, MARKUP (June 15, 2022), https://themarkup.org/pixel-hunt/2022/06/15/facebook-and-anti-abortion-clinics-are-collecting-highly-sensitive-info-on-would-be-patients. Privacy invasions resulting in harassment are baked into Facebook's origin story. Never forget that Mark Zuckerberg's first foray into social media was Facemash, which let users rank the hotness of scraped photographs of his Harvard classmates—and which the Fuerza Latina and Association of Black Women both blasted. Katharine A. Kaplan, *Facemash Creator Survives Ad Board*, HARV. CRIMSON (Nov. 19, 2003), https://www.thecrimson.com/article/2003/11/19/facemash-creator-survives-ad-board-the/.

daughter's abortion.[343] But there are even more surreptitious ways for Facebook to aid surveillance.

Despite the platform's prohibition on sites and apps using Facebook advertising technology that send the company "sexual and reproductive health data,"[344] an investigation by Grace Oldham and Dhruv Mehortra revealed that hundreds of anti-abortion clinics use a piece of Facebook's code called a tracking pixel.[345] The pixel lets those sites capture sensitive information, including appointments for "abortion consultation" or "pre-termination screening," alongside schedulers' names, emails, or phone numbers.[346] Those details are then shared with Facebook.[347] As a result, the company retains a treasure trove of data about who is making, or attempting to make, abortion-related appointments and where those appointments are located.[348]

Unlike technology companies, data brokers aren't just in the business of hoarding data—they're in the business of selling it. One particularly popular type of sellable data is location data. As the Supreme Court has recognized, location data can reveal the most sensitive information about people, including who's attending church, sleeping at a lover's apartment, or visiting an abortion clinic.[349] There was a market for the that data even before *Dobbs*. One company called SafeGraph obtains location data from apps and resells it.[350] The company claims to track granular information about how often people visit a location, how long they stay there, where else they go, and—most alarmingly—where they live, down to a census block level.[351] Perhaps spotting an opportunity, the company already marked "Planned Parenthood" as a

343. Albert Fox Cahn, *Facebook's Message Encryption Was Built to Fail*, WIRED (Aug. 10, 2022), https://www.wired.com/story/facebook-message-encryption-abortion/.

344. *About Sensitive Health Information*, META (2022), https://www.facebook.com/business/help/361948878201809?id=188852726110565.

345. Oldham & Mehrotra, *supra* note 342.

346. *Id.*

347. *Id.*

348. *Id.*

349. United States v. Carpenter, 585 U.S. ___ at 18 (2018). Exposure of abortion clinic location data is, unfortunately, not a new problem. Jennifer Valentino-DeVries, Natasha Singer, Michael H. Keller & Aaron Krolik, *Your Apps Know Where You Were Last Night, and They're Not Keeping It a Secret*, N.Y. TIMES (Dec. 10, 2018), https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html.

350. Joseph Cox, *Data Broker Is Selling Location Data of People Who Visit Abortion Clinics*, VICE (May 3, 2022), https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood. Alarmingly, it's not alone. Jon Keegan, *Planned Parenthood Data Found on Another Location Data Dashboard*, MARKUP (July 15, 2022), https://themarkup.org/privacy/2022/07/15/planned-parenthood-data-found-on-another-location-data-dashboard.

351. *Id.*

trackable "brand" and sold data on more than six hundred Planned Parenthood locations, some of which provide abortion services.[352]

These sensitive disclosures can fuel harassment by anti-abortion activists and law enforcement alike. Search engine data can replicate, or even amplify, harassment like that experienced by Latice Fisher, both by targeting people who have abortions and people who did not obtain one. Anti-abortion clinics can masquerade as abortion providers to collect information about would-be patients and feed that data back to technology companies. Or activists and law enforcement can simply purchase providers' and seekers' location data.[353] These routes lead to a long road of potential harassment, from mailing or emailing targets harassing anti-abortion messages such as "BABY MURDERER," or pummeling them with harmful misinformation about abortion procedures. Other techniques, like doxxing, continuing ACLA's campaign by creating hitlists, or increasing abortion providers' and pregnant peoples' contact with law enforcement, can pose serious threats to people's safety.

Post-*Dobbs* surveillance will not be felt equally. Black and low-income pregnant people are already disproportionately surveilled.[354] People of color are more likely to have pregnancy complications, such as ectopic pregnancies.[355] And Black people miscarry at higher rates.[356] Together, these realities increase the likelihood of contact between pregnant people of color, low-income pregnant people, and law enforcement. That contact can be dangerous. Once investigated by law enforcement, pregnant low-income

352. *Id.* SafeGraph has said it will stop selling such sensitive data. Joseph Cox, *Data Broker SafeGraph Stops Selling Location Data of People Who Visit Planned Parenthood*, VICE (May 4, 2022), https://www.vice.com/en/article/88gyn5/data-broker-safegraph-stops-selling-location-data-of-people-who-visit-planned-parenthood. Other data brokers are still stepping up.

353. Sharon Bradford Franklin, Greg Nojeim & Dhanaraj Thakur, *Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence Agencies Are Buying Your Data From Brokers*, CTR. FOR DEMOCRACY & TECH. (Dec. 2021), https://cdt.org/wp-content/uploads/2021/12/2021-12-08-Legal-Loopholes-and-Data-for-Dollars-Report-final.pdf.

354. Lynn M. Paltrow & Jeanne Flavin, *Arrests of and Forced Interventions on Pregnant Women in the United States, 1973-2005: Implications for Women's Legal Status and Public Health*, 38 J. HEALTH POL. POL'Y L. 299, 333 (2013).

355. Debra B. Stulberg, Loretta R. Cain, Irma Dahlquist & Diane Lauderdale, *Ectopic Pregnancy Rates and Racial Disparities in the Medicaid Population, 2004-08*, 102 FERTILITY & STERILITY 1671, 1674 (2014). This research does not address trans women, but this Article uses inclusive language.

356. Sudeshna Mukherjee, Digna R. Velez Edwards, Donna D. Baird, David A. Savitz & Katherine E. Hartmann, *Risk of Miscarriage Among Black Women and White Women in a US Prospective Cohort Study*, 177 AM. J. EPIDEMIOLOGY 1271 (2013).

people and people of color, especially Black people, are more likely to be arrested or otherwise deprived of liberty.[357]

Abortion seekers face a dilemma: disclose private information that makes abortion attainable and risk its weaponization, or deprive oneself of crucial information that could make a life-changing decision easier.[358] Legally, these technological entities owe users limited duties to protect their privacy.[359] But that does not always align with people's perceptions. Radical feminists may not want those expectations to be realigned entirely.[360] Invasive surveillance techniques threaten the safety of abortion providers and pregnant people, but they can also be deployed to investigate misogynistic crimes that some feminists consider more worthy of prosecution, such as intimate partner violence.[361] However, barring legislative intervention regulating these techniques, abortion providers, abortion seekers, and people experiencing

357. Paltrow & Flavin, *supra* note 354, at 322.

358. Helen Nissenbaum's theory of contextual integrity explains why people are willing to disclose information in some circumstances or to some people but not others. Helen Nissenbaum, *Privacy as Contextual Integrity*, 79 WASH. L. REV. 119 (2004), https://core.ac.uk/download/pdf/267979739.pdf. Margot Kaminski's conceptualization of "boundary management," adapted from social psychologist Irwin Altman, also offers a useful framework for understanding privacy harms. Margot E. Kaminski, *Regulating Real-World Surveillance*, 9 WASH. L. REV. 1113 (2015).

359. Some scholars think those duties should be more robust. *See, e.g.*, Jack M. Balkin, Information Fiduciaries and the First Amendment, 49 U.C. DAVIS L. REV. 1183 (2016); ARI EZRA WALDMAN, PRIVACY AS TRUST: INFORMATION PRIVACY FOR AN INFORMATION AGE (2018); Lindsey Barrett, Confiding in Con Men: U.S. Privacy Law, the GDPR, and Information Fiduciaries, 42 SEATTLE U. L. REV. 1057, 1058 (2019); Lauren Henry Scholz, *Fiduciary Boilerplate: Locating Fiduciary Relationships in Information Age Consumer Transactions*, J. CORP. L. 144, 144 (2020); Neil M. Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. 961 (2021). The idea of corporations as "information fiduciaries" is not universally popular; *cf.* Lina M. Khan & David E. Pozen, *A Skeptical View of Information Fiduciaries*, 133 HARV. L. REV. 497 (2019).

360. Radical feminism played a powerful role in shifting and reshaping the discourse around intimate partner violence. For a deeper dive into the role of radical feminism in criminalizing intimate partner violence, see Carolyn Hoyle, *Feminism, Victimology and Domestic Violence*, *in* HANDBOOK OF VICTIMS AND VICTIMOLOGY 165 (Sandra Walklate ed., Willan Publishing 2007) ("Feminism, particularly radical feminism, has done more to help those harmed by domestic violence than any other movement. It was essential in altering policymakers and practitioners to the physical and emotional abuse that occurs within families.").

361. Internet search information was famously invoked in Scott Peterson's murder of Laci Peterson, his pregnant wife. *Peterson Compute Shows Internet Searches on Boat Launches*, BAY CITY NEWS (Aug. 4, 2004), https://www.sfgate.com/news/article/Peterson-computer-shows-internet-searches-on-boat-2703609.php. Sensitive data has factored into multiple murders of wives by their husbands. *See, e.g.*, Jack Morse, *He Said He Was Asleep at Time of Wife's Murder. His Health App Said Otherwise*, MASHABLE (Feb. 9, 2021), https://mashable.com/article/smartphone-health-app-data-police.

miscarriages have limited legal means of invoking privacy to protect themselves.[362]

B. HACKING UNDER THE COMPUTER FRAUD AND ABUSE ACT

Not all harassment is preventable with better tools or methods. In 2010, Hunter Moore launched the website isanyoneup.com to solicit and distribute nonconsensual intimate images, mostly of women.[363] Alongside their photographs, Moore doxxed victims by including their full names, jobs, social media profiles, and cities of residence, all but ensuring the images would show up in Google Search results.[364] Moore quickly established himself as the most hated man on the internet. He responded to desperate cease-and-desist letters with "LOL."[365] He described himself as a "professional life ruiner."[366] He reported having no trouble sleeping at night.[367] Until the FBI arrested him for obtaining dozens of nudes by hacking email accounts, which violates the only criminal law inspired by the Matthew Broderick film War Games.[368]

362. Congressional inaction is not for lack of trying. Daniel J. Solove, *A Brief History of Information Privacy, in* PROSKAUER ON PRIVACY (PLI 2006); Anupam Chander, Margot Kaminski & William McGeveran, *Catalyzing Privacy Law*, 105 MINN. L. REV. 1733, 1769–76 (2021) (discussing state and local privacy developments absent a comprehensive federal privacy law). And on June 15, 2022, Senator Elizabeth Warren introduced the Health and Location Data Protection Act, which could curb some of these privacy-invasive practices. S. 4408 (117th Cong. 2022). For a critical take on privacy legislation drafting, see Julie E. Cohen, *How (Not) To Write A Privacy Law*, KNIGHT KNIGHT FIRST AMENDMENT INST. (Mar. 23, 2021), https://knightcolumbia.org/content/how-not-to-write-a-privacy-law.

363. Alex Morris, *Hunter Moore: The Most Hated Man on the Internet*, ROLLING STONE (Nov. 13, 2012), https://www.rollingstone.com/culture/culture-news/hunter-moore-the-most-hated-man-on-the-internet-184668/.

364. *Id.* With the CFAA, the feminist values of consent and safety intersect.

365. *Id.* at 3. Moore invoked the provisions of CDA § 230 to protect himself from liability (though it was later revealed that he created some of the content himself). *Id.*

366. Carole Cadwalladr, *Charlotte Laws' Fight with Hunter Moore, the Internet's Revenge Porn King*, GUARDIAN (Mar. 30, 2014), https://www.theguardian.com/culture/2014/mar/30/charlotte-laws-fight-with-internet-revenge-porn-king.

367. Alex Morris, *Hunter Moore: The Most Hated Man on the Internet*, ROLLING STONE (Nov. 13, 2012), https://www.rollingstone.com/culture/culture-news/hunter-moore-the-most-hated-man-on-the-internet-184668/.

368. United States v. Moore, Indictment, No. 2:13-CR-00917 (C.D. Cal. 2013), https://www.wired.com/images_blogs/threatlevel/2014/01/revenge-porn-Moore-Evens-indictment.pdf; WARGAMES (1983). It is not the only Broderick film with legal consequences, however—*Project X* led to the invocation of animal abuse laws. Deborah Caulfield, *New Charges of Animal Abuse in 'Project X': D.A. Office Asked to File Criminal Complaints*, L.A. TIMES (Nov. 2, 1987), https://www.latimes.com/archives/la-xpm-1987-11-02-ca-12056-story.html. This section riffs on my prior discussion of the CFAA in Amanda Levendowski, *Teaching Doctrine for Justice Readiness*, 29 CLINICAL L. REV. 1 (forthcoming 2022).

As a refresher, Broderick circa 1983 plays a teen hacker who accidentally hacks a military supercomputer.[369] Several members of Congress embraced the view that the film was a "realistic representation of the automatic dialing and access capabilities of the personal computer" and responded by enacting what became the Computer Fraud and Abuse Act (CFAA).[370] The CFAA penalizes, in its broadest provision, "intentionally access[ing] a computer without authorization or exceed[ing] authorization, and thereby obtain[ing] information from any protected computer."[371] Because a protected computer includes any computer "used in or affecting interstate or foreign commerce or communication," the CFAA effectively applies to any device connected to the internet.[372] The CFAA falls within the second category of cyberlaws, as it's a cyberlaw that cannot—despite prosecutorial attempts to the contrary—be appropriated for feminist goals of mitigating misogynistic harassment. Ironically, however, a narrow reading of the CFAA that permits certain types of harassment also paves the way for pursuing the feminist goals of investigating employment discrimination and corporate malfeasance.

In its early years, prosecutors used the CFAA to target various forms of hacking.[373] But invocation of the CFAA as a straightforward hacking law did not last.[374] In the thirty-seven years since the CFAA's enactment, a deep, contentious split developed between the circuits that restricted the CFAA to hacking and interpreted its provisions narrowly[375] and the others that significantly expanded its scope.[376] In those latter jurisdictions, common uses

369. WARGAMES (1983). The film was nominated for three Academy Awards. *The 56th Academy Awards*, OSCAR (Apr. 9, 1984), https://www.oscars.org/oscars/ceremonies/1984.

370. H.R. REP. NO. 98-894, at 6 (1984).

371. 18 U.S.C. § 1030(a)(2)(C). Technically, the law was enacted as the Comprehensive Crime Control Act and expanded into the CFAA two years later. Orin Kerr, *Vagueness Challenges to the Computer Fraud and Abuse Act*, 94 MINN. L. REV. 1561, 1563–64 (2010).

372. 18 U.S.C. § 1030(e)(2).; *See, e.g.*, United States v. Drew, 259 F.R.D. 449, 457 (C.D. Cal. 2009) (noting that the final elements of 18 U.S.C. § 1030(a)(2)(C) "will always be met when an individual using a computer contacts or communicates with an Internet website").

373. *See, e.g.*, United States v. Morris, 928 F.2d 504 (2d Cir. 1991) (prosecuting hacker who released the eponymous Morris worm).

374. *See, e.g.*, United States v. Drew, 259 F.R.D. 449 (C.D. Cal. 2009) (invoking the CFAA to prosecute cyberbullying).

375. WEC Caroline Energy Sols. LLC v. Miller, 687 F.3d 199, 207 (4th Cir. 2012), United States v. Nosal, 676 F.3d 854, 852–63 (9th Cir. 2012), United States v. Valle, 807 F.3d 508, 528 (2d Cir. 2015). For an in-depth account of the so-called "narrow interpretation," see Jonathan Mayer, *The "Narrow" Interpretation of the Computer Fraud and Abuse Act: A User Guide for Applying United States v. Nosal*, 84 GEO. WASH. L. REV. 1655 (2016).

376. EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 583–84 (1st Cir. 2001); Int'l Airport Ctrs., L.L.C. v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006); United States v. John, 597 F.3d 263, 272 (5th Cir. 2010); Brown Jordan Int'l, Inc. v. Carmicle, 846 F.3d 1167, 1174–75 (11th Cir. 2017), *all abrogated by* Van Buren v. United States, 940 F.3d 1192 (11th Cir. 2019).

of the internet—such as lying in social media profiles,[377] sharing passwords for streaming services,[378] and even scraping websites[379]—could amount to CFAA violations. The law later garnered national attention for its breadth after the death of internet activist Aaron Swartz, who was prosecuted under the law.[380]

Several scholars have written about the scope of the CFAA.[381] But existing work overlooks an unexplored trend among high-profile CFAA cases: prosecutors stretching the CFAA to tackle technology-fueled harassment targeting girls and women. Moore's harassment happened to involve the kind of hacking squarely in the CFAA's crosshairs, but the harassing behaviors of suburban mothers, law enforcement officers, and police sergeants were less so. Prosecutors brought CFAA charges against each of those people anyway. And they failed.

When Lorri Drew created a Myspace profile in 2006, it wasn't for herself.[382] She was a mother living in O'Fallon, Missouri—the account was for a fictional

---

The expansive circuits seemed well aware that their position was contested. EarthCam, Inc. v. OxBlue Corp., 703 F. App'x 803, 808 (11th Cir. 2017) ("We decided Rodriguez [628 F.3d 1258] in 2010 without the benefit of a national discourse on the CFAA. Since then, several of our sister circuits have roundly criticized decisions like Rodriguez because, in their view, simply defining 'authorized access' according to the terms of use of a software or program risks criminalizing everyday behavior . . . . Neither the text, nor the purpose, nor the legislative history of the CFAA, those courts maintain, requires such a draconian outcome. We are, of course, bound by Rodriguez, but note its lack of acceptance.").

377. Orin Kerr, Testimony, "Cyber Security: Protecting America's New Frontier," House of Representatives Committee on the Judiciary Subcommittee on Crime, Terrorism, and Homeland Security (Nov. 15, 2011), http://volokh.com/wp/wp-content/uploads/2011/11/Testimony-of-Orin-S-Kerr.pdf ("In the Justice Department's view, the CFAA criminalizes conduct as innocuous as using a fake name on Facebook or lying about your weight in an online dating profile. The situation is intolerable.").

378. Staff Editor, *Is Using a Shared Netflix Password a Federal Crime?*, J. INTELL. PROP. & ENT. L. BLOG (Apr. 23, 2018), https://blog.jipel.law.nyu.edu/2018/04/is-using-a-shared-netflix-password-a-federal-crime/.

379. For a thorough chronological catalog of every CFAA scraping case through 2018, see Andrew Sellars, *Twenty Years of Web Scraping and the Computer Fraud and Abuse Act*, 24 B.U. J. SCI. & TECH. L. 372, 378–79 (2018).

380. For a deeper dive into the life of Swartz, who killed himself while being prosecuted under the CFAA, see THE INTERNET'S OWN BOY: THE STORY OF AARON SWARTZ (Luminant Media 2014).

381. *See, e.g.*, Orin Kerr, *Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes*, 78 N.Y.U. L. REV. 1596 (2003) (representative of multiple articles about the CFAA); David Thaw, *Criminalizing Hacking, Not Dating: Reconstructing the CFAA Intent Requirement*,103 J. CRIM. L. & CRIMINOLOGY 907 (2013); Andrew Sellars, *Twenty Years of Web Scraping and the Computer Fraud and Abuse Act*, 24 B.U. J. SCI. & TECH. L. 372, 378–79 (2018).

382. Decision on defendant's F.R.Crim.P. 29(c) motion, United States v. Drew, 259 F.R.D. 449, at 3 (C.D. Cal 2009) (No. Cr. 08-0582-GW). https://storage.courtlistener.com/recap/gov.uscourts.cacd.415703.162.0.pdf. Orin Kerr, who has discussed the CFAA at length,

teen named Josh Evans.[383] Masquerading as Evans, Drew began flirting with a girl named Megan Meier, a classmate of her daughter.[384] This went on for weeks until "Evans" told Megan that he no longer liked her and that "the world would be a better place without her in it."[385] Later that day, Megan died by suicide.[386] Prosecutors responded by charging Moore with violating the CFAA, alleging that she breached the Myspace Terms of Service (TOS), which, in part, required representation that "all registration information you submit is truthful and accurate."[387] Under their theory, Moore's violation of the TOS amounted to unauthorized access of the website.[388]

While the District Court was hypothetically open to some TOS violations amounting to CFAA violations, it found that "[t]reating a violation of a website's terms of service, without more, to be sufficient to constitute [a CFAA violation] would result in transforming § 1030(a)(2)(C) into an overwhelmingly overbroad enactment that would convert a multitude of otherwise innocent internet users into misdemeanant criminals."[389] Judge Hu declined to do so and granted Drew's motion for a judgment acquittal.[390]

New York Police Department (NYPD) officer Gilberto Valle engaged in a different type of harassment. He lived with his then-wife and baby daughter in Forest Hills, Queens.[391] He also had an active late-night second life where he graphically chatted with strangers about "kidnapping, torturing, cooking, raping, murdering, and cannibalizing various women," including his wife and other women the couple knew.[392] After discovering images of dead women on the couple's shared laptop, Valle's wife deployed the sort of spyware used to surveil victims of intimate partner violence and discovered Valle's messages.[393]

---

was part of Lori Drew's defense team. *See* All Things Considered, Fighting the Pseudonym Cyberwar, NPR (Nov. 19, 2011), https://www.npr.org/2011/11/19/142550202/fighting-the-pseudonym-cyberwar. The District Court cited Kerr's scholarship in its decision. Decision on defendant's F.R.Crim.P. 29(c) motion *United States v. Drew*, 259 F.R.D. 449, at 18 (C.D. Cal. 2009) (No. Cr. 08-0582-GW).

383. Decision on defendant's F.R.Crim.P. 29(c) motion at 3, United States v. Drew, 259 F.R.D. 449, at 3. She also used an unknown teen boy's photograph without his consent. *Id.*

384. *Id.*

385. *Id.*

386. *Id.* People considering suicide can call the National Suicide Prevention Lifeline at 1-800-273-TALK (8255).

387. *Id.* at 6–7.

388. *Id.*

389. *Id.* at 29.

390. *Id.* at 32.

391. United States v. Valle, 807 F.3d 508, 512 (2d Cir. 2015).

392. *Id.*

393. *Id.*

She alerted law enforcement about her findings.[394] During the investigation, it was uncovered that Valle violated NYPD policy by accessing a program that enables searches of restricted databases containing sensitive information such as home addresses.[395] He searched one woman's name with no law enforcement purpose.[396] Prosecutors charged Valle with "exceeding unauthorized access" in a companion provision to § 1030(a)(2)(C) focused on obtaining information from departments or agencies of the United States.[397]

Until the investigation, most of the women were unaware that Valle brutally fantasized about them online, but they were nevertheless victims of harassment who likely felt that their safety was threatened.[398] As Judge Parker explained, "fantasies of violence against women are both a symptom of a contributor to a culture of exploitation, a massive social harm that demeans women."[399] However, he continued, "in a free and functioning society, not every harm is meant to be addressed with the federal criminal law."[400] Valle claimed that because he was authorized to access the law enforcement program as part of his job, his lack of law enforcement purpose was irrelevant.[401] Rejecting an Eleventh Circuit interpretation—in which a bureaucrat was found guilty of violating CFAA to surveil a string of women[402]—Judge Parker determined that the CFAA was ambiguous, and concluded that the Second Circuit was compelled by the rule of lenity to adopt Valle's narrow interpretation of the CFAA.[403]

While Drew and Valle targeted real women, an imaginary one was the subject of Georgia police sergeant Nathan Van Buren's attempted harassment.

---

394. *Id.*

395. *Id.* at 512–13.

396. *Id.* at 524, 537.

397. *Id.* at 524.

398. *Id.* at 512. This is particularly true of Valle's ex-wife, who sought a divorce. *See* Alexander Abad-Santos, *What the Cannibal Cop's Wife Knew Is What No Wife Ever Wants to Know*, ATLANTIC (Feb. 26, 2013), https://www.theatlantic.com/national/archive/2013/02/cannibal-cop-wife-testimony/317976/.

399. United States v. Valle, 807 F.3d 508, 511 (2d Cir. 2015).

400. *Id.* at 511.

401. *Id.* at 523–24.

402. United States v. Rodriguez, 628 F.3d 1258, 1261–62 (11th Cir. 2010). Rodriguez's invasive behavior was extensive: he accessed his ex-wife's salary information, an ex-girlfriend's personal information sixty-two times, a former co-worker's daughter's information twenty-two times, a waitress' information twenty times, and multiple women from his church study group's information anywhere between ten and thirty-four times; he also used that illicit information offline in social interactions. *Id.* His is a rare case in which harassment of women led to a successful CFAA conviction, though it would likely no longer stand under *Van Buren*. *Id.*

403. Valle, 807 F.3d at 526–27.

Through his job, Van Buren encountered a man named Andrew Albo.[404] The two developed a rapport—Van Buren handled disputes between Albo and various women, and in turn Van Buren asked Albo for a personal loan for $15,368.[405] Unbeknownst to Van Buren, Albo surreptitiously recorded their conversation and presented it to the local sheriff's office.[406] The tape wound its way to the Federal Bureau of Investigation (FBI), which wondered just how far Van Buren would go for money.[407]

To find out, the FBI asked Albo to ask Van Buren to search the Georgia law enforcement computer database for the license plate of a woman that Albo supposedly met at a strip club—he claimed to be concerned that the woman was an undercover officer.[408] Given that several colleagues warned Van Buren about Albo's volatility, one can imagine the danger in which a real woman undercover officer might find herself.[409] Van Buren ignored department policy and accessed the database from his patrol car using his valid credentials, searched for the falsified license plate provided by Albo, and texted Albo that he'd uncovered information.[410] But before Van Buren could get his reward, he was charged with a felony for exceeding authorized access under § 1030(a)(2)(C) of the CFAA.[411]

After decades of the CFAA's interpretive schism, the Supreme Court confronted this slippery law. Echoing Valle's arguments, Van Buren claimed that misusing access does not amount to exceeding it.[412] Justice Barrett interrogated the absurdity of the government's argument, observing that "[i]f the 'exceeds authorized access' clause criminalizes every violation of a computer-use policy, then millions of otherwise law abiding citizens are criminals."[413] The Court declined to adopt such an interpretation, finally clarifying that violating TOS or computer use policies do not amount to federal crimes.[414]

404. Van Buren v. United States, 940 F.3d 1192, 1197 (11th Cir. 2019).
405. *Id.*
406. *Id.*
407. *Id.*
408. *Id.* Albo offered Van Buren $5,000 for his trouble. *Id.*
409. *Id.*
410. *Id.*
411. *Id.* at 1198.
412. Van Buren v. United States, 141 S. Ct. 1648, 1653 (2019).
413. *Id.* at 1661.
414. *Id.* The Court did not, however, invoke the rule of lenity. It also remains unclear how far the narrow interpretation extends. *See id.* at 1659 n.9 ("For present purposes, we need not address whether this inquiry turns only on technological (or "code-based") limitations on access, or instead also looks to limits contained in contracts or policies."); *cf.* Brief for Orin Kerr as *Amicus Curiae* 7 (urging adoption of code-based approach).

Consistently, courts bent the bounds of the CFAA beyond hacking when it came to competing travel agencies, disgruntled personnel, and nosy employees, but not when it came to protecting the safety of girls and women.[415] And, perhaps counterintuitively, that's a good thing. The Supreme Court's decision to adopt a narrow interpretation of the CFAA creates opportunities to combat oppression in ways that would otherwise be criminalized. It enables researchers to investigate race and gender disparities on employment websites.[416] It empowers journalists to scrape data needed to report on racial discrimination, police misconduct, and anti-competitive behavior.[417] It resists the temptation of carceral feminism by declining to rely on criminal law to promote feminist goals. And it reserves a range of non-carceral responses, such as civil lawsuits, adverse employment action, and medical interventions. However, the CFAA remains the key law used to prosecute Hunter Moore, which radical and other feminists would herald as a necessary invocation of criminal law against misogynistic abuse.

V. CONCLUSION

While Ringley launched Jennicam and Barlow penned his manifesto, Judge Easterbrook spoke at a symposium about Property in Cyberspace.[418] He observed that any effort to create a course collecting varying strands of law relating to horses, from sales to torts, into a so-called Law of the Horse would be "doomed to be shallow and miss unifying principles."[419] So too, he said, of the law of cyberspace.[420] He was wrong, but not for the reason other scholars

415. *See, e.g.*, EF Cultural Travel BV v. Explorica, Inc., 274 F.3d 577, 583–84 (1st Cir. 2001) (scraping website by competitor violated CFAA); Int'l Airport Ctrs. L.L.C. v. Citrin, 440 F.3d 418, 420–21 (7th Cir. 2006) (installing program that deleted files violated CFAA); Brown Jordan Int'l, Inc. v. Carmicle, 846 F.3d 1167, 1174–75 (11th Cir. 2017) (reading others' emails violated CFAA); all abrogated by United States v. Van Buren, 141 S. Ct. 1648 (2021). The CFAA creates civil and criminal penalties for the same provisions, and a fair number of broad interpretations were in the civil context.

416. Sandvig v. Barr, 451 F. Supp. 3d 73 (D.D.C. 2020) (violating employment websites' TOS not CFAA violation).

417. Brief for The Markup as Amicus Curiae Supporting Petitioner, Van Buren v. United States, 593 U.S. ___ (2021) (No. 19-783), https://www.supremecourt.gov/DocketPDF/19/19-783/147271/20200708180752488_19-783%20-%20the%20markup%20amicus%20brief%20for%20e-filing%207-8-2020.pdf.

418. Frank H. Easterbrook, *Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207, 208 (1996). The theory of the law of the horse was originated by Karl N. Llewellyn. *See generally* Karl N. Llewellyn, *Across Sales on Horseback*, 52 HARV. L. REV. 725 (1939); Karl N. Llewellyn, *The First Struggle to Unhorse Sales*, 52 HARV. L. REV. 873 (1939).

419. Frank H. Easterbrook, *Cyberspace and the Law of the Horse, Cyberspace and the Law of the Horse*, 1996 U. CHI. LEGAL F. 207, 207 (1996).

420. *Id.*

stated.[421] One unifying principle of cyberlaw is feminism. Cyberlaw is constantly amplifying and abridging the feminist values of consent, accessibility, and safety. Cyberlaw also engages with feminist goals, like preventing intimate partner violence, protecting sex workers, and preserving the privacy of pregnant people. And cyberlaw, viewed through a feminist lens, urges the emergence of legal practices that could create a more truly feminist cyberlaw. Feminism offers a means of making sense of cyberlaw. But, to be clear, cyberlaw is not feminist—yet.

Hopefully, scholars, advocates, and legislators will take an active role in developing feminist cyberlaw practice. Academics can center feminist cyberlaw perspectives in scholarship that influences law and policy. Practitioners can integrate feminist cyberlaw approaches into client counseling and advocacy. And lawmakers can prioritize legislation that embraces the feminist values of consent, accessibility, and safety to create a fourth category of cyberlaws: feminist cyberlaws that serve the overarching feminist goal of dismantling oppression. Contemporary cyberspace may feel bleak,[422] but feminist cyberlaw can provide a playbook for a better future.

421. *See, e.g.*, Joel R. Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules Through Technology*, 76 TEX. L. REV. 553 (1997) (offering unifying principles for technology law); Lawrence Lessig, Commentary, *The Law of the Horse: What Cyberlaw Might Teach*, 113 HARV. L. REV. 501 (1999) (developing a case for cyberlaw); Ira Steven Nathenson, B*est Practices for the Law of the Horse: Teaching Cyberlaw and Illuminating Law Through Online Simulations*, 28 SANTA CLARA HIGH TECH. L.J. 657 (2012) (making a pedagogical case for cyberlaw); Meg Leta Jones, *Does Technology Drive Law? The Dilemma of Technological Exceptionalism in Cyberlaw*, J.L. TECH. & POL'Y (2018) (disconfirming technological exceptionalism as an approach to cyberlaw); Alicia Solow-Niederman, *Emerging Digital Technology and the "Law of the Horse,"* UCLA L. REV. DISC.: LAW MEETS WORLD (2019) (connecting cyberlaw topics to fundamental legal principles); BJ Ard & Rebecca Crootof, *Structuring Techlaw*, 34 HARV. J.L. & TECH. 347 (2021) (defining the adjacent field of "techlaw"); Margot E. Kaminski, *Technological 'Disruption' of the Law's Imagined Scene: Some Lessons from Lex Informatic*a, 36 BERKLEY TECH. L.J. 102 (2022) (revisiting unifying principles offered by Joel Reidenberg); *cf.* JAMES GRIMMELMANN, INTERNET LAW: CASES AND PROBLEMS (Semaphore Press 2023) ("What if Internet law is no longer a 'specialized area of law' because all law is Internet law now?").

422. *See generally* WILLIAM GIBSON, NEUROMANCER 5 (Ace 1984) (ironically not coining the term "cyberspace"). The term "cyberspace" was coined by artist Susanne Ussing in the late 1960s. Jacob Lillemose & Mathias Kryger, *The (Re)invention of Cyberspace*, KUNSTKRITIKK (Aug. 24, 2015), https://kunstkritikk.com/the-reinvention-of-cyberspace/.