35:3 BERKELEY TECHNOLOGY LAW JOURNAL

2020

Pages
663
to
910

Berkeley Technology Law Journal
Volume 35, Number 3

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 35 NUMBER 3 2020

TABLE OF CONTENTS

ARTICLES

THE USE OF TECHNICAL EXPERTS IN SOFTWARE COPYRIGHT CASES: RECTIFYING THE NINTH CIRCUIT'S "NUTTY" RULE 663
Shyamkrishna Balganesh & Peter S. Menell

PATHWAYS TO INFORMATION PRIVACY POLICY: PLURALIST VS EXPERT? 717
Priscilla M. Regan

PERFORMING CYBERSECURITY EXPERTISE: CHALLENGES FOR PUBLIC UTILITY COMMISSIONS 757
Rebecca Slayton

ILLUSORY CONFLICTS: POST-EMPLOYMENT CLEARANCE PROCEDURES AND THE FTC'S TECHNOLOGICAL EXPERTISE 793
Lindsey Barrett, Laura Moy, Paul Ohm & Ashkan Soltani

THROUGH THE HANDOFF LENS: COMPETING VISIONS OF AUTONOMOUS FUTURES 835
Jake Goldenfein, Deirdre K. Mulligan, Helen Nissenbaum & Wendy Ju

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, University of California, Berkeley Law—Library, LL123 Boalt Hall—South Addition, 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, University of California, Berkeley Law—Library, LL123 Boalt Hall—South Addition, Berkeley, CA 94705-7210; (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 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., 20th ed. 2015). Please cite this issue of the *Berkeley Technology Law Journal* as 35 BERKELEY TECH. L.J. ___ (2020).

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.

DONORS

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

Partners

FENWICK & WEST LLP

ORRICK, HERRINGTON & SUTCLIFFE LLP

WHITE & CASE LLP

Benefactors

BAKER BOTTS LLP

COOLEY LLP

COVINGTON & BURLING LLP

FISH & RICHARDSON P.C.

JONES DAY

KIRKLAND & ELLIS LLP

LATHAM & WATKINS LLP

MCDERMOTT WILL & EMERY

MORRISON & FOERSTER LLP

PAUL HASTINGS LLP

POLSINELLI LLP

SIDLEY AUSTIN LLP

WEIL, GOTSHAL & MANGES LLP

WILMER CUTLER PICKERING HALE AND DORR LLP

WILSON SONSINI GOODRICH & ROSATI

WINSTON & STRAWN LLP

Corporate, Government, Individual, and Foundation Sponsors

ATLASSIAN

CORNERSTONE RESEARCH

DARTS IP

DORSEY & WHITNEY

FUTURE OF PRIVACY FORUM

ROBERT GLUSHKO

GOOGLE, INC.

H. WILLIAM HARLAN

HICKMAN PALERMO BECKER BINGHAM LLC

INTEL

INVENTIONSHARE

KILBURN & STRODE LLP

LITINOMICS

MARKS & CLERK LAW LLP

MICROSOFT CORPORATION

NERA ECONOMIC CONSULTING

PALANTIR

PHARMACEUTICAL RESEARCH AND MANUFACTURERS OF AMERICA

PWC

QUALCOMM

VIA LICENSING CORP

VYNYL

WESTERN DIGITAL

Members

ANJIE LAW FIRM

BAKER & MCKENZIE LLP

BEIJING EAST IP

CROWELL & MORING

DESMARAIS LLP

DURIE TANGRI LLP

GREENBERG TRAURIG

GTC LAW GROUP LLP & AFFILIATES

HAYNES AND BOONE, LLP

HOGAN LOVELLS, LLP

IRELL & MANELLA LLP

KEKER VAN NEST & PETERS LLP

KILPATRICK TOWNSEND & STOCKTON LLP

KNOBBE MARTENS OLSON & BEAR LLP

MORGAN, LEWIS & BOCKIUS LLP

ROBINS KAPLAN LLP

ROPES & GRAY LLP

SIMPSON THACHER & BARTLETT LLP

TENSEGRITY LAW GROUP LLP

TROUTMAN SANDERS LLP

VAN PELT, YI & JAMES LLP

WANHUIDA INTELLECTUAL PROPERTY

WEAVER AUSTIN VILLENEUVE & SAMPSON LLP

WILLKIE FARR & GALLAGHER LLP

WOMBLE BOND DICKINSON LLP

BOARD OF EDITORS 2019–2020

Executive Board

Editor-in-Chief
CHELSEA ANDRE

Managing Editor
AISLINN SMALLING

Senior Articles Editors
LESLIE DIAZ
CRISTINA MORA
COURTNEY REED

Senior Executive Editor
SAVANNAH CARNES

Senior Production Editor
MEGAN MCKNELLY

Senior Scholarship Editor
DANIEL CHASE

Senior Annual Review Editors
JULEA LIPIZ
MIRANDA RUTHERFORD

Senior Online Content Editor
CONCORD CHEUNG

Editorial Board

Production Editors
ANGELA GRIGGS
JANELLE LAMB
EMILY ROBERTS
HAILEY YOOK

Symposium Editor
ARMBIEN SABILLO

Online Content Editor
GINETTA SAGAN

Technical Editors
MADISON BOWER
MIN JUNG "MJ" HAN
ZACK JACOBS
RACHEL WILSON

Annual Review Editors
KRISTINA KRASNIKOVA
KEVIN YANG

Submissions Editors
CHRISTINA CROWLEY
DAVID FANG
MEHTAB KHAN

Notes & Comments Editors
HARRISON GERON
ALLAA MAGEID

Podcast Editor
ALLAN HOLDER

Web & Technology Editor
KARNIK HAJJAR

LLM Editor
IGOR SILVA

Alumni Relations Editor
NICK CALCATERRA

External Relations Editor
ASHLEIGH LUSSENDEN

Member Relations Editor
MICHELLE ZIPERSTEIN

Articles Editors

MUHTADI CHOUDHURY
MATTHEW CHUNG
SHWETA DUGGAL
JASON FRANCIS
KELLY GO
EMMA LEE
WALTER MOSTOWY
JOSH SEDGWICK
CARMEN SOBCZAK
MARTA STUDNICKA
MEI XUAN

MEMBERSHIP

Vol. 35 No. 3

Associate Editors

ELIZABETH FU
LOC HO
NOAHLANI LITWINSELLA
JENNY QUANG
ANDY ZACHRICH

Members

LIAM AARTASH
SHAHAD ALFAWAZ
BADER ALSHABANAT
TAIT ANDERSON
CHRISTOPHER BARCLAY
JOHN BATOHA
MAYA BAUMER
MARGERITE BLASE
RASMUS BLOM
CONNOR BOEHM
VERONICA BOGNOT
JONATHAN CHACON
SUSIE CHEN
KEVIN J. CHEN
JENNIFER CHUNG
HENDRIK COPPOOLSE
NATALIE CRAWFORD
KATHARINE CURRAULT
JAMESON DAVIS
CHENXI DUAN
EVAN ENZER
ANUJ EZEKIEL
JOSHUA FRANK
LIZ FREEMAN ROSENZWEIG
ADITI GHATLIA
BEN GOLDFEIN
EDWIN JESUS GONZALEZ
JAKE GORHAM
ISHA GULATI
SALONI GUPTA
CALVIN HANNAGAN
ALEXANDRA HARVEY
ELIZABETH HECKMANN
SOONYOUNG HEO
JENNIFER HEWITT
THOMAS HORN
JEFFREY JACOBSEN
TOM JAMES
CARTER JANSEN
ANJANAYE JARIWALA
GIA JUNG
PHILIP KATZ
IAN KELLY
YEJI KIM
GRACE HO JUNG KIM
JOSEPH KROON
TZU-I LEE
YI SHYUAN LEE
GASPARE LODERER
ANNE LUQUETTE
MARGARET LYNCH
CHRISTIAN MCFALL
GRACE MCFEE
MEET MEHTA
MEHREEN MIR
ERIN MOORE
JACKSON MORAWSKI
DEBBIE MOSLEY
GODHULI NANDA
DAN NOEL
MAXIMIN ORSERO
JOSHUA PARZIVAND
NINA POUGET
GAYATRI RAGHUNANDAN
EMILY ROBERTS
FABIOLA ROSSY SEPTYA CHRISTINA
EILEEN SANFORD
SHEETAL SARAN
YEMAJ SHEIK
ZIYU SHI
DAKOTA SNEED
TAYLOR TAM
THERESA TAN
AMREEN TANEJA
RACHEL TERRELL-PERICA
ELHITA THAMPURAN
RACHEL THOMPSON
MICKEALA TU
BLAINE VALENCIA
ARPAWAN WAEN VEJJAJIVA
DEREK WEST
CRISTINA WHTIE
MELODY WONG
BILLY WU
YEXI XU
MEI XUAN
JOSHUA YOO
CHENZHAO YU
MICHELLE ZHOU

BTLJ ADVISORY BOARD

BERKELEY CENTER FOR LAW & TECHNOLOGY 2019–2020

Executive Director

JIM DEMPSEY

Faculty Directors

KENNETH A. BAMBERGER
CATHERINE CRUMP
CATHERINE FISK
CHRIS HOOFNAGLE
SONIA KATYAL
ORIN KERR
PETER S. MENELL
ROBERT P. MERGES
DEIRDRE K. MULLIGAN
TEJAS NARECHANIA
ANDREA ROTH
PAMELA SAMUELSON
PAUL SCHWARTZ
ERIK STALLMAN
JENNIFER M. URBAN
MOLLY S. VAN HOUWELING
REBECCA WEXLER

Fellows

KATHRYN HASHIMOTO
CHRISTINA KONINGISOR

Staff

MARK COHEN
NATHALIE COLETTA
JANN DUDLEY
RICHARD FISK
MATTHEW RAY
IRYS SCHENKER

THE USE OF TECHNICAL EXPERTS IN SOFTWARE COPYRIGHT CASES: RECTIFYING THE NINTH CIRCUIT'S "NUTTY" RULE

Shyamkrishna Balganesh† *& Peter S. Menell*††

ABSTRACT

Courts have long been skeptical about the use of expert witnesses in copyright cases. More than four decades ago, and before Congress extended copyright law to protect computer software, the Ninth Circuit in *Krofft Television Productions, Inc. v. McDonald's Corp.* ruled that expert testimony was inadmissible to determine whether Mayor McCheese and the merry band of McDonald's characters infringed copyright protection for Wilhelmina W. Witchiepoo and the other imaginative H.R. Pufnstuf costumed characters. Since the emergence of software copyright infringement cases in the 1980s, substantially all software copyright cases have permitted expert witnesses to aid juries in understanding software code. As the Second Circuit recognized in *Computer Associates International, Inc. v. Altai, Inc.*, the ordinary observer standard "may well have served its purpose when the material under scrutiny was limited to art forms readily comprehensible and generally familiar to the average lay person," but as to computer programs, district courts must have "discretion . . . to decide to what extent, if any, expert opinion, regarding the highly technical nature of computer programs, is warranted in a given case."

In a shocking departure from the decisions of every other circuit that has confronted software copyright infringement litigation, the Ninth Circuit reaffirmed and applied the bar on expert testimony originating in *Krofft Television Productions* to all copyright disputes, including those involving highly technical computer software code. The court in *Antonick v. Electronic Arts, Inc.* held that lay juries must decipher and analyze software code—distinct hexadecimal assembly code languages for different processors—without the assistance of expert witnesses, a rule that the authoring judge characterized at the oral argument as "nutty."

The Ninth Circuit's rule overlooks the key distinction between the use of technical experts to *analyze* substantial similarity as opposed to enabling lay judges and jurors to *perceive* the underlying works. Just as it would be absurd to ask a lay jury with no familiarity with Kanji characters to assess whether a translation of HARRY POTTER AND THE PHILOSOPHER'S STONE into Japanese infringed the English original without the aid of a bilingual translator, it makes no sense to ask a non-technical jury to compare computer source codes written in different assembly languages to determine substantial similarity without expert assistance. We contend, consistent with the views of every court outside of the Ninth Circuit that has addressed the issue, that courts should permit the use of technical experts to enable lay judges and juries to perceive the meaning of computer languages and computer code.

DOI: https://doi.org/10.15779/Z38ST7DX70

† Sol Goldman Professor of Law, Columbia Law School.

†† Koret Professor of Law; Director, Berkeley Center for Law & Technology; Faculty Director, Berkeley Judicial Institute; University of California, Berkeley, School of Law. Professor Menell served as counsel in the appeal, *en banc* petition, and *certiorari* petition in *Antonick v. Electronic Arts, Inc.*, 841 F.3d 1062 (9th Cir. 2016), *cert. denied*, 138 S. Ct. 422 (2017).

TABLE OF CONTENTS

I. INTRODUCTION 664

II. THE HISTORICAL ROOTS OF EXPERT WITNESS SKEPTICISM 666

III. COMPUTER SOFTWARE CASES: AN EXCEPTION TO THE TRADITIONAL RULE LIMITING EXPERT TESTIMONY 671

IV. THE UNWITTING ORIGIN OF THE NINTH CIRCUIT'S "NUTTY" RULE: *KROFFT TELEVISION PRODUCTIONS, INC. V. MCDONALD'S CORP.* 675

V. *ANTONICK V. ELECTRONIC ARTS*: MANIFESTATION OF THE "NUTTY" RULE 679

A. DEVELOPMENT OF THE MADDEN FOOTBALL VIDEO GAME 680
B. ANTONICK'S DISCOVERY THAT EA BASED SEGA MADDEN ON APPLE II MADDEN 683
C. ANTONICK'S COMPLAINT AND THE COPYRIGHT INFRINGEMENT ISSUE 685
D. PRE-TRIAL PROCEEDINGS: IMPROPER WHITTLING OF THE PLAINTIFF'S BASIS FOR SHOWING THAT EA DERIVED SEGA MADDEN FROM APPLE II MADDEN 686
E. JURY TRIAL: VERDICTS FOR ANTONICK 692
F. POST-TRIAL PROCEEDINGS: JUDGMENT FOR EA AS A MATTER OF LAW 700
G. NINTH CIRCUIT APPEAL: RECOGNITION, AFFIRMANCE, AND EXPANSION OF THE "NUTTY" RULE 704
H. EN BANC AND CERTIORARI PETITIONS: DENIED 713

VI. RECTIFYING THE NINTH CIRCUIT'S NUTTY RULE 714

I. INTRODUCTION

Copyright law has long relied on the views of lay audiences to assess the critical infringement question: whether the defendant's work is substantially similar to protected elements of the plaintiff's work of authorship. The Seventh Amendment right to a jury trial reinforces lay juries' role in resolving copyright cases. For much of U.S. history, lay jurors were capable of comparing literary and artistic works through direct observation of the manuscripts, pictures, and sculptures. Copyright law achieved a democratic

character. Subject to the jury instructions regarding the contours of the law, a diverse group of lay people assesses infringement if either party so requests.

Consequently, courts have long been skeptical about the use of expert witnesses in copyright cases. Courts have long allowed experts to assist in the objective assessment of which aspects of the copyrighted work are protectable. All the same, courts have also prohibited experts from assisting the fact-finder in comparing the works in question to determine substantial similarity of protected expression—the subjective or intrinsic inquiry. With the extension of copyright protection to computer software, however, the Second Circuit recognized that while the ordinary observer standard "may well have served its purpose when the material under scrutiny was limited to art forms readily comprehensible and generally familiar to the average lay person," district courts must have "discretion . . . to decide to what extent, if any, expert opinion, regarding the highly technical nature of computer programs, is warranted in a given case."[1] Most other circuits to confront software copyright cases came to the same conclusion.[2]

In a shocking departure from the decisions of every other circuit that has confronted software copyright infringement litigation, the Ninth Circuit has continued to bar expert testimony on the intrinsic test in cases involving highly technical computer software code. It held in *Antonick v. Electronic Arts, Inc.* that lay juries must decipher and analyze software code—distinct hexadecimal[3] assembly code languages for different processors—without the assistance of

1. Comput. Assocs. Int'l, Inc. v. Altai, Inc., 982 F.2d 693, 713 (2d Cir. 1992).

2. *See, e.g.*, Gates Rubber Co. v. Bando Chem. Indus., 9 F.3d 823, 834–35 (10th Cir. 1993) ("[W]e decline to set forth any strict methodology for the abstraction of computer programs. . . . [W]e foresee that the use of experts will provide substantial guidance to the court in applying an abstractions test.").

3. Hexadecimal provides a convenient way of representing binary information, which is very important for computer systems. Computer systems store information in arrays of on/off switches. Thus, the basic unit of information in computer systems is a binary digit ("0" or "1") or "bit." *See generally Bit*, WIKIPEDIA, https://en.wikipedia.org/wiki/Bit (last visited Aug. 29, 2020). Hexadecimal features a base of sixteen symbols ("0"–"9," "A"–"F") as opposed to the more common decimal ("0"–"9") system. *See generally Hexadecimal*, WIKIPEDIA, https://en.wikipedia.org/wiki/Hexadecimal (last visited Aug. 29, 2020). Hence, hexadecimal symbols provide a human-friendly representation of binary-coded values. Each hexadecimal digit represents four binary digits, also known as a "nibble," which is half a byte. A "byte" is a unit of digital information that most commonly consists of eight bits. *See generally Byte*, WIKIPEDIA, https://en.wikipedia.org/wiki/Byte (last visited Aug. 29, 2020). Historically, the byte was the number of bits used to encode a single character of text in a computer and for this reason was the smallest addressable unit of memory in many computer architectures. For example, a single byte can have values ranging from 00000000 to 11111111 in binary form, which can be conveniently represented as 00 to FF in hexadecimal.

expert witnesses,[4] a rule that the authoring judge characterized at the oral argument as "nutty."[5]

This Article explores the role of technical experts in copyright cases. Part II traces the history of expert witness skepticism in copyright infringement analysis. Part III discusses the departure from that skepticism in software copyright cases in most circuit courts. Part IV surveys the Ninth Circuit's unusual infringement jurisprudence. Part V then extensively and critically examines *Antonick v. Electronic Arts, Inc*, which prohibited the use of expert witness testimony to assist a jury deciphering complex computer languages. Part VI contends the time is long overdue for the Ninth Circuit, home to much of the computer software industry, to join the chorus of other circuits that allows expert witnesses to assist juries in perceiving complex computer programs.

II. THE HISTORICAL ROOTS OF EXPERT WITNESS SKEPTICISM

The earliest use of expert testimony in adversarial common law litigation is usually traced back to 1782 and Chief Justice Mansfield's famed decision in *Folkes v. Chadd*.[6] Scholars have long regarded this case as having developed the "foundation" for the rules governing expert witnesses.[7] *Folkes* was a property dispute, and the witnesses involved in the case were primarily engineers. In permitting the court to receive their testimony, Justice Mansfield developed the position that the opinions of experts when "formed on facts was very proper evidence."[8] Even though *Folkes* was not a copyright case, Justice Mansfield's role in it is noteworthy given his prominence at the time, especially in the world of copyright law.[9]

By the turn of the nineteenth century, it appears to have become fairly common for litigants in English music copyright cases to present the court with the testimony of experts. The 1835 decision in *D'Almaine v. Boosey* is a perfect example.[10] The facts involved an operatic composition assigned to the plaintiff, which the defendant had copied and published but with some

4. *See* Antonick v. Elec. Arts, Inc., 841 F.3d 1062, 1065–66 (9th Cir. 2016).

5. *Infra* note 197.

6. *See* Folkes v. Chadd, 99 Eng. Rep. 589 (1782).

7. *See, e.g.*, Tal Golan, *Revisiting the History of Scientific Expert Testimony*, 73 BROOKLYN L. REV. 879, 887 (2008).

8. *Folkes*, 99 Eng. Rep. at 590.

9. Judge Mansfield had decided in 1769 the celebrated case of *Millar v. Taylor*. *See* 98 Eng. Rep. 291 (1769).

10. D'Almaine v. Boosey, 160 Eng. Rep. 117 (1835).

significant substantive embellishments.[11] Among other arguments, the defendant claimed that these embellishments rendered his work an altogether different one and thus his publication non-piratical.[12] In support of their claims, both the plaintiff and defendant relied on affidavits from "experienced musician[s]," which the court accepted as entirely unproblematic.[13] Perhaps more importantly, in finding for the plaintiff the court itself granted relief on a prior (unnamed) decision dealing with musical compositions, and noted how that prior decision was significant because it was based on the views of the famed musician and composer "Sir George Smart, who was a witness in the case."[14]

It remains unclear when U.S. courts developed a regularized sense of comfort with expert testimony in copyright matters. What we do know is that they seem to have largely followed the English model of allowing experts in cases involving musical compositions. The court adopted and followed the English case of *D'Almaine* in the notable case *Jollie v. Jaques*.[15] A decision of the federal district court in New York, the case involved a matter largely similar to *D'Almaine,* and the court was called upon to examine whether the defendant's work was an infringement of the plaintiff's despite having added multiple variations.[16] Relying on the English precedent, the court denied the plaintiff's request for an injunction. Important for us though is the fact that in support of its argument the defendant presented the testimony of "an expert, who had examined and compared the two pieces of music."[17] The court accepted this testimony as uncontroversial, in almost identical manner as the court had in *D'Almaine.*

A federal district court adopted a similar approach a few years prior to *Jollie*. In *Reed v. Carusi*,[18] the plaintiff alleged an infringement of the copyright in its ballad, a musical composition. As part of its unsuccessful defense, the defendant claimed that the plaintiff's work was itself drawn from a prior source—and to support this claim the defendant introduced the testimony of

11. *See id.* at 118–21.
12. *See id.* at 122.
13. *Id.* at 118–19.
14. *Id.* at 123.
15. Jollie v. Jaques, 13 F. Cas. 910, 913 (C.C.S.D.N.Y. 1850). For an excellent discussion of the substantive issue involved in both *D'Almaine* and *Jollie*, see Joseph P. Fishman, *Music as a Matter of Law*, 131 HARV. L. REV. 1861, 1877–79 (2018).
16. *See Jollie*, 13 F. Cas. at 913–14.
17. *Id.* at 913.
18. Reed v. Carusi, 20 F. Cas. 431 (C.C.D. Md. 1845).

various experts in music, which was delivered to the jury without any documented controversy.[19]

Neither of the two leading copyright treatises from the nineteenth century—*Curtis on Copyright* and *Drone on Copyright*—however, address the issue directly.[20] All the same, neither expresses any disagreement with the English cases that rely on the affidavits of experts, or with the U.S. cases that adopt a similar approach.

Eaton S. Drone, in particular, spends a good amount of time describing the test for "piracy," i.e., copyright infringement, where the use of experts has since become a matter of controversy. Recognizing that the comparison of the works is usually a laborious and time-intensive process that entails a complex analysis of the two works, Drone notes how "[i]n the United States, the usual practice in cases involving much labor has been to make a reference to a master."[21] He further notes that "[t]he master may be required not only to report the facts, but also to give his opinion as to whether the plaintiff's work is original, and whether it has been infringed by the defendant."[22] While this account tracks the modern practice of a court-appointed expert or master, it is nevertheless telling in two respects. First, it involves the court—rather than the parties—directly relying on the master. And second, the rationale for such reliance, in Drone's view, was not expertise over subject-matter but rather the labor and time involved in undertaking a scrutiny and comparison of the works, which was seemingly unworthy of the court's attention at the time. This suggests that treatise-writers and perhaps courts as well hardly saw nineteenth-century U.S. copyright law as requiring specific expertise beyond knowledge of the doctrine and the standard legal principles and methods of argumentation and reasoning commonly deployed. A comparison of the works—however complex—was a matter of perception, which required little more than time and patience and was entirely a question of fact and judgment internal to a court's ordinary role.

To the extent that such expertise was required or allowed, it seems to have been relegated to the domain of music. This trend continued through the nineteenth century and into the early part of the twentieth century. The developmental jurisprudence around the law relating to infringement of musical works routinely contains references to expert reports, testimony, and

19. *See id.* at 432.

20. *See generally* EATON S. DRONE, A TREATISE ON THE LAW OF PROPERTY IN INTELLECTUAL PRODUCTIONS (1879); GEORGE TICKNOR CURTIS, A TREATISE ON THE LAW OF COPYRIGHT (1847).

21. DRONE, *supra* note 20, at 513.

22. *Id.* at 514.

affidavits presented to courts for proof of copying.[23] And while courts for the most part relied on the notion of the "average ear," they nevertheless appear to have somewhat routinely allowed expert opinions to influence their views on originality and copying.

As copyright litigation matured, savvy litigants and their lawyers attempted to cloak perceptibility with the need for expertise that was well beyond something a judge ordinarily possessed. In so doing, they implicitly pushed the idea that courts should make use of expert witnesses with knowledge of the subject-matter at issue in the lawsuit, a claim that went well beyond music. In the late 1920s, Moses Malevinsky, counsel to Anne Nichols in the seminal case of *Nichols v. Universal Pictures Corp.*,[24] sought to offer his own scientific theory as the basis for assessing similarity of dramatic works, a theory which he had published as a freestanding monograph at the time of the litigation.[25] While acknowledging Malevinsky's "deep study of the technical construction of plays and motion pictures," District Judge Henry Goddard concluded that Malevinsky's theory called for a "new test, or at least a new method of approach" that impermissibly would extend protection to ideas.[26] On appeal, Judge Learned Hand was especially skeptical of the use of experts to aid the court in judging copyright infringement:

> We cannot approve the length of the record, which was due chiefly to the use of expert witnesses. Argument is argument whether in the box or at the bar, and its proper place is the last. The testimony of an expert upon such issues, especially his cross-examination, greatly extends the trial and contributes nothing which cannot be better heard after the evidence is all submitted. It ought not to be allowed at all; and while its admission is not a ground for reversal, it cumbers the case and tends to confusion, for the more the court is led into the intricacies of dramatic craftsmanship, the less likely it is to stand upon the firmer, if more naive, ground of its considered impressions upon its own perusal. We hope that in this class of cases such evidence may in the future be entirely excluded, and the case

23. For a general overview, see generally Paul W. Orth, *The Use of Expert Witnesses in Musical Infringement Cases*, 16 U. PITT. L. REV. 232 (1955).

24. Nichols v. Universal Pictures Corp., 34 F.2d 145 (S.D.N.Y. 1929) [hereinafter *Nichols I*], *aff'd*, 45 F.2d 119 (2d Cir. 1930) [hereinafter *Nichols II*].

25. *See* MOSES MALEVINSKY, THE SCIENCE OF PLAYWRITING (1925); *see generally* MARK ROSE, AUTHORS IN COURT: SCENES FROM THE THEATER OF COPYRIGHT 98–103 (2016) (discussing Malevinsky's unusual trial strategy, which included himself testifying for seven days).

26. *See Nichols I*, 34 F.2d at 147.

> confined to the actual issues; that is, whether the defendant copied it, so far as the supposed infringement is identical.[27]

The modern formulation of copyright infringement analysis emerged sixteen years later in the Second Circuit. Ira Arnstein, a litigious and prolific but largely unknown composer, alleged that five of famed composer Cole Porter's popular compositions infringed multiple Arnstein compositions.[28] Porter denied ever hearing Arnstein's composition. The case unfolded shortly after the promulgation of the Federal Rules of Civil Procedure, which played a significant role in the formulation of the modern infringement framework.

Arnstein set forth a two-part test focused on what became known as "illicit" copying. As formulated then, the plaintiff had to prove "(a) that defendant copied from plaintiff's copyrighted work and (b) that the copying (assuming it to be proved) went to [sic] far as to constitute improper appropriation."[29] The first prong allowed expert testimony. "On this issue, analysis ('dissection') is relevant, and the testimony of experts may be received to aid the trier of the facts."[30] The second prong required proof of "illicit copying (unlawful appropriation)."[31] Judge Jerome Frank declared that "the test is the response of the ordinary lay hearer; accordingly, on that issue, 'dissection' and expert testimony are irrelevant."[32] Judge Frank's reasons for the categorical rejection of expert testimony on this second question remain perplexing and appear to have been motivated more by the unique interpersonal interaction between the judges on the panel than any rational belief in the value of experts.[33] Nevertheless, it found its way into the majority's opinion.

The *Arnstein* court, however, did not altogether preclude the use of expert testimony during the actual comparison of the two works, even where it was the jury who determines the issue. To the contrary, the court emphasized that expert testimony (there from trained musicians) could instead aid the fact-finder in assessing the responses of the intended audience (music listeners) for the work.[34] The court explicitly determined that use of expert testimony may

27. *Nichols II*, 45 F.2d at 123.

28. *See* Arnstein v. Porter, 154 F.2d 464, 467 (2d Cir. 1946); *see generally* GARY A. ROSEN, UNFAIR TO GENIUS: THE STRANGE AND LITIGIOUS CAREER OF IRA B. ARNSTEIN (2012).

29. *Arnstein*, 154 F.2d at 468.

30. *Id.*

31. *Id.*

32. *Id.*

33. *See* Shyamkrishna Balganesh, *The Questionable Origins of the Copyright Infringement Analysis*, 68 STAN. L. REV. 791, 832–37 (2016).

34. *See Arnstein*, 154 F.2d at 473 ("[Expert testimony of musicians] may aid the jury in reaching its conclusion as to the responses of [lay listeners].").

be appropriate in aiding the fact-finder even under the second prong.[35] Yet, it forewarned that such expertise not become "controlling" on the question, but instead an aid to the decision-maker.[36]

The *Arnstein* framework was developed against the backdrop of a deep skepticism towards courts' reliance on summary judgment to decide the question of infringement. In the many years since the decision, much has changed on that front.[37] Not only has the standard for summary judgment as articulated in *Arnstein* been significantly overhauled, but courts' very resort to summary judgment is now actively encouraged in the jurisprudence.[38] Despite this reality, courts around the country continue to rely on Judge Frank's two-step formulation.

The modern reliance on summary judgment to decide infringement has further complicated the two-part test formulated in *Arnstein*, which was designed for use principally in trials. With courts in most jurisdictions able to decide both steps of the test on a motion for summary judgement,[39] the prohibition on expert testimony to aid the second step is often rendered functionally moot. Since they make use of such testimony on the first step, the prohibition on using it for the second merely translates into courts avoiding a complete (or "determinative") reliance on such testimony in their decision on the second prong. Nevertheless, to the extent that infringement cases proceed to trial—either bench or jury—the prohibition on expert testimony on the second prong remains widespread. And here the unfortunate reality remains that even though *Arnstein* did not altogether preclude expert testimony on the second prong but merely prohibited treating it as determinative, the Ninth Circuit, as we shall see, has treated the rule as a firm prohibition.

III. COMPUTER SOFTWARE CASES: AN EXCEPTION TO THE TRADITIONAL RULE LIMITING EXPERT TESTIMONY

As the computer software marketplace emerged in the early 1970s, Congress included computer software within the scope of "literary works" in

35. *See id.*
36. *See id.*
37. *See* Balganesh, *supra* note 33, at 852–53.
38. *Id.*
39. *See* ROBERT C. OSTERBERG & ERIC C. OSTERBERG, SUBSTANTIAL SIMILARITY IN COPYRIGHT LAW § 3 (2018).

the Copyright Act of 1976.[40] In view of the technological complexity of computer software—entailing unusual and technical computer languages that are unfamiliar to lay judges and juries[41]—courts came to see that expert testimony would be necessary to perceive the similarity of computer programs. In *Whelan Associates, Inc. v. Jaslow Dental Laboratory, Inc.*,[42] the Third Circuit recognized that the *Arnstein* limitation on the use of expert witnesses in the subjective stage of the infringement analysis did not make sense in computer software cases:

> The ordinary observer test, which was developed in cases involving novels, plays, and paintings, and which does not permit expert testimony, is of doubtful value in cases involving computer programs on account of the programs' complexity and unfamiliarity to most members of the public. *See* Note, *Copyright Infringement of Computer Programs: A Modification of the Substantial Similarity Test*, 68 MINN. L. REV. 1264, 1285–88 (1984). *Cf.* Note, *Copyright Infringement Actions: The Proper Role for Audience Reactions in Determining Substantial Similarity*, 54 S. CAL. L. REV. 385 (1981) (criticizing lay observer standard when objects in question are intended for particular, identifiable audiences). Moreover, the distinction between the two parts of the *Arnstein* test may be of doubtful value when the finder of fact is the same person for each step: that person has been exposed to expert evidence in the first step, yet she or he is supposed to ignore or "forget" that evidence in analyzing the problem under the second step. Especially in complex cases, we doubt that the "forgetting" can be effective when the expert testimony is essential

40. The Act includes "literary works" within the class of "works of authorship." *See* 17 U.S.C. § 102(a)(1). The House Report explains:

> The term 'literary works' does not connote any criterion of literary merit or qualitative value: it includes catalogs, directories, and similar factual, reference, or instructional works and compilations of data. It also includes computer data bases, and computer programs to the extent that they incorporate authorship in the programmer's expression of original ideas, as distinguished from the ideas themselves.

H.R. REP. NO. 94-1476, at 54 (1976) (emphasis added). Other provisions of the 1976 Act, however, maintained traditional exclusions for ideas and functional features, 17 U.S.C. § 102(b), and Congress added additional safeguards against overbroad protection in 1980, Act of Dec. 12, 1980, Pub. L. No. 96-517, 94 Stat. 3007, 3028 (codified at 17 U.S.C. §§ 101, 117) (adopting recommendations of the NAT'L COMM'N ON NEW TECH. USES OF COPYRIGHTED WORKS, FINAL REPORT 1 (1979)). *See* Peter S. Menell, *Rise of the API Copyright Dead?: An Updated Epitaph for Copyright Protection of Network and Functional Features of Computer Software*, 31 HARV. J.L. & TECH. 305, 315–18 (2018).

41. *See* Peter S. Menell, *An Analysis of the Scope of Copyright Protection for Application Programs*, 41 STAN. L. REV. 1045, 1051–57 (1989).

42. Whelan Assocs., Inc. v. Jaslow Dental Lab'y, Inc., 797 F.2d 1222 (3d Cir. 1986).

> to even the most fundamental understanding of the objects in question.
>
> On account of these problems with the standard, we believe that the ordinary observer test is not useful and is potentially misleading when the subjects of the copyright are particularly complex, such as computer programs. We therefore join the growing number of courts which do not apply the ordinary observer test in copyright cases involving exceptionally difficult materials, like computer programs, but instead adopt a single substantial similarity inquiry according to which both lay and expert testimony would be admissible. *See E.F. Johnson Co. v. Uniden Corp.*, 623 F. Supp. 1485, 1493 (D. Minn. 1985); *Hubco Data Products Corp. v. Management Assistance Inc.*, 2 Copyright L. Rep. (CCH) para. 25,529 (D. Idaho Feb. 3, 1983) (enunciating bifurcated test, but relying entirely on expert testimony); *Midway Mfg. Co. v. Strohon*, 564 F. Supp. 741, 752–53 (N.D. Ill. 1983) (relying entirely on expert testimony to find substantial similarity); *see also* Fed. R. Evid. 701 ("If [expert testimony] will assist the trier of fact to understand the evidence or to determine a fact in issue, a witness . . . may testify thereto in the form of an opinion or otherwise.").[43]

In the landmark *Altai* case, the Second Circuit distinguished *Arnstein* and held that the prohibition on expert testimony was inapplicable to comparisons of computer software under the second prong because "we cannot disregard the highly complicated and technical subject matter at the heart of these claims."[44] The court observed that "computer programs are likely to be somewhat impenetrable by lay observers—whether they be judges or juries—and, thus, seem to fall outside the category of works contemplated by those who engineered the *Arnstein* test."[45] Consequently, the *Altai* court concluded that "on substantial similarity with respect to computer programs, we believe that the trier of fact need not be limited by the strictures of its own lay perspective," and it was at "the discretion of the district court to decide to what extent, if any, expert opinion, regarding the highly technical nature of computer programs, is warranted in a given case."[46] The *Altai* decision expressly permits expert testimony at the discretion of the district court.[47]

43. *Id.* at 1232–33 (citations omitted). While we agree with the *Whelan* court's determination that software experts ought to be permitted to aid judges and juries in perceiving the works at issue in computer software cases, we question the manner in which the *Whelan* court applied copyright's limiting doctrines. *See* Menell, *supra* note 41, at 1074.

44. Comput. Assocs. Int'l, Inc. v. Altai, Inc., 982 F.2d 693, 713 (2d Cir. 1992).

45. *Id.*

46. *Id.*

47. *See id.*

Other courts followed the Second Circuit's lead. The Tenth Circuit has "[i]n substantial part . . . adopt[ed]" the *Altai* test in *Gates Rubber Co. v. Bando Chemical Industries, Ltd.*[48] Although *Gates Rubber* did not explicitly address expert testimony at all stages of the test, *Altai* allows such testimony, and the *Gates Rubber* court endorsed use of experts in at least some of the inquiry.[49] The Fifth Circuit has also adopted the *Altai* test, although it did not explicitly address the use of experts to aid comparison.[50]

Three other circuits have approved the use of expert testimony to evaluate substantial similarity in cases involving difficult or complex works other than software. The Fourth Circuit in *Dawson v. Hinshaw Music Inc.* firmly rejected the approach of refusing to permit expert testimony in a music case, noting that "only a reckless indifference to common sense would lead a court to embrace a doctrine that requires a copyright case to turn on the opinion of someone who is ignorant of the relevant differences and similarities between two works."[51] The court replaced the "ordinary observer" with the "intended audience" of the work and permitted the fact-finder to rely on expert testimony.[52] The *Dawson* court noted that "the advent of computer programming infringement actions" forced the trend towards allowing expert testimony for complex subject matter.[53]

The Sixth Circuit addressed the use of experts in a case alleging copyright infringement of technical patent drawings.[54] Its two-step test contemplates use of expert testimony; in its second step, "the trier of fact should make the substantial similarity determination from the perspective of the intended audience. *Expert testimony will usually be necessary to educate the trier of fact* in those elements for which the specialist will look."[55]

Although the First Circuit uses a traditional "ordinary observer" test, it recognized in a case involving architectural works that "*the need for expert testimony may be greater in cases involving complex subject matters* where an ordinary

48. Gates Rubber Co. v. Bando Chem. Indus., 9 F.3d 823, 834 (10th Cir. 1993).

49. *See id.* at 834–35 ("[I]n most cases we foresee that *the use of experts will provide substantial guidance to the court* in applying an abstractions test.") (emphasis added).

50. *See* Eng'g Dynamics, Inc. v. Structural Software, Inc., 26 F.3d 1335, 1342 (5th Cir. 1994), *opinion supplemented on denial of reh'g*, 46 F.3d 408 (5th Cir. 1995).

51. Dawson v. Hinshaw Music Inc., 905 F.2d 731, 735 (4th Cir. 1990).

52. *Id.* at 736 ("When conducting the second prong of the substantial similarity inquiry, a district court must consider the nature of the intended audience of the plaintiff's work. . . . Such an inquiry may include, and no doubt in many cases will require, admission of testimony from members of the intended audience or, possibly, from those who possess expertise with reference to the tastes and perceptions of the intended audience.").

53. *Id.* at 735.

54. *See* Kohus v. Mariol, 328 F.3d 848 (6th Cir. 2003).

55. *Id.* at 857 (emphasis added).

observer may find it difficult to properly evaluate the similarity of two works without the aid of expert testimony."[56] The D.C. Circuit has noted the trend of allowing expert testimony for comparison of complex works like software, though without explicitly addressing the issue.[57]

IV. THE UNWITTING ORIGIN OF THE NINTH CIRCUIT'S "NUTTY" RULE: *KROFFT TELEVISION PRODUCTIONS, INC. V. MCDONALD'S CORP.*

Even though *Arnstein* was decided under a now-overruled standard for summary judgment,[58] it remains influential. And unfortunately, so does the misunderstanding of its views on the use of expert testimony. Nowhere is this more prominent than in the Ninth Circuit, which purported to develop its own two-part test based on *Arnstein*.

In *Krofft*, the Ninth Circuit was called upon to develop an approach to the infringement analysis that recognized copyrightable works as embodying both protected and unprotected elements.[59] In recognizing therefore that protectability was a seemingly objective enterprise that entailed analyzing components of a work against a set of objective principles—such as originality, the idea-expression dichotomy, scènes-à-faire, and the like—the court adopted a two-part formulation:

> The test for infringement therefore has been given a new dimension. There must be ownership of the copyright and access to the copyrighted work. But there also must be substantial similarity not only of the general ideas but of the expressions of those ideas as well.

---

56. T-Peg, Inc. v. Vermont Timber Works, Inc., 459 F.3d 97, 116 (1st Cir. 2006) (emphasis added). It then explicitly "le[ft] to the district court the determination of whether this may be a case in which expert testimony would be helpful on the issue of substantial similarity." *Id.* (reversing the district court's decision in part for rejecting expert testimony on substantial similarity). Although *T-Peg* endorses a rule that allows use of experts in some circumstances, at least one later First Circuit opinion indicates that the issue is not fully settled. *See* Airframe Sys., Inc. v. L-3 Commc'ns Corp., 658 F.3d 100, 106 n.7 (1st Cir. 2011) ("Where, as here, the copyrighted work involves specialized subject matter such as a computer program, some courts have held that the 'ordinary observer' is a member of the work's 'intended audience' who possesses 'specialized expertise.' . . . This court has yet to directly address this issue, and it is unnecessary to do so here.") (citing *Dawson*, *Kohus, Altai*, and *Whelan*).

57. *See* Sturdza v. U.A.E., 281 F.3d 1287, 1300–01 (D.C. Cir. 2002) (noting that "[a] growing number of courts now permit expert testimony regarding substantial similarity in cases involving computer programs, reasoning that such testimony is needed due to the complexity and unfamiliarity of computer programs to most members of the public" and remanding for further development) (internal quotations omitted).

58. *See* Balganesh, *supra* note 33, at 852–55.

59. *See* Sid & Marty Krofft Television v. McDonald's Corp., 562 F.2d 1157 (9th Cir. 1977).

> Thus two steps in the analytic process are implied by the requirement of substantial similarity. . . .
>
> We shall call [the test for the similarity of ideas] the 'extrinsic test.' It is extrinsic because it depends not on the responses of the trier of fact, but on specific criteria which can be listed and analyzed. Such criteria include the type of artwork involved, the materials used, the subject matter, and the setting for the subject. Since it is an extrinsic test, analytic dissection and expert testimony are appropriate. Moreover, this question may often be decided as a matter of law. . . .
>
> The test to be applied in determining whether there is substantial similarity in expressions shall be labeled an intrinsic one — depending on the response of the ordinary reasonable person. . . .
>
> This same type of bifurcated test was announced in *Arnstein*. . . . We believe that the court in *Arnstein* was alluding to the idea-expression dichotomy which we make explicit today.[60]

In developing its own two-part formulation, *Krofft* fundamentally misunderstood the analytical basis and rationale behind the *Arnstein* test and its rules about expert testimony. Appreciating this misunderstanding requires delving a little bit deeper into the *Arnstein* test and the analytical basis of its rules.

To begin with the basics, the first step in the *Arnstein* formulation—the question of factual copying—is an entirely evidentiary question. Indeed, it is for this reason that some have referred to this step as the question of "probative similarity," to the extent that it relies on a comparison of the two works *in order to infer such copying*.[61] Yet, the question is not whether the defendant simply copied from the plaintiff's work. Instead, it is whether the defendant copied *protectable expression* from the plaintiff's work. And this is because, as a corollary of the fundamental precept of copyright law that not all copying is infringement,[62] all works contain both protectable and unprotectable elements. Indeed, this part of the test is meant to weed out the possibility that the plaintiff and defendant both drew from a common source, the public domain, or indeed altogether unprotected materials, such as ideas or unoriginal expression. It is for this reason that *Arnstein*'s reference to expert

60. *Id.* at 1164.

61. *See, e.g.*, Alan Latman, *"Probative Similarity" as Proof of Copying: Toward Dispelling Some Myths in Copyright Infringement*, 90 COLUM. L. REV. 1187, 1194–95 (1990).

62. *See* Feist Publ'ns, Inc. v. Rural Tel. Serv. Co., 499 U.S. 340, 361 (1991) ("Not all copying, however, is copyright infringement.").

testimony here is in conjunction with its mention of analytic "dissection," a reference to the process of breaking down the work into its constituent parts in order to analyze the origin and protectability of different components.[63] As should be apparent, the expert is meant to aid the court in determining just this breakdown—i.e., how much of the plaintiff's work is itself unprotected since it draws on prior sources or materials that are in the public domain. Expert testimony, in other words, aids on the question of protectability that is implicit—yet crucial—in the first step of *Arnstein*. Built into the infringement analysis is thus an implicit emphasis on protectability.

At least as framed by the court, *Krofft*'s first step—extrinsic copying—has little to do with actual copying by the defendant. All the same, even in the Ninth Circuit, and by *Krofft*'s own admission,[64] such actual copying is needed. This then reveals that in *Krofft* there is in reality a step zero, which covers a part of *Arnstein*'s first step. The Ninth Circuit refers to this as the question of "access" rather than factual copying,[65] but it is a crucial preliminary to any further analysis. Access is meant to allow courts to infer actual copying and then proceed to the question of substantial similarity, which *Krofft* breaks down into two further steps. By framing its step zero as being about access, the Ninth Circuit effectively eliminates the issue of copying from this step and, instead, merely focuses on whether the defendant had reasonable access to the plaintiff's work, regardless of what the defendant actually did with such access. To the extent that the *Krofft* test must give effect to the idea that works embody uncopyrightable elements, the extrinsic test becomes crucial.

Bringing the *Krofft* framework on parallel with the *Arnstein* test on the first step would thus imply having the extrinsic test expressly address the issue of protectability, before proceeding to a side-by-side comparison of the two works. Yet, the extrinsic test—as formulated in *Krofft*—does just the opposite. In focusing on the similarity of "ideas" and other potentially unprotectable elements (such as the "type of artwork involved, the materials used, the subject matter, and the setting for the subject"), *Krofft* sidesteps focusing on protectability.[66] Later panels of the Ninth Circuit have noted this absurdity and attempted to re-focus the extrinsic test on protectability by characterizing it as being about "objective manifestations of creativity" focused on "the measurable, objective elements that constitute . . . expression,"[67] as well as by

63. *See* Arnstein v. Porter, 154 F.2d 464, 468 (2d Cir. 1946).

64. *See Krofft*, 562 F.2d at 1163 ("The real task in a copyright infringement action, then, is to determine whether there has been copying of the expression of an idea rather than just the idea itself.").

65. *Id.* at 1172.

66. *See id.* at 1164.

67. Shaw v. Lindheim, 919 F.2d 1353, 1359 (9th Cir. 1990).

noting that "only those elements of a work that are protectable and used without the author's permission can be compared . . . ."[68] All the same, even in this reformulation the focus does not appear to be primarily on protectability. It instead emphasizes the objective breakdown of the work in order to enable a court to determine whether the similarity is sufficient to allow for a subjective comparison.

The second step in *Arnstein* focuses on wrongful copying and asks the fact-finder, i.e., ordinarily the jury, to determine whether the defendant's copying of protected expression from the plaintiff's work was sufficient in both qualitative and quantitative terms so as to amount to an infringement. Hence the test uses the phrase "wrongful" or "illicit" copying. The comparison is meant to be subjective in that the fact-finder is meant to rely on his or her perception (or equivalent sensorial facility) and intuition for the determination. With perceived similarity being the crucial touchstone of this step, the framework attempts to limit (though not prohibit) expert testimony, which could obviously influence such perception. A professional musician's ability to distinguish two musical compositions will thus obviously be different from a lay person's comparison of them, and the test strongly prefers the latter.[69] Yet it is crucial to recognize that the reason why this framework can be comfortable in relying on such subjectivity without worrying about the fact-finder's misunderstanding about the protected elements of the work is because the prior step focused entirely on protectability. In other words, the *Arnstein* framework quite neatly parses out *protectability* and *perceivable similarity* in its two steps, even if it presents other problems.

Krofft's second step replicates the subjective assessment contained in the *Arnstein* second step. It thus focuses on the perception of the works by lay fact-finders. And while it endorses *Arnstein*'s idea of keeping expert testimony out of this analysis by noting that "expert testimony [is] not appropriate,"[70] it pays little attention to the fact that the extrinsic test may not have sufficiently addressed the question of protectability. The extrinsic test's focus on "objective" elements may at times overlap with copyright's criteria for protection, but it need not have to. Finding a similarity in plot lines or characters in two works is of little use if those common elements are themselves drawn from another source. This inevitably means that the notion

68. Apple Comput., Inc. v. Microsoft Corp., 35 F.3d 1435, 1443 (9th Cir. 1994).

69. Judge Frank vividly made this point in *Arnstein v. Porter*. *See* 154 F.2d 464, 473 (2d Cir. 1946) ("The impression made on the refined ears of musical experts or their views as to the musical excellence of plaintiff's or defendant's works are utterly immaterial on the issue of misappropriation; for the views of such persons are caviar to the general—and plaintiff's and defendant's compositions are not caviar.").

70. *Krofft*, 562 F.2d at 1164.

of protectability—central to copyright—cannot be eliminated altogether from the intrinsic test. And for this, expert testimony is essential and cannot be foregone.

The *Krofft* test's conflation of protectability and perceivability remained largely manageable in practice when the dispute involved non-technical subject matter that lay audiences routinely encountered—literary works, artistic works, musical works, and the like. When it came to technical subject matter such as computer software, the problem became exacerbated. Here, like with literary works in a foreign language, lay juries are incapable of making analytical sense of the expression itself. Without being able to understand and contextualize the expression, they became forced to invariably conflate protectability and similarity. Juries had to shoot in the dark in making side-by-side comparisons of subject matter of which they had little understanding and were unlikely to have ever encountered before.

Altai recognized this problem—inherent in both the *Arnstein* and *Krofft* tests, but more trenchant in the latter—and modified the prohibition on expert testimony during comparisons of computer software. Since the Ninth Circuit never expressly endorsed (or applied) this modification in *Altai*, the circuit continues to adhere to the original formulation tracing back to *Krofft* and without any consideration of its implications for technical subject matter.[71] Therein emerged the nuttiness of the Ninth Circuit's rule.

V. *ANTONICK V. ELECTRONIC ARTS*: MANIFESTATION OF THE "NUTTY" RULE[72]

Several cases in the Ninth Circuit suggested that wooden application of the *Krofft* rule limiting the use of experts would not make much sense in software cases,[73] but it was not until *Antonick v. Electronic Arts Inc.*[74] that the Ninth Circuit

71. In *Brown Bag Software v. Symantec Corp.*, Judge Sneed noted in a concurring opinion that the Ninth Circuit precedent "provides a poor analytic structure by which to determine the substantial similarity of an allegedly infringing computer program," preferring the Third Circuit's "integrated substantial similarity test pursuant to which both lay and expert testimony would be admissible." 960 F.2d 1465, 1478 (9th Cir. 1992) (Sneed, J., concurring).

72. This Part draws on Appellant's Brief, *Antonick*, 841 F.3d 1062 (9th Cir. 2016) (No. 14-15298), 2014 WL 3909266 [hereinafter Antonick 9th Circuit Opening Brief], and Complaint, Antonick v. Electronic Arts, Inc., No. C 11–1543 CRB, 2014 WL 245018 (N.D. Cal. Jan. 22, 2014) [hereinafter Antonick Complaint].

73. *See id.*; Broderbund Software, Inc. v. Unison World, Inc., 648 F. Supp. 1127, 1136 (N.D. Cal. 1986) (suggesting that "an integrated test involving expert testimony and analytic dissection may well be the wave of the future in [computer software cases]" but noting that the Ninth Circuit's position "is clearly marked out in *Krofft*, and controls the analysis here").

74. Antonick v. Electronic Arts Inc., 841 F.3d 1062 (9th Cir. 2016).

directly confronted the admissibility of expert witness testimony in computer software cases. The backstory to this litigation is important to understanding the Ninth Circuit's surprising decisions to bar expert testimony that would enable lay jurors to compare the works at issue.

A. DEVELOPMENT OF THE MADDEN FOOTBALL VIDEO GAME

The *Antonick* case grew out of the development of Madden Football, the iconic video game that launched the sports video game industry.[75] As an industry observer aptly noted in 2013, the 25th anniversary of the game,

> From its humble beginnings on an Apple II computer in 1988 to the modern marvels now featured on PS3 and Xbox 360 (and soon to further amaze on the next generation consoles), Madden's evolution largely mirrors the evolution of video games in general. Few franchises—really, only Mario and Zelda—have had the cultural staying power and impact of Madden.[76]

Prior to Madden Football, video games were relatively primitive in their simulation of sport activities. In the early 1980s, the state of the art for video football games featured only three or five players per side due to the limitations of early microcomputers. The early games did not hold users' attention for long because the players ran predetermined routes and the outcomes were determined by static rules. In 1983, Robin Antonick, a former college football player and skilled computer programmer, conceived of a far more authentic football video game that could simulate 11-on-11 player action and sophisticated dynamic models of player behavior. He showed a prototype to William "Trip" Hawkins, founder and Chief Executive Officer of Electronic Arts (EA), then a fledging video game publisher.[77] Hawkins was impressed. Soon thereafter EA hired Antonick as an independent contractor to develop a commercial version of the game. The EA-Antonick contract provided Antonick with royalties on versions of the game that Antonick developed as well as games derived from his versions.

After that deal was signed and Antonick had begun work on the commercial version of the video game, Hawkins persuaded John Madden, former coach of the Oakland Raiders and a popular NFL broadcaster, to lend his name to the game. Antonick and Hawkins translated Madden's playbook

75. *See* John Gaudiosi, *Madden: The $4 billion video game franchise*, CNN (Sept. 5, 2013, 11:51 AM), https://money.cnn.com/2013/09/05/technology/innovation/madden-25/.

76. Timothy Rapp, *Madden 25: Rounding Up Reviews of Iconic Game*, BLEACHER REP. (Aug. 27, 2013), https://bleacherreport.com/articles/1751592-madden-25-rounding-up-reviews-of-iconic-game.

77. Trip Hawkins, a former Apple employee, founded Electronic Arts in 1982. *See generally Electronic Arts*, WIKIPEDIA, https://en.wikipedia.org/wiki/Electronic_Arts.

and play calling into computer algorithms and integrated them into the computer program.

In December 1986, EA and Antonick revised the agreement, pursuant to which Antonick would develop the newly titled "John Madden Football" videogame for the Apple II, Commodore 64, and IBM platforms.[78] In addition to receiving compensation for those "Works,"[79] Antonick would be entitled to royalties on all "Derivative Works," defined as:

> any computer software program or electronic game which either (a) constitutes a derivative work of the Work within the meaning of the United States copyright law or (b) produces audiovisual effects which infringe the copyright in the audiovisual effects produced by the Work. Derivative Works include, for example, significant enhancements of the Work to add additional features or improve performance and adaptations of the Work to operate on computers or operating systems other than those described in the Specifications.[80]

EA also promised to (1) protect against unauthorized use of Antonick's intellectual property, including his Development Aids,[81] and (2) offer Antonick a right of first refusal to develop Derivative Works.

Over the next two years, Antonick developed the computer source code for the original John Madden Football video game, which was implemented on the Apple II computer ("Apple II Madden"). Antonick's game took the sports video game genre from primitive abstract games with few players and simple actions to sophisticated simulation of multi-faceted, 11-on-11 football action integrating player data, complex strategies, and user manipulation of player controls.

In February 1987, Antonick and EA executed Amendment I to the 1986 Contract. Among other things, Antonick agreed to a higher royalty rate on sales of Works and "Derivative Works by Artist" and, depending on the microprocessor used, a lower or higher royalty rate on "Derivative Works by Publisher." Antonick was to receive a royalty for any Derivative Work in the same "Microprocessor Family" as the Apple II's microprocessor. Amendment I limited Antonick's right of first refusal to Derivative Works developed for certain Microprocessor Families, but also provided that if Antonick developed

78. *See* ELEC. ARTS, INC., SOFTWARE DEVELOPMENT AND PUBLISHING AGREEMENT § 4 [hereinafter 1986 Contract].

79. *Id.* at § 5.

80. *Id.* at Exhibit A § 1.03 (defining "Derivative Work").

81. "Development Aids" included "equipment, firmware, and software utilities . . . used or developed by [Antonick] which might be useful . . . in developing any Derivative Work." *Id.* at Exhibit A § 5.05.

a Derivative Work for a "new" Microprocessor Family, his right of first refusal would be revived with respect to that family. Finally, EA promised "not to use or otherwise provide" Antonick's Development Aids to employees or third parties in preparing Derivative Works on different microprocessor families.

As a means of simulating actual National Football League games, Antonick integrated the physics of player and ball movement with a player ratings model based on multiple attributes. Drawing on his football knowledge, Antonick combined the player ratings structure with an elaborate system of hundreds of offensive and defensive plays. After EA signed John Madden to collaborate and lend his name to the game, Antonick adapted and refined the existing plays and play-calling to incorporate Madden's ideas.

Around that time, Richard Hilleman, an EA employee, joined the project as the Apple II Madden producer. Antonick spoke with Hilleman regularly, discussing, among other things, the execution of game features and solutions to implementation issues.

Pursuant to the agreements, Antonick was required to deliver detailed documentation of his code and other intellectual property, including (1) "complete assembled source code with sufficient comments to allow the easy understanding of each routine, subroutine and table by an individual conversant with 6502 assembly language"; (2) "an overall program description, including the file name of each module of code," "a narrative of the flow of control," "a complete list of subroutines with a short description of each," and "an explanation of key data structures"; and (3) a description of "any firmware or software utilities used."[82]

In 1988, EA released Apple II Madden. According to EA, the game was an "overnight success" that "exceeded its high expectations" and "went on to sell more copies than any other sports game of its time."[83] On the heels of this acclaim, Antonick programmed Madden games for the Commodore 64 and IBM-compatible computer platforms. In 1989, he began work on Madden games for the Nintendo and Sega Genesis entertainment systems. In October 1989, Antonick and EA entered into Amendment VIII to the 1986 Contract, requiring Antonick to develop a "script" and a technical design review for Sega Genesis and Nintendo versions and providing that Antonick would receive "additional compensation" in the form of 3% royalties on sales of any "Nintendo Derivative Work" or "Sega Genesis Derivative Work." As

82. *See* Antonick 9th Circuit Opening Brief, *supra* note 72, at 9–10.

83. Plaintiff's Opposition to Electronic Arts' Second Motion for Summary Judgment at 5, Antonick v. Elec. Arts Inc., No. 3:11-CV-01543-CRB (Document 224) [hereinafter Plaintiff's Opposition to Second MSJ].

producer on the Nintendo version, Hilleman reviewed Antonick's design script and discussed Antonick's ideas for console games.

In an abrupt shift of course, Hilleman told Antonick in August 1990 that EA had decided not to publish Derivative Works for Nintendo or Sega Genesis.[84] Instead, Hilleman said that EA was going in a different direction with a Sega Genesis game with "more of an arcade style." Hilleman said that EA had already hired another company, Park Place Productions, to develop the new Sega game "independently" of Antonick's work. Because there would be a separation between Antonick's work and the development of the Sega game, Antonick would have no royalty or other rights in the Sega game. Hilleman also told Antonick that the "Nintendo marketplace had started to disintegrate" and to stop working on Nintendo Madden.

Just three months later—barely in time for the holiday shopping season—EA released its first version of Sega Madden.[85] EA continued to issue Madden games for Sega Genesis, Super Nintendo, and other platforms annually since 1992. After Antonick completed the second IBM game in 1992, his work with EA was substantially over, and he moved on to other projects. EA's Madden Football franchise would go on to remarkable sustained success, racking up billions of dollars in revenue.[86]

B. ANTONICK'S DISCOVERY THAT EA BASED SEGA MADDEN ON APPLE II MADDEN

In conjunction with its celebration of Madden Football's twentieth anniversary in 2009, EA released publicity materials describing the game's history. To Antonick's surprise, the materials traced the Sega Madden to Antonick's Apple II Madden version. Antonick viewed a CNBC interview of Trip Hawkins, who also connected the design and coding of the later editions of the Madden Football video game software franchise back to Apple II Madden. Antonick looked further into the matter and discovered on the website of Park Place co-founder Troy Lyndon that he credited EA's Hilleman with helping to develop 1990 Sega Madden, noting that Hilleman spent "countless hours" with Park Place programmer Jim Simmons to make the game more realistic. Antonick then realized that, contrary to Hilleman's assurances in 1990, Sega Madden had not been developed independently of

84. *Id.* at 7–9.

85. *See* Transcript of Proceedings at 478, *Antonick*, No. 3:11-CV-01543-CRB [hereinafter Trial Transcript].

86. By 2013, EA had sold more than 100 million copies of Madden NFL, generating more than four billion dollars in total sales. *Madden NFL*, WIKIPEDIA, https://en.wikipedia.org/wiki/Madden_NFL (last visited Sept. 4, 2020).

Apple II Madden.[87] Hilleman, who had worked on Apple II Madden and had intimate knowledge of its design and code, apparently played a direct and critical role in developing Sega Madden.

Antonick alleged that until these revelations, he had no reason to question EA's account of how Sega Madden was developed. The Sega Genesis gaming platform had a more powerful microprocessor than the Apple II resulting in a more realistic visual simulation. Therefore, the Madden Sega screen displays differed substantially from the Madden Apple II visual appearance.[88] Yet the underlying code could well have been derived from Madden Apple II. Antonick did not have access to the Sega Madden source code and therefore could not have assessed the extent to which Park Place based Sega Madden on Apple II Madden's software code and design.

As a result of the 2009 information, Antonick became suspicious that Park Place had not, as EA informed him, developed Sega Madden independently. EA had assured Antonick that it would safeguard his source code and design documents, and would ensure that the development of any subsequent works that were outside of the "derivative works" definition would only be produced using a "clean room" process.[89] Growing out of a seminal copyright case involving Sega,[90] the software industry came to follow a "clean room" process for independently developing interoperable software,[91] but the 2009

87. In a November 2009 interview, Lyndon stated that "Hilleman came down to our office and liver there for well over a month with Simmons turning something that looked good into something that actually played great football." Antonick Complaint, *supra* note 72, at ¶ 77.

88. The parties stipulated that "[p]laying or viewing a John Madden Football video game for the Sega Genesis or Super Nintendo would not have allowed the person looking at the screen or playing the game to determine how a particular game element was expressed in source code." Trial Transcript, *supra* note 85, at 466.

89. Antonick Complaint, *supra* note 72, at ¶¶ 59–65.

90. *See* Sega Enters. Ltd. v. Accolade, Inc., 977 F.2d 1510 (9th Cir. 1992) (holding that reverse engineering of copyrighted software to discover its unprotected features constitutes fair use).

91. The "clean room" process was formalized during the first wave of software copyright litigation as a means of developing interoperable software and ensuring that proprietary materials do not infect software development. The clean room process typically involves three teams of engineers and legal specialists. The first team—referred to as the "specification" or "dirty room" team—works with the target software to determine the functional specifications. A second "coordination" or "audit" team, comprised of attorneys and engineers, establishes clear ground rules for managing the clean room process, screens programmers for the "clean room" team so as to ensure they have never seen the copyright-protected code, documents the activities and communication of the "dirty room" and "clean room" teams, oversees the process, and advises on what constitutes functional specifications and how to determine code segments that are unprotectable—segments that are unoriginal, standard programming practices, and necessary for interoperability or to accomplish specific processes or methods.

revelations appeared to contradict EA's assurances that Sega Madden was not derived from Antonick's work product.[92] EA was entitled to pursue such derivative works, but was required pursuant to its contracts with Antonick to pay him an ongoing royalty.

C. ANTONICK'S COMPLAINT AND THE COPYRIGHT INFRINGEMENT ISSUE

In March 2011, Antonick filed suit against EA alleging breach of contract and fraud.[93] The complaint implicated copyright law through the clause of the Antonick-EA contact that entitled Antonick to royalties if subsequent versions of Madden Football "constitute[] a derivative work of [Apple II Madden] within the meaning of the United States copyright law."[94] The contract defined "Derivative Works" to include, for example, "significant enhancements of the Work to add additional features or improve performance and adaptations of the Work to operate on computers or operating systems other than those described in the Specifications."[95] Hence, the Antonick contract cause of action turned on whether Sega Madden was derived, the copyright sense, from Apple II Madden.

The Copyright Act defines a "derivative work" as

> a work based upon one or more preexisting works, such as a translation, musical arrangement, dramatization, fictionalization, motion picture version, sound recording, art reproduction, abridgment, condensation, or any other form in which a work may

---

The coordination team seeks to ensure that no copyright-protected expression or misappropriated trade secrets get communicated to the clean room team. It is only after those checks are completed that the process of independently coding an interoperable program commences. The functional specifications detailing the particular processes or results that the target program accomplishes is then passed to the "clean room" team of programmers. This team remains shielded from the copyright-protected code. It designs, writes, and tests code aimed at accomplishing the target functional specifications. *See* Jorge Contreras, Laura Handley & Terrence Yang, NEC v. Intel: *Breaking New Ground in the Law of Copyright*, 3 HARV. J.L. & TECH. 209 (1990); G. Gervaise Davis III, *Scope of Protection of Computer-Based Works: Reverse Engineering, Clean Rooms and Decompilation*, 370 COMPUT. L. INST. 115 (PLI Patents, Copyrights, Trademarks, and Literary Property Practice Course Handbook Series No. G-370, 1993); Menell, *supra* note 39, at 448–49; P. Anthony Sammi, Christopher A. Lisy & Andrew Gish, *Good Clean Fun: Using Clean Room Procedures in Intellectual Property Litigation*, 25 INTELL. PROP. & TECH. L.J. 3 (2013).

92. *See* Plaintiff's Opposition to Second MSJ, *supra* note 83, at 9–12.

93. *See* Antonick Complaint, *supra* note 72; John Gaudiosi, *Madden Creator Sues Electronic Arts for Millions in Royalties*, FORBES (Apr. 1, 2011, 5:39 PM), https://www.forbes.com/sites/johngaudiosi/2011/04/01/madden-creator-sues-electronic-arts-for-millions-in-royalties/#cbfdcba4d32a.

94. Antonick Complaint, *supra* note 72, at 7.

95. *Id.*

> be recast, transformed, or adapted. A work consisting of editorial revisions, annotations, elaborations, or other modifications which, as a whole, represent an original work of authorship, is a "derivative work."[96]

Courts base the determination of whether a subsequent work constitutes a derivative work on whether it violates the right to reproduce, i.e., whether it is an infringement of the copyrighted work.[97] Therefore, the key legal issue was whether Sega Madden infringed Apple II Madden.

D. PRE-TRIAL PROCEEDINGS: IMPROPER WHITTLING OF THE PLAINTIFF'S BASIS FOR SHOWING THAT EA DERIVED SEGA MADDEN FROM APPLE II MADDEN

The case was ultimately assigned to Judge Charles Breyer of the Northern District of California. EA sought to dismiss the complaint on the ground that Antonick waited too long to file suit. Judge Breyer denied EA's motion to dismiss and ordered the case to be tried in three phases: (1) EA's statute of limitations defense; (2) EA's liability with respect to Madden games released before 1996; and (3) EA's liability with respect to non-Madden games[98] and post-1996 Madden games.[99] Phases (1) and (2) were to be done seriatim with the same jury. Phase 3, if necessary, would follow at a later time.[100]

In view of the technical and legal complexity of the case, the parties engaged in extensive discovery disputes and motion practice. Remarkably, EA failed to locate complete copies of the source code for Apple II Madden and early versions of Sega Madden. Nonetheless, Antonick had retained source code for versions of the games that he designed and other documentation, including a sixty-page game manual detailing the Apple II Madden design. He

96. 17 U.S.C. § 101 (defining "derivative work").

97. *See* Litchfield v. Spielberg, 736 F.2d 1352, 1354 (9th Cir. 1984) (holding that a work is derivative "*only if it would be considered an infringing work if* the material which it has derived from a prior work had been taken without the consent of the copyright proprietor of such prior work" (emphasis in original) (citing United States v. Taxe, 540 F.2d 961, 965 n.2 (9th Cir. 1976))); MELVILLE NIMMER, 2 NIMMER ON COPYRIGHT § 8.09[A][1] (2019) (suggesting that right to prepare derivative works is superfluous in that "[u]nless enough of the pre-existing work is contained in the later work to constitute the latter an infringement of the former, the latter, by definition, is not a derivative work").

98. Antonick alleged that other EA sports games, such as NCAA Football and NHL Hockey, also constituted derivative works of Apple II Madden for which royalties should have been paid. *See* Antonick Complaint, *supra* note 72, at 23.

99. *See* Antonick v. Elec. Arts, Inc., 841 F.3d 1062, 1065 (9th Cir. 2016) (noting the trial phases).

100. *See id.*; Antonick 9th Circuit Opening Brief, *supra* note 72, at 16; Eriq Garner, *Electronic Arts Faces Jury Trial over 'Madden NFL'*, HOLLYWOOD REP. (Apr. 26, 2013, 10:42 AM), https://www.hollywoodreporter.com/thr-esq/electronic-arts-faces-jury-trial-447243.

retained Michael Barr, an experienced computer engineering expert.[101] Barr prepared a detailed report analyzing Antonick's source code files, source code and EA's technical files containing source code for eight distinct versions of Madden football games for Sega Genesis and Super Nintendo, as well as various documents, declarations, discovery responses, and depositions.[102]

Antonick alleged that Simmons, Park Place's lead programmer, was woefully behind schedule producing Sega Madden and called in EA's Hilleman, who was intimately familiar with Antonick's design and code, in order to meet the tight production deadline. Antonick also alleged that although Sega Madden was written in a different assembly code language for the Sega Genesis console (which used the Motorola 68000 microprocessor as opposed to the Apple II's MOS Technology 6502 microprocessor),[103] Simmons and his team followed the Apple II Madden design down to the non-standard field dimensions,[104] player directional tracking system,[105] particular play routes, naming (including misspellings) and ordering of plays, player rating model, decision points, data flow architecture, and game engine design (e.g., representation of ball carrier positioning and player pursuit, use of randomness in conjunction with player ability to introduce variable uncertainty). Barr's analysis showed that Sega Madden's compilation of features, as well as sub-feature design, choice, and particular code elements, were substantially similar to Apple II Madden.

In response, EA sought to whittle down Antonick's basis for proving that Sega Madden was a derivative work through summary judgment motions, motions *in limine*, and jury instructions. Drawing on inapt lines of cases limiting the scope of copyright protection for *general* functional features of computer

101. *See* Michael Barr, Expert Resume, Antonick, v. Elec. Arts Inc., No. 3:11-cv-01543-CRB (N.D. Cal. Jan. 22, 2014), 2012 WL 7160593.

102. *See* Fed. R. Civ. P. 26(a)(2)(B); Report of Michael Barr at Exhibit B, *Antonick*, No. 3:11-cv-01543-CRB [hereinafter "Barr Report"] (explaining "[t]he source code for a pair of programs written in different assembly languages will look very different to the casual observer—even if they do the very same things—just as a pair of contracts for the same purpose but written in German and Spanish will appear visually different") (under seal).

103. *See* Barr Report, *supra* note 102, at 18, 27–29.

104. Whereas the NFL uses a field width of 53.33 yards, Antonick used an 80-yard width. This feature carries over to many aspects of the coding and representation of the video game as the game players, unlike actual NFL players, will move more quickly up and down the field than they will laterally.

105. Barr opined that the use of the same directional tracking system made it easier for Park Place to emulate many other aspects of Antonick's game design, subroutines, and coding. *See* Barr Report, *supra* note 102, at 51.

software,[106] EA persuaded Judge Breyer to restrict the basis for asserting similarity to two of the ten elements that Antonick sought to use in showing that Sega Madden constituted a derivative work of Apple II Madden: (1) non-standard field width and (2) plays and formations.[107] Thus, the court severely impeded Antonick's core compilation theory, but the granular design and coding decisions relating to plays and formations left some room for pursuing the derivative work case. Further stacking the deck in EA's favor, Judge Breyer drew on another line of inapt cases[108] to require that Antonick prove not merely that Sega Madden was substantially similar to Apple II Madden, but that it was *virtually identical*.[109]

These rulings fundamentally misconstrued applicable copyright principles. Copyright law protects original compilations of even individually unprotectable elements.[110] Although all of the individual words in a language are unprotectable, copyright law robustly protects the compilation that

106. *See* Incredible Techs., Inc. v. Virtual Techs., Inc., 400 F.3d 1007 (7th Cir. 2005) (involving an independently developed video golf game); Apple Comput., Inc. v. Microsoft Corp., 35 F.3d 1435 (9th Cir. 1994) (involving a microcomputer graphical user interface using a desktop metaphor, much of which was licensed to the defendant); Data East USA, Inc. v. Epyx, Inc., 862 F.2d 204 (9th Cir. 1988) (involving an independently developed video karate game); Oracle Am., Inc. v. Google Inc., 872 F. Supp. 2d 974 (N.D. Cal. 2012) (involving the declarations necessary for interoperability). We explain further below why these cases are inapt. *See infra* text accompanying notes 115–118.

107. *See* Jury Instructions at 5–6, *Antonick*, No. 3:11-cv-01543-CRB (Document 509) [hereinafter Jury Instructions]; Phase Two Pretrial Order, *Antonick*, No. 3:11-cv-01543-CRB (Document 460), 2013 WL 9774980; Memorandum and Order re Defendant's Third Motion for Summary Judgment, *Antonick*, No. 3:11-cv-01543-CRB (N.D. Cal. Jan. 22, 2014) [hereinafter Third MSJ Order] (sealed).

108. *See* Mattel, Inc. v. MGA Entm't, Inc., 616 F.3d 904 (9th Cir. 2010); *Incredible Techs.*, 400 F.3d 1007; Satava v. Lowry, 323 F.3d 805 (9th Cir. 2003); Apple Comput., Inc. v. Microsoft Corp., 35 F.3d 1435 (9th Cir. 1994); Harper House, Inc. v. Thomas Nelson, Inc., 889 F.2d 197 (9th Cir. 1989); *Data East USA*, 862 F.2d 204. We explain below why these cases are inapt. *See infra* text accompanying notes 123–125.

109. *See* Jury Instructions, *supra* note 107, at 6 (instructing the jury that Antonick "must prove by a preponderance of the evidence that considering Sega Madden as a whole—that is, considering both the protected and unprotected elements—an ordinary reasonable observer would find Sega Madden *virtually identical* to Apple II Madden" (emphasis added)); Third MSJ Order, *supra* note 107.

110. *See* 17 U.S.C. § 103 (protecting compilations); 17 U.S.C. § 101 (defining a "compilation" as "a work formed by the collection and assembling of preexisting materials or of data that are selected, coordinated, or arranged in such a way that the resulting work as a whole constitutes an original work of authorship"). *See generally* MELVILLE NIMMER, 1 NIMMER ON COPYRIGHT § 3.04[B] (2019) (discussing the legal standard for protection of compilations); Eng'g Dynamics, Inc. v. Structural Software, Inc., 26 F.3d 1335 (5th Cir. 1994) (finding an original compilation of otherwise uncopyrightable components to be protected); Kregos v. Associated Press, 937 F.2d 700 (2d Cir. 1991) (finding the format of baseball form containing pitching statistics copyrightable).

comprises a novel. Similarly, although copyright law does not protect individual colors, copyright generally subsists in paintings comprising an original compilation of colors. In the computer software context, even though individual 1's and 0's of object code and general processes and algorithms are not copyrightable, original compilations of specific coding and design choices are generally protectable, unless there is only one or a few ways of accomplishing the functional task.[111] The robustness of copyright protection for computer programs—their thickness or thinness—depends, as in other copyrightable works, on the range of expressive choice.[112] The design and coding of a very intricate video game, such as Apple II Madden, attracts significant copyright protection as a compilation of protectable and unprotectable elements, even though particular names, plays, directional tracking designs, and decision points are individually unprotectable. And even though the rules of football cannot be monopolized through copyright protection, the compilation of particular ways that they are implemented in a sophisticated software product can be copyrightable.

Even after the first football video game is published, others are free to independently develop their own football video games, but they are not free to copy highly particularized design and coding choices of the first comer without authorization. Nor can they develop sequels or more advanced versions that draw significantly upon on the granular design and coding elements of the original work.[113] Second comers usually lack access to the source code, which is typically not publicly released. Video game publishers typically protect their source code as trade secrets. They distribute their games

111. *See* NAT'L COMM'N ON NEW TECH. USES OF COPYRIGHTED WORKS, FINAL REPORT 18-21 (1979). Courts have treated this report as legislative history to the 1980 amendments to the 1976 Act. *See* Vault Corp. v. Quaid Software Ltd., 847 F.2d 255, 260–61 (5th Cir. 1988); Apple Comput., Inc. v. Franklin Comput. Corp., 714 F.2d 1240, 1252 (3d Cir. 1983).

112. *See* Shyamkrishna Balganesh, *The Normativity of Copying in Copyright Law*, 62 DUKE L.J. 203, 221–26 (2012) (discussing thickness as a variable in copyright infringement analysis).

113. The language in the EA-Antonick contract arguably went further than copyright law's derivative work right in stating that "derivative works" "include, for example, significant enhancements of the Work to add additional features or improve performance and adaptations of the Work to operate on computers or operating systems other than those described in the Specifications." *See* 1986 Contract, *supra* note 78. Based on the contract's preceding sentence stating that "derivative works" for which royalties were due "constitute[] a derivative work of [Apple II Madden] within the meaning of the United States copyright law," Judge Breyer accorded no weight to the express enhancement example in the contract. *Id.* This interpretation was questionable as the scope of the derivative work right under the 1976 Act was somewhat ambiguous at the time that the contract was drafted, and the enhancement example provides a concrete indication of the parties' intent.

in object code format from which it is very difficult to decipher the source code.[114]

EA drew Judge Breyer off-course by focusing on software cases that fundamentally differed from the alleged copying that occurred in the *Antonick* case. In *Data East USA, Inc. v. Epyx, Inc.*,[115] and *Incredible Technologies, Inc. v. Virtual Technologies, Inc.*,[116] the plaintiff sought to monopolize karate and golf video games, respectively, by seeking to block *independently* developed video games based on the general rules of these sports as well as general hardware and software constraints. In *Oracle America, Inc. v. Google Inc.*, Oracle seeks to protect arguably unprotectable declarations necessary for computer system interoperability.[117] And in *Apple Computer, Inc. v. Microsoft Corp.*, Apple sought to block Microsoft and others to whom it licensed many elements of its graphical user interface from implementing the desktop metaphor for organizing microcomputer screen layout and functionality.[118]

While all of these cases are important to understanding the general contours of copyright protection for computer software, they differ fundamentally from the issues raised in *Antonick v. Electronic Arts*. In *Data East* and *Incredible Technologies*, the defendants *independently developed* their software from scratch; they had no access to the source code or particular design architecture of the plaintiff's software. Furthermore, unlike *Antonick v. Electronic Arts*, those cases related to audiovisual elements, not the underlying code. The games appeared similar to the plaintiffs' works because they followed the rules and context of the sport (soccer or golf) and general software and video game principles. In *Oracle v. Google*, Google *independently implemented* the source code using only the declarations necessary for interoperability.[119] And in *Apple v. Microsoft*, a prior licensing agreement

114. Trade secret protection, however, is not absolute. Trade secret law does not bar reverse engineering. *See* Peter S. Menell, *Tailoring Legal Protection for Computer Software*, 39 STAN. L. REV. 1329, 1351–53 (1987). Competitors can at times (but often at great cost) reverse engineer the functional specifications of computer programs. They can use those functional specifications to produce interoperable or otherwise competing products without violating copyright law. *See* Sega Enters. v. Accolade, Inc., 977 F.2d 1510 (9th Cir. 1992); Donald S. Chisum, Rochelle Cooper Dreyfuss, Paul Goldstein, Robert A. Gorman, Dennis S. Karjala, Edmund W. Kitch, Peter S. Menell, Leo J. Raskind, Jerome H. Reichman & Pamela Samuelson, *LaST Frontier Conference on Copyright Protection of Computer Software*, 30 JURIMETRICS J. 15, 23–25, 32 (1989).

115. Data East USA, Inc. v. Epyx, Inc., 862 F.2d 204 (9th Cir. 1988).

116. Incredible Techs., Inc. v. Virtual Tech., Inc., 400 F.3d 1007 (7th Cir. 2005).

117. *See* Menell, *supra* note 40, at 376–89.

118. *See* Apple Comput., Inc. v. Microsoft Corp., 799 F. Supp. 1006 (N.D. Cal. 1992), *aff'd in part, rev'd in part*, 35 F.2d 1435 (9th Cir. 1994).

119. *See* Menell, *supra* note 40, at 366–67.

afforded the defendants use of many of the elements of Apple's graphical user interface. Furthermore, the desktop metaphor for a user interface was both obvious and developed originally by Xerox for its Star workstation.[120] Apple's design team based the Apple Lisa and Apple Macintosh on the Xerox Star design and Smalltalk, an object-oriented programming language also developed at Xerox's Palo Alto Research Center (PARC).[121] Moreover, Apple hired Larry Tesler, one of the developers of the Xerox Star, to join the Apple development team.[122] None of these cases involved an insider with access to source code.

By contrast, the central issue in *Antonick v. Electronic Arts* was whether EA and Park Place used Antonick's detailed program design, documentation, and source code in developing Sega Madden. Simmons allegedly had unfettered access to Antonick's design documents and code, and he received guidance and supervision from Hilleman and other EA employees intimately familiar with Antonick's granular programming choices. Under impossibly tight time-to-market pressure, EA and Park Place's inexperienced programmer took shortcuts—copying protectable design and coding elements—to complete in three months what Antonick's experienced team had taken four years to accomplish.

EA also drew Judge Breyer off-course on the standard for similarity by focusing on cases involving simple, narrowly protected elements, none of which involved the sophisticated, granular, integrated design and coding choices involved in the Madden football video games. *Harper House, Inc. v. Thomas Nelson, Inc.*,[123] involved the largely standardized visual layout of a day planner (comprising a calendar and ruled lines). *Data East* and *Incredible Technologies* solely involved the *conventional audiovisual elements* for karate and golf videogames. *Apple Computer, Inc. v. Microsoft Corp.* involved largely unoriginal (and licensed) graphical office icons. *Satava v. Lowry*,[124] involved a jellyfish sculpture encased in a domed glass cylinder. And *Mattel, Inc. v. MGA*

120. *See Xerox Star*, WIKIPEDIA, https://en.wikipedia.org/wiki/Xerox_Star (last visited Aug. 30, 2020).

121. Members of the Apple Lisa engineering team saw Star at its introduction at the 1981 National Computer Conference and converted their desktop manager to an icon-based interface modeled on the Star. Chris Morgan, *An Interview with Wayne Rosing, Bruce Daniels, and Larry Tesler*, 2 BYTE 90, 108 (1983); *Smalltalk*, WIKIPEDIA, https://en.wikipedia.org/wiki/Smalltalk (last visited Aug. 30, 2020)

122. John Markoff, *Lawrence Tesler, who Made Personal Computing Easier, Dies at 74*, N.Y. TIMES (Feb. 20, 2020), https://www.nytimes.com/2020/02/20/technology/lawrence-tesler-dead.html; *see also Larry Tesler*, WIKIPEDIA, https://en.wikipedia.org/wiki/Larry_Tesler (last visited Aug. 30, 2020).

123. Harper House, Inc. v. Thomas Nelson, Inc., 889 F.2d 197 (9th Cir. 1989).

124. Satava v. Lowry, 323 F.3d 805 (9th Cir. 2003).

Entertainment, Inc.,[125] involved a "sculpt" for human-based dolls with enlarged facial features and feet. None of these cases involved anywhere near the complexity and range of choice reflected in the Apple II Madden video game.

Consequently, the court should not have elevated the standard for similarity. While the court was correct in filtering out unprotectable elements as *separate* bases for infringement, it erred in effectively blocking the core of Antonick's compilation infringement allegation. The full Barr Report provided just that type of analysis. He examined both the Apple II Madden compilation forest and the particularized trees.[126] Judge Breyer's severe whittling of the case excluded not only most of the trees but also the forest.

Copyright law does not work that way. Novelists can enjoin those who reproduce their compilation of unprotectable words and artists can enjoin those who reproduce their compilation of unprotectable colors. By treating *Antonick v. Electronic Arts* like cases in which software developers independently produce competing sports video games without access to the underlying code, visual artists take only the idea and not the particularized expression for an artistic work (e.g., a jelly fish encased in a glass dome or a doll with pronounced facial features and feet), and a mobile phone developer uses unprotectable code necessary for interoperable sub-systems and implements the operating system in a clean room, Judge Breyer improperly ripped the heart out of the plaintiff's case.

E. JURY TRIAL: VERDICTS FOR ANTONICK

The statute of limitations trial commenced on June 17, 2013.[127] EA contended that Antonick waited too long to file his lawsuit. Antonick countered that he only became aware of the alleged breach of contract as a result of Hawkins' revelations during the Madden Football 20th anniversary celebration. After several days of proceedings, the jury unanimously found that Antonick did not discover or know of facts that would have caused a reasonable person to suspect that EA had breached its 1986 contract with Antonick before November, 21, 2005, and therefore the statute of limitations did not bar the case.[128]

After a two-week hiatus to prepare for the liability phase, the parties presented their opening arguments on July 9, 2013, to the same jury. Both

125. Mattel, Inc. v. MGA Ent., Inc., 616 F.3d 904 (9th Cir. 2010).

126. *See generally* Barr Report, *supra* note 102.

127. *See* Beth Winegarner, *EA Can't Sink 'Madden' Royalties Suit in Jury Trial*, LAW360 (June 21, 2013, 7:32 PM), https://www.law360.com/articles/452353.

128. *See* Special Form of Verdict, Antonick v. Elec. Arts Inc., No. C 11-1543 CRB (N.D. Cal. Jan. 22, 2014) (Document 441), 2013 WL 12183203.

parties (and Judge Breyer) recognized that software experts would be needed for the jury to understand computer programming and software code. During her opening statement, EA's lead counsel displayed some source code from Sega Madden and forthrightly acknowledged that "[t]here are people who can read it. I cannot."[129]

Antonick constructed his argument that Sega Madden was derived from Apple II Madden on circumstantial and direct forms of evidence.[130] Antonick contended that the only way that Park Place could have produced the fully functional, highly sophisticated Sega Madden football video in just a few months was by translating Antonick's binary play data[131] into source code for the Sega Genesis 68000 microprocessor. Antonick emphasized the painstaking effort required to produce well-functioning, bug-free code for a sophisticated football video game,[132] and Antonick reinforced his derivative work contention by showing Simmons' lack of prior experience playing football or programming football video games[133] and EA's failure to provide any credible explanation for how Simmons obtained or developed the critical play data.[134]

129. Trial Transcript, *supra* note 85, at 649 ll. 5–6.

130. The court instructed the jury that "[e]vidence may be direct or circumstantial. You should consider both kinds of evidence. The law makes no distinction between the weight to be given to direct or circumstantial evidence. It is for you to decide how much weight to give to any evidence." *Id.* at 2053 ll. 2–6.

131. Judge Breyer ultimately instructed the jury that "the term source code includes binary files." *Id.* at 2055 ll. 19–20.

132. *See id.* at 675–79 (Michael Kawahara), 741–57 (Robin Antonick). Kawahara testified that a particular defensive play took over a week to create, test, and tune. *See id.* at 677 l. 25, 678 l. 1. Antonick testified that it would take "days and possibly more than a week" to test a single play against all 81 defensive plays, *id.* at 749 l. 25, 750 l. 1, and "we had to log hundreds of hours of testing per play to be able to get to the point where we felt confident that that play was executing up to the norms that we had—that standard that we had set for the ultimate NFL simulation," *id.* at 753 ll. 10–13.

133. *See id.* at 1643 ll. 17–25 (Jim Simmons). EA sought to work with Park Place on Sega Madden because it had produced the successful "Monday Night Football" video arcade game (MNF). *Id.* at 1245 ll. 2–12 (Richard Hilleman). EA thought that Scott Orr, the lead programmer for MNF, would be leading the Sega Madden team. *See id.* at 976 ll. 21–23 (Scott Orr) (testifying that he designed MNF in 1989), 2064 ll. 11–21 (referring to Exhibit 133, a Park Place planning document for SEGA Football noting Scott Orr was to provide play data). Orr, however, only wrote the high-level script for Sega Madden and declined to code the game. *See id.* at 1591 l. 10, 1661 l. 7–1662 l. 6 (Jim Simmons). EA's Hilleman complained about Park Place's shift in staffing for Sega Madden as a "bait and switch." *Id.* at 1157 l. 17. Antonick contended that Simmons lacked the football and video football coding experience to handle the responsibilities assigned to him and that he was chosen principally because he was a high school buddy of Troy Linden, Park Place's CEO. *See id.* at 1584 ll. 4–6 (Jim Simmons).

134. According to assistant producer Michael Brook, Sega Madden had "[n]o plays, nothing. No play calling." as late as July 1990 for a game that was published in November 1990. *Id.* at 1557 l. 20.

Antonick suggested that EA employees with access to Antonick's code—likely Michael Brook, EA's Associate Producer for Sega Madden, and Richard Hilleman—provided Simmons with the critical source code (and play data) needed for Park Place to get Sega Madden to function properly.[135] EA conceded that it had access to Antonick's source code.[136]

Antonick offered evidence that EA rushed Sega Madden to market as part of plan to sabotage Sega's efforts to gain a strong position in the emerging video football marketplace. This entailed showing that Trip Hawkins duped Sega into thinking that EA's development of Sega's Joe Montana video football game—a competing game on the Sega Genesis platform—would use innovations planned for Sega Madden.[137]

Antonick called upon Michael Barr, its principal software expert, to explain the design and coding of the two video games.[138] Barr generally explained how embedded systems, like the Apple II and the Sega Genesis, function.[139] He also generally discussed programming languages, coding of embedded systems, compilers, and the distinction between source code and executable code that computer systems can process.[140]

Barr then explained the files that he had been provided for analyzing the source code in the case[141] and how he went about deciphering the code bases and design elements to gain insight into the extent to which the field width, plays, and formations in Sega Madden were derived from Apple II Madden. He used demonstrative examples from his expert report to illustrate the similarities that the different code languages and data structures would otherwise obscure. This in part involved explaining hexadecimal (base-16) representation of numerical information.[142] Through his deciphering of code, Barr was able to show numerous examples of code and play data that were similar or identical in Apple II Madden and Sega Madden. These examples were then illustrated to the jury using demonstrative exhibits.

Figure 1 (demonstrative Exhibit 485) illustrated how the internal numbering of offensive plays in 1990 Sega Madden matched the numbering, selection, and arrangement of plays in Apple II Madden.[143] The 1990 edition of Sega Madden had fewer plays than Apple II Madden, but it drew almost

135. *See id.* at 1557–58 (Michael Brook), 1659 ll. 8–16, 1664–67 (Jim Simmons).
136. *See id.* at 2062 ll. 8–12.
137. *See id.* at 1715–19, 1748–50 (Trip Hawkins).
138. *See id.* at 1295–1325, 1342–1456, 1475–90.
139. *See id.* at 1299–1303.
140. *See id.* at 1303–05.
141. *See id.* at 1305–12.
142. *See id.* at 1322–23.
143. *See id.* at 1362–71.

entirely from the eighty-one offensive plays in Apple II Madden and used a nearly identical internal numbering system.

Figure 1: Comparison of Football Play Names and Order in Apple Madden and Sega Madden

Apple	Sega	Apple	Sega	Apple	Sega
10 Series		**40 Series**		**70 Series**	
11 I H15 **LEAD**	fb **lead**	41 F F63 HOE	fb trap left	71 P COMEBACK	
12 I F66 ODD	hb pull	42 F F61 MAN		72 P TURN IN	
13 I H16 **LEAD**	fb **lead** right	43 F F54 **CNTR**	fb **counter**	73 P STREAKS	
14 I F61 MAN	hb cut left	44 F F69 BOOM	fb lead	74 E F19 BILL	
15 I H18 BOB	fb cut right	45 F F51 MAN		75 E H30 LOG	
16 I P61 PASS	flood left	46 F H48 EVEN	hb sweep right	76 E WAGGLE	
17 PUNT		47 F **SCREEN** L	hb **screen**	77 E QUICK	
18 FIELD GOAL		48 F P63 PASS	cross right	78 E P30 PASS	
19 **FAKE FG**	**fake field goal**	49 F H48 PASS		79 E PA WHEEL	
20 Series		**50 Series**		**80 Series**	
21 G F69 BOOM		51 N H19 MANO	hb trap left	81 S FLOOD L	
22 G F51 MAN		52 N H13 BILL		82 N DEEP IN	
23 G FG8 BOOM		53 N F68 LEAD		83 S POST OUT	
24 G F61 MAN		54 N H59 **CNTR**	hb **counter**	84 S CROSS UP	
25 G F54 CNTR		55 N F64 LEAD	fb off tackle	85 F FLAGPOST	
26 G F64 LEAD		56 N H38 TOSS		86 S TURMOIL	
27 G F69 SWEEP		57 N P64 PASS	cross in	87 T H39 TOSS	
28 G QB SNEAK		58 N P68 PASS	play action	88 T P39 PASS	
29 G P54 PASS		59 N **SCREEN** R	hb **screen**	89 S F38 TOSS	
30 Series		**60 Series**		**90 Series**	
31 G H39 TOSS		61 P F31 **TRAP**	fb center **trap**	91 4 **FLOOD R**	off91 **flood right**
32 G H10 LEAD		62 P H14 LEAD		92 4 **QUICKOUTS**	off92 **quick outs**
33 G H14 LEAD		63 P H16 BOB	hb off tackle	93 4 POST IN	
34 G H59 CNTR		64 P H39 **TOSS**	hb **toss left**	94 4 **POST UP**	off94 **post up**
35 G H40 ICE		65 P F42 MAN		95 4 **DEEP OUT**	off95 **deep outs**
36 G H38 TOSS		66 P H18 BOB		96 4 UP HOOK	
37 G H13 BILL		67 P **FB DRAW**	fb **draw**	97 4 **FLAGPOST**	off97 **flag left**
38 G P14 PASS		68 P P42 PASS	down and out	98 4 F CIRCLE	
39 G XY CROSS		69 P P31 **PASS**	cross **pass**	99 4 HAILMARY	
				New from Sega	
				offfbd fb draw	
				offfp fake punt	

Barr next explained how it was possible to compare the player formations and movements across the two games. Figure 2 (demonstrative Exhibit 645) depicts the data from the Apple II Madden assembly language program.[144] The semicolons indicated comments. Thus, the first row indicates that this is the "Nickel," or five defensive back formation. The second row indicates the eleven player designations (0 followed by 1-10 to equal 11). The third row indicates the X coordinate position in the two-dimensional field grid. The fourth row indicates the Y coordinate position. The locations in the grid are represented in hexadecimal (dollar sign followed by a two element representation with the size indicated by 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, and F).

144. *See id.*

Figure 2: Illustrative Apple II Madden Assembly Code Data

```
;       NICKEL
;               0    1    2    3    4    5    6    7    8    9    10
FX42  DB  $8D, $75, $99, $69, $99, $69 $5D, $39, $D5, $81,  $B1 ;X COORDINATE
FY43  DB  $7F, $7F, $7F, $7F, $7C, $7C,  $73  $79  $79  $70  $76 ;Y COORDINATE
FP42  DB   01,   02,   05,   06,   08,   10,   13,   15,   14,   18,   17  ;POSITION
```

Figure 3 (demonstrative Exhibit 646) is the data that the Apple II Madden play editor generated.[145] It provides the data for simulating the play called NIC reddog, which indicates a defensive rush or blitz,[146] from the Nickel defensive formation.

Figure 3: Apple II Madden Play Editor Data

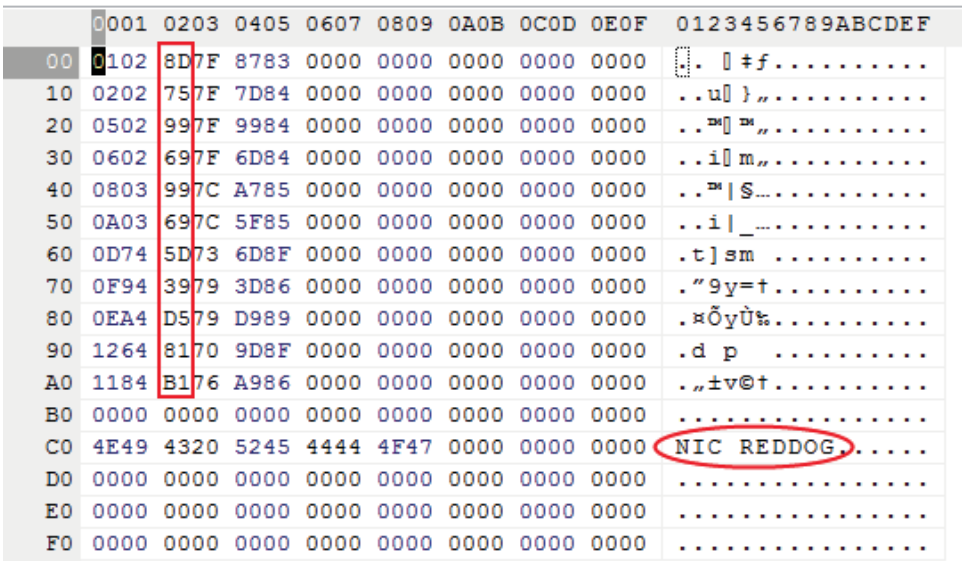


Figure 4 (demonstrative Exhibit 647) depicts source code from 1990 Sega Madden for a formation and play.[147] Barr explained that the play data is in binary code.

145. *See id.* at 1373–75.

146. *See Blitz (gridiron football)*, WIKIPEDIA, https://en.wikipedia.org/wiki/Blitz_(gridiron_football) (last visited Aug. 30, 2020) (explaining the origin of the term "red-dog" in football).

147. *See* Trial Transcript, *supra* note 85, at 1375–77.

Figure 4: Illustrative 1990 Sega Madden Formation and Play Source Code

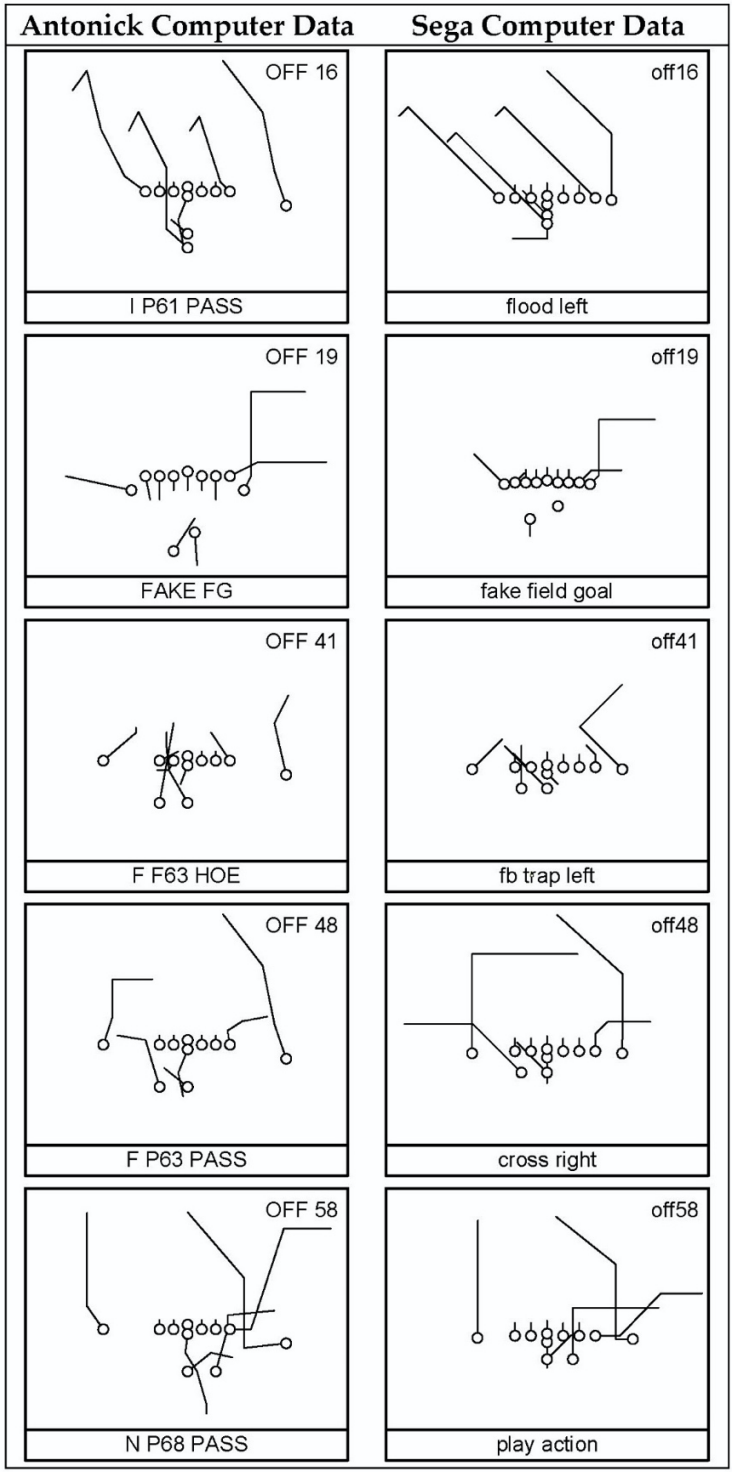
```
off63 ;hb off tackle
      dc    proset1     ;formation pro-set
      dc.b  -1,-1,-1    ;pass players

      dc.b  oasm,-1,4,7
      dc.b  oapt,3,0,0
      dc.b  oaorb,0,0,0,-1   ;
      dc.b  oara,16,1,0
      dc.b  oara,80,0,0
      dc.b  oaorb,0,0,0,-1   ;
      dc.b  oara,20,7,0
      dc.b  oaorb,0,0,0,-1   ;
      dc.b  oara,10,2,0
      dc.b  oara,20,1,0
      dc.b  oaorb,0,0,0,-1   ;
      dc.b  oarb,16,0,0
      dc.b  oaorb,0,0,0,-1   ;
      dc.b  oarb,6,7,0
      dc.b  oaorb,0,0,0,-1   ;
      dc.b  oarb,6,1,0
      dc.b  oaorb,0,0,0,-1   ;
      dc.b  apaz,2,0,0
      dc.b  oarb,16,2,0
      dc.b  oaorb,0,0,0,-1   ;
      dc.b  oarb,6,0,0
      dc.b  oaorb,0,0,0,-1   ;
      dc.b  oarb,6,0,0
      dc.b  oaorb,0,0,0,-1   ;
      dc.b  oarb,6,0,0
      dc.b  oaorb,0,0,0,-1   ;
```

As a way of enabling the jury to visually compare the plays and formations of the two games, Barr developed software to read in the data from both games and generate side-by-side depictions of formations and player movements in relationship to the line of scrimmage.[148] Figure 5 (first page of demonstrative Exhibit 476) shows that comparison. The left side depicts offensive plays 16, 19, 41, 48, and 58 from Apple II Madden. The right side depicts offensive plays 16, 19, 41, 48, and 58 from Sega Madden. The other plays represented in demonstrative Exhibit 476 showed similar patterns.

148. *See id.* at 1377–82.

Figure 5: Comparison of Offensive Plays—Apple II Madden and Sega Madden



Barr also testified to the presence of various misspellings and distinctive character strings from the source code for Apple II Madden that show up in Sega Madden source code.[149]

Regarding later versions of Sega Madden, Barr testified that the plays in 1990 Sega, derived from Apple II Madden, were also found in subsequent Sega versions.[150] Barr illustrated this point by walking through an example of a play from 1995 Sega Madden, demonstrating how plays persisted from Apple II Madden to 1995 Sega Madden.[151] Barr also testified that he found no evidence that subsequent versions of Sega Madden ever eliminated plays used in both Apple II Madden and 1990 Sega Madden.[152] He further noted that additional plays from Apple II Madden were added to later Sega versions.[153]

EA's defense centered on the theme that Park Place independently developed Sega Madden and the only reason for the similarity of the plays and formations was that Simmons used a selection of plays from playbooks that Judge Breyer ruled unprotectable. EA's lead counsel used the following analogy to illustrate the point:

> Let's suppose two people have decided to do a painting of the Golden Gate Bridge. Their paintings likely would look similar. And if you look at these two paintings they look similar. There are differences, but they don't look similar . . . because one copied the other's painting. They look similar because they are both painting the same thing, the Golden Gate bridge.
>
> In the same way, Jim Simmons and Robin Antonick used the plays that Trip Hawkins wrote and implemented them into their game by writing source code. Jim Simmons had as much right as Robin Antonick to use the plays in the Apple II playbook, just as one painter has as much right as another to paint the Golden Gate bridge.[154]

In his closing argument, Antonick's lead counsel contended that the only plausible explanation for Park Place's rapid successful implementation of Sega Madden, its avoidance of inevitable software bugs, the nearly identical play formations and player movement, the selection and arrangement of plays and play names, and the telltale misspellings and other similarities with Apple II

149. *See id.* at 1384–93.
150. *See id.* at 1397–98.
151. *See id.* at 1398–99.
152. *See id.* at 1397–98.
153. *See id.* at 1399–1401.
154. *See id.* at 656 ll. 13–25.

Madden source code was that Simmons received and emulated Antonick's code, play data, and other granular details of Apple II Madden.[155]

EA responded by reminding the jury of its Golden Gate bridge painting analogy to contend that Simmons independently developed Sega Madden.[156] She emphasized that "[e]very single EA witness who testified told you they did not see Mr. Antonick's source code in connection with the making of the Sega Madden game or any other game."[157] She admonished the jury that "[i]n order to find in favor of Mr. Antonick, you would have to find that each and every one of these witnesses came in here, swore to tell the jury under penalty of perjury, and deliberately lied to you."[158]

Antonick's counsel responded by paraphrasing an insight commonly attributed to C.S. Lewis—"[i]ntegrity is what you do when no one is looking"[159]—as the key to solving the puzzle.[160]

The jury unanimously found for Antonick on the plays and formations element, finding that there were substantial similarities in the source code for Apple II Madden and Sega Madden, and that Antonick had proven that all seven editions of Sega Madden under consideration (from 1990 to 1996), considered as a whole, were virtually identical to Apple II Madden.[161] The jury's verdict set the stage for a third phase focused on EA games released after 1996. Before undertaking that process, the court turned its attention to post-trial motions.

F. POST-TRIAL PROCEEDINGS: JUDGMENT FOR EA AS A MATTER OF LAW

EA filed a motion pursuant to Rule 50 to overturn both of the jury's verdicts—statute of limitations and breach of contract—as a matter of law.[162]

---

155. *See id.* at 2057–85.

156. *See id.* at 2107–08.

157. *See id.* at 2087 ll. 8–10.

158. *See id.* at 2087 ll. 13–16.

159. C.S. Lewis Found., *Quotes Misattributed to C.S. Lewis*, LIVING THE LEGACY OF C.S. LEWIS, http://www.cslewis.org/aboutus/faq/quotes-misattributed/ (last visited Aug. 30, 2020).

160. *See* Trial Transcript, *supra* note 85, at 2129 ll. 19–20.

161. *See* Special Verdict Form, *Antonick*, No. CV 11-01543 CRB (Document 516), 2013 WL 9768250; Beth Winegarner, *EA Owes 'Madden NFL' Coder $3.6M in Royalties, Jury Finds*, LAW360 (July 23, 2013, 8:03 PM), https://www.law360.com/articles/459582.

162. *See* EA's Amended Renewed Phase II Motion for Judgment as A Matter of Law Under Fed. R. Civ. P. 50(B), or, Alternatively, Motion for New Trial Under Fed. R. Civ. P. 59, *Antonick*, No. 3:11-cv-01543-CRB (Document 540); Electronic Arts Inc.'s Notice of Motion and Motion for Judgment as a Matter of Law that Antonick's Claims Are Barred by the Statute of Limitations, *Antonick*, No. 3:11-cv-01543-CRB (Document 443); FED. R. CIV. P. 50(b).

Under Ninth Circuit law, "Judgment as a matter of law is appropriate when the evidence, construed in the light most favorable to the nonmoving party, permits only one reasonable conclusion, which is contrary to the jury's verdict."[163] The court may grant a motion for judgment as a matter of law only if " 'there is no legally sufficient basis for a reasonable jury to find for [the non-moving] party on that issue.' "[164] If, however, "there is 'such relevant evidence as reasonable minds might accept as adequate to support the jury's conclusion,' " the motion should be denied.[165] When considering a motion for judgment as a matter of law, the court may not make credibility determinations, weigh the evidence, or substitute its own view of the evidence for the jury's.[166]

Notwithstanding the high threshold for overturning a jury verdict, Judge Breyer granted EA's motion with respect to the jury's breach of contract determination.[167] The court drew heavily on its pretrial ruling that Apple II Madden was only entitled to thin protection, and hence Sega Madden would only constitute a derivative work "if an ordinary reasonable observer comparing Apple II Madden as a whole to Sega Madden as a whole would consider the works virtually identical."[168] While acknowledging that Antonick identified a broad range of similarities, Judge Breyer concluded that "Antonick does not point to any evidence of the works 'as a whole.' "[169] The court noted that "Barr's opinion that all seven Sega Madden games are 'essentially the same' as a whole cannot substitute for the jury's subjective comparison of each of the seven Sega Madden games as a whole to Apple II Madden as a whole."[170]

The court based this conclusory statement on the limitation on expert opinion first announced in *Krofft*:

> Because the intrinsic test requires the perspective of an ordinary, reasonable observer, *Funky Films, Inc.* [*v. Time Warner Entertainment Co., L.P.*], 462 F.3d 1072, 1077 [(9th Cir. 2006)], expert testimony is not admissible evidence of similarity for purposes of the intrinsic

163. Hagen v. City of Eugene, 736 F.3d 1251, 1256 (9th Cir. 2013) (quoting Omega Envtl., Inc. v. Gilbarco, Inc., 127 F.3d 1157, 1161 (9th Cir. 1997)).

164. Jorgensen v. Cassiday, 320 F.3d 906, 917 (9th Cir. 2003) (quoting Reeves v. Sanderson Plumbing Prods., Inc., 530 U.S. 133, 149 (2000)).

165. *Hagen*, 736 F.3d at 1256 (quoting Gilbrook v. City of Westminster, 177 F.3d 839, 856 (9th Cir. 1999) (quoting Landes Constr. Co. v. Royal Bank of Can., 833 F.2d 1365, 1371 (9th Cir. 1987))).

166. *See* EEOC v. Go Daddy Software, Inc., 581 F.3d 951, 961 (9th Cir. 2009) (citing *Reeves*, 530 U.S. at 150).

167. *See Antonick*, No. C 11–1543 CRB, 2014 WL 245018 (order granting EA's Amended Renewed Phase II Motion).

168. *Id.* at *6 (citing Third MSJ Order in n.6).

169. *Id.* at *7.

170. *Id.* at *9.

> test. *See, e.g., Olson v. Nat'l Broad. Co., Inc.*, 855 F.2d 1446, 1448–49 (9th Cir.1988) (stating that expert testimony is appropriate under the extrinsic test, but not under the intrinsic test); *Express, LLC v. Fetish Grp., Inc.*, 424 F.Supp.2d 1211, 1228 (C.D. Cal.2006) ("While expert testimony is generally appropriate in conducting the extrinsic test, expert testimony may not be considered in conducting the intrinsic test.") (internal citation omitted); *Trust Co. Bank v. Putman Publ'g Grp., Inc.*, No. CV 87 07393 AHS(JRX), 1988 WL 62755, at *6 (C.D.Cal. Jan. 4, 1988) ("Expert testimony is inadmissible on this intrinsic test."). *See also Computer Associates Int'l, Inc. v. Altai, Inc.*, 982 F.2d 693, 713 (2d Cir.1992) ("[E]xpert testimony may be used to assist the fact finder in ascertaining whether the defendant had copied any part of the plaintiff's work. . . . However, once some amount of copying has been established, it remains solely for the trier of fact to determine whether the copying was 'illicit'. . . . Since the test for illicit copying is based upon the response of ordinary lay observers, expert testimony is thus 'irrelevant' and not permitted.") (citations omitted).[171]

Funky Films, *Olson v. National Broadcasting Co., Inc.*, and *Trust Co. Bank v. Putman Publishing Group, Inc.* rely on *Krofft*'s questionable standard.[172] These decisions don't address whether experts should be permitted to translate technical computer design and coding into a form that a jury can comprehend for the purposes of comparing works written in different computer languages.

It is particularly unnerving to see the court's reliance on footnote 10 in *Altai*, which expressly *permitted* the use of expert witnesses in software copyright cases for the very purpose of enabling lay judges and juries to surmount the task of making the illicit copying determination.[173] Had Judge Breyer continued reading the *Altai* decision following the excerpt he quoted in footnote 10, he would have seen that the Second Circuit carefully explained why it was *departing* from traditional expert witness rule for computer software cases. The Second Circuit explains:

> Historically, *Arnstein*'s ordinary observer standard had its roots in "an attempt to apply the 'reasonable person' doctrine as found in other areas of the law to copyright." 3 NIMMER § 13.03[E][2], at 13–62.10–11. That approach may well have served its purpose when the material under scrutiny was limited to art forms readily comprehensible and generally familiar to the average lay person.

171. *Id.* at *9, *9 n.9.

172. *See* Funky Films, Inc. v. Time Warner Entm't Co., L.P., 462 F.3d 1072, 1076–77 (9th Cir. 2006) (citing *Krofft*); Olson v. Nat'l Broad. Co., Inc., 855 F.2d 1446, 1448–49 (9th Cir. 1988) (citing *Krofft*); Trust Co. Bank v. Putman Publ'g Grp., Inc., No. CV 87 07393 AHS(JRX), 1988 WL 62755, at *5–*6 (C.D. Cal. Jan. 4, 1988).

173. *See supra* text accompanying notes 44–47.

However, in considering the extension of the rule to the present case, we are reminded of Holmes' admonition that, "[t]he life of the law has not been logic: it has been experience." O.W. Holmes, Jr., THE COMMON LAW 1 (1881).

Thus, in deciding the limits to which expert opinion may be employed in ascertaining the substantial similarity of computer programs, we cannot disregard the highly complicated and technical subject matter at the heart of these claims. Rather, we recognize the reality that computer programs are likely to be somewhat impenetrable by lay observers—whether they be judges or juries—and, thus, seem to fall outside the category of works contemplated by those who engineered the *Arnstein* test. *Cf. Dawson v. Hinshaw Music Inc.*, 905 F.2d 731, 737 (4th Cir.) ("departure from the lay characterization is warranted only where the intended audience possesses 'specialized expertise' "), *cert. denied*, 498 U.S. 981 (1990). As Judge Pratt correctly observed:

> In the context of computer programs, many of the familiar tests of similarity prove to be inadequate, for they were developed historically in the context of artistic and literary, rather than utilitarian, works.

Computer Assocs., 775 F.Supp. at 558.

In making its finding on substantial similarity with respect to computer programs, we believe that the trier of fact need not be limited by the strictures of its own lay perspective. *See Dawson*, 905 F.2d at 735; *Whelan*, 797 F.2d at 1233; *Broderbund*, 648 F.Supp. at 1136 (stating in dictum: "an integrated test involving expert testimony and analytic dissection may well be the wave of the future in this area. . . ."); Brown Bag Software, 960 F.2d at 1478–79 (Sneed, J., concurring); *see also* 3 NIMMER § 13.03[E][4]; *but see Brown Bag Software*, 960 F.2d at 1475 (applying the "ordinary reasonable person" standard in substantial similarity test for computer programs). Rather, we leave it to the discretion of the district court to decide to what extent, if any, expert opinion, regarding the highly technical nature of computer programs, is warranted in a given case.

In so holding, we do not intend to disturb the traditional role of lay observers in judging substantial similarity in copyright cases that involve the aesthetic arts, such as music, visual works or literature.

In this case, [MIT Computer Science Professor] Dr. Davis' opinion was instrumental in dismantling the intricacies of computer science so that the court could formulate and apply an appropriate rule of law. While Dr. Davis' report and testimony undoubtedly shed valuable light on the subject matter of the litigation, Judge Pratt remained, in the final analysis, the trier of fact. The district court's

> use of the expert's assistance, in the context of this case, was entirely appropriate.[174]

Similarly, in the *Antonick* trial, Barr's testimony and demonstrative exhibits were "instrumental in dismantling the intricacies of computer science so that the court could formulate and apply an appropriate rule of law."[175] Since *Altai* was a bench trial, Judge Pratt stood in the jury's shoes.

To make matters worse, faithful application of Rule 50(b) dictates affirmance of the jury's liability determination. Judge Breyer should have credited the jury's assessment of both circumstantial and direct evidence, just as he instructed.[176] In conjunction with the extensive circumstantial evidence that Simmons used Antonick's code to complete Sega Madden, Barr's testimony enabled the jury to understand the binary play data and many other technical aspects of video game programming necessary for lay jurors to evaluate the questions before it. Viewing the evidence in the light most favorable to Antonick, including credibility determinations, should have led Judge Breyer to reject EA's Phase II Judgment as a Matter of Law (JMOL) motion and uphold the jury's verdict. The jury was fully entitled to conclude, as Antonick argued, that Simmons faithfully emulated the Apple II Madden play data in writing Sega Madden source code and that subsequent editions of Sega Madden reproduced the derived code.[177] Thus, it is difficult to see how Judge Breyer did not usurp the jury's role.

G. NINTH CIRCUIT APPEAL: RECOGNITION, AFFIRMANCE, AND EXPANSION OF THE "NUTTY" RULE

While it was astounding to see the district court so badly misinterpret copyright jurisprudence in its pretrial rulings, misapply the Rule 50(b) standard in its post-trial ruling, and misread *Altai* in overturning the jury's verdict, surely the Ninth Circuit would correct these errors. It seemed inconceivable that the Ninth Circuit would not distinguish software code cases from cases involving works that are readily perceptible to lay fact-finders as regards the admissibility of expert testimony, as all of the circuits to consider the issue had,[178] or, at a

174. Comput. Assocs. Int'l, Inc. v. Altai, Inc., 982 F.2d 693, 713–14 (2d Cir. 1992) (citations omitted).

175. *Id.* at 714.

176. *See supra* note 130.

177. It is also worthwhile noting that the definition "derivate works" in the EA-Antonick contract expressly included "significant enhancements of the Work to add additional features or improve performance and adaptations of the Work to operate on computers or operating systems other than those described in the Specifications." 1986 Contract, *supra* note 78, at Exhibit A § 1.03 (defining "Derivative Work").

178. *See supra* Part III.

minimum, call for en banc reconsideration of *Krofft*, at least with regard to computer software copyright cases, as Judge Sneed had intimated.[179]

Antonick's opening appellate brief squarely presented the errors,[180] including the argument that EA waived its Rule 50(b) argument regarding insufficiency of the evidence of virtual identity of the works as a whole by failing to preserve the issue.[181] EA's opposition echoed the "thin" copyright arguments that it used to mislead the district court in its pretrial rulings—namely that competitors are free to independently develop competing video games—even though this case involved alleged sequels developed with full access to the underlying source code and design documents.[182] The jury ruled that Simmons did not independently develop Sega Madden based on ample evidence.

EA also argued that Antonick's complaint must fail because "[a] copyright plaintiff cannot establish that one work infringes another without proving the content of the two works so that they can be compared."[183] Although EA failed to produce the final source for Apple II Madden, Antonick located and produced original drafts of source code, data files, and design documents for Apple II Madden that enabled Michael Barr to provide the jury with comparisons of the Apple II Madden and Sega Madden design and code bases that laypeople could understand. Barr explained similarities in, among other things, selection and expression of plays and formations, ordering and numbering of plays, player ratings, nonstandard and disproportionate field width, names of plays and variables, and misspellings that were unlikely to occur absent copying of Antonick's code by Park Place.[184] EA also sought to revive its statute of limitations defense, which the jury rejected in the phase I trial[185] and Judge Breyer upheld in his post-trial ruling.[186]

179. *See supra* note 71.

180. *See* Appellant's Brief, Antonick v. Elec. Arts, Inc., 841 F.3d 1062 (9th Cir. 2016) (No. 14-15298), 2014 WL 3909266.

181. *See* Murphy v. City of Long Beach, 914 F.2d 183, 186 (9th Cir. 1990) (holding that a party may not seek a judgment notwithstanding the verdict on grounds not alleged in their motion for directed verdict).

182. *See* Appellant's Brief, *supra* note 180, at 60–68.

183. *Id.* at 29.

184. *See* Trial Transcript, *supra* note 85, at 1295–1325, 1342–1456, 1475–90.

185. *See* Appellant's Brief, *supra* note 180, at 80–89.

186. *See* Antonick v. Electronic Arts Inc., No. C 11–1543 CRB, 2014 WL 245018, at *3–*6 (N.D. Cal. Jan. 22, 2014).

At oral argument on March 16, 2016,[187] Judges Andrew Kleinfeld, Johnnie Rawlinson, and Andrew Hurwitz launched into the statute of limitations defense. Drawing on his experience programming computers decades earlier,[188] Judge Kleinfeld suggested—contrary to the stipulation at trial, the significant differences between the Apple II and Sega Genesis platforms, and the testimony of software experts from both sides—that "it's inconceivable that a game developer would not notice that his game had been copied until many years later when there was an anniversary special. You would think that he'd been playing football games."[189] Judge Kleinfeld then opined:

> [W]hen you have written a computer program, you can usually tell something about the technique of how it was created even though you can't tell the details just as if you know some other craft, traditional dark room photography, you can make a pretty good judgment about how a particular effect was produced. Now you can't do it for sure until you have disassembled the code, but if you have a big economic interest, one would think that you would.[190]

The parties' stipulation[191] and trial record contradicted Judge Kleinfeld's assertion.[192]

Shortly thereafter, Judge Kleinfeld pursued his hunch that Antonick could have easily disassembled the Sega Madden code to determine whether it was copied from Apple II. Madden offered his opinion that the 68000 microprocessor used in the Sega Genesis is a descendent of the 6502 microprocessor used in the Apple II.[193] As Antonick's counsel pointed out,

187. Video Recording of Oral Argument, *Antonick*, 841 F.3d 1062 (No. 14-15298) [hereinafter 9th Circuit Oral Argument], https://www.ca9.uscourts.gov/media/view_video.php?pk_vid=0000009278.

188. *See id.* at 13:48–14:32 (showing Judge Kleinfeld explaining that he had programmed code for the Zilog Z80 microprocessor chip and that it was easy to disassemble code for that chip).

189. *Id.* at 0:59–1:16. Antonick had expressly denied playing the video football games after he completed his work with EA. *See* Trial Transcript, *supra* note 83, at 251.

190. 9th Circuit Oral Argument, *supra* note 187, at 1:33–2:06.

191. *See* Trial Transcript, *supra* note 85, at 1953 ("Playing or viewing a John Madden Football game for the Sega Genesis or Super Nintendo would not have allowed the person looking at the screen or playing the game to determine how a particular game element was expressed in the source code.").

192. *See id.* at 1277–78 (Michael Barr), 1821–22, 1856, 1860, 1896, 1911–14 (Robert Zeidman) (discussing the challenges of detecting copying of source code in different language). Later in the argument, EA's counsel contradicted Judge Kleinfeld's assertion that disassembly of the object code to obtain the source code could have been done. *See* 9th Circuit Oral Argument, *supra* note 187, at 3:49–4:30.

193. *See id.*

EA had not pursued that issue.[194] More to the point, disassembling the video games at issue from the object code was very difficult, as software experts for both sides testified.[195] As a result of this digression—in which a Ninth Circuit judge who had programed some code for a more primitive microprocessor in the early 1980s offered his own opinions about microprocessors and disassembly—nearly half of Antonick's oral argument time was gone.[196]

When the argument turned to the role of expert witnesses in software copyright cases, Judge Hurwitz stated:

> The brief from [Antonick's] side says that in the 9th Circuit expert testimony is allowed on the extrinsic, on the intrinsic test. I find I don't know eight, nine, ten cases, some involving computer code, in our circuit saying no it's not. Who's right? And let me preface this by saying that I think that's a nutty rule if it is our rule. But my question is: Is that our rule?[197]

After Antonick's counsel responded that there was room for doubt as to the Ninth Circuit's rule, Judge Hurwitz responded: "You don't have to convince me that [the *Krofft* rule] is wrong in terms of policy, but you'll have to convince eleven judges on the court to call it en banc."[198]

Since the Ninth Circuit clearly permits expert testimony of the extrinsic aspect of the copyright infringement test, the court then delved into how the role of experts works in practice:

Judge Hurwitz:	[The Ninth Circuit has] cases in which we have specifically said that you cannot use expert testimony on the intrinsic side of the test. And I understand that we have generally said we think that the Second Circuit is smarter than us and does a better job. I'll take that. My question is: Is there any case in which we have said, and because we've been so dumb in the past that we do allow testimony on the intrinsic standard.
David Nimmer (Antonick's Copyright Appellate Counsel):	Your Honor, I don't have a citation to a case that says "we have been dumb in the past," however

194. *See id.* at 15:00–15:06.

195. *See supra* note 192.

196. Judge Kleinfeld returned to this digression later in the argument, further cutting into Antonick's argument time. *See* 9th Circuit Oral Argument, *supra* note 187, at 51:11–51:29.

197. *Id.* at 25:00–25:28.

198. *Id.* at 28:00–28:07.

Judge Hurwitz: [chuckling] Try the second part, OK [laughter]

David Nimmer: I do have the past experience of Ninth Circuit cases and there is no case in which the jury has been asked unaided by expert testimony to simply code for non-literal copying.

Judge Rawlinson: But the expert testimony is on the extrinsic test, isn't it? Not the intrinsic.

David Nimmer: Nominally it is on the extrinsic test.

Judge Kleinfeld: Can Ninth Circuit law be read to mean that you don't need, and therefore cannot use, an expert to say that the two expressions look alike, but you may well need and can use an expert to say whether the source code is alike?

David Nimmer: I think that is one possibility your Honor.

Judge Rawlinson: When you're comparing the source code, would that be the intrinsic test or the extrinsic test?

David Nimmer:

Well, your Honor has identified exactly the problem, and then the dilemma in the context of software. There has been no case in which juries have been asked to compare different source codes to find non-literal identity.

I think that the answer to the court's collective question can be as follows: How should the intrinsic test be applied? First of all, it's obvious that expert testimony needs to be admitted, and all cases in all circuits, including the Ninth Circuit, have admitted expert testimony.

But then when the question comes to the jury, "jury make the intrinsic test," I could understand not allowing the expert to give his or her ultimate opinion—"I believe that these are, that these express, the same idea, and that's my personal opinion." The jury can be asked exactly the question that EA poses in its own brief when it characterizes the intrinsic test on page 33 [of its brief]. It says in effect that the intrinsic asks whether the defendant took from plaintiff's work so much of what is pleasing to the work's intended audience that the defendant wrongfully appropriated something which belongs to the

plaintiff, quoting *Cavalier v. Random House*, a case involving children's books.

That's a question that after expert testimony has been admitted, the jury can make in its determination, in its subjective consideration as the voice of the community. And that is not precisely what happened here because Judge Breyer framed the jury instruction.

Judge Hurwitz: If we disagree with you and find that Mr. Barr's testimony is not admissible on the intrinsic side of the equation, is there any other evidence that shows, that would satisfy the intrinsic part of the test?

David Nimmer: OK, let's take that step-by-step here you Honor. Mr. Barr's testimony, we're going to imagine, is admissible because it illuminates the extrinsic test.

Judge Hurwitz: Right.

David Nimmer: Now the jury in its sole discretion has to apply the intrinsic test. The jury has to determine, OK now that we've heard the testimony and we've heard the defense and we've heard the cross-examination, did EA take so much of what is pleasing to the work's intended audience that it wrongfully appropriated something which belongs to the plaintiff? That is a test the jury can make in its subjective determination based on all of the evidence that it has heard in the case.

Judge Hurwitz: Even in the absence of the code being in evidence?

David Nimmer: Absolutely. In the presence of the code being in evidence, nothing is added except confusion to the jury. Let's imagine that the code was added.

Judge Kleinfeld: I can't see that. I mean, even a layman can compare what may be meaningless instruction in the code. It would be like reading two texts that are in a foreign language and having no idea what the text means but being able to see that its the same characters.

David Nimmer: Your Honor, this court has said in the case of *Swirsky* that when music is copied not identically, we need expert testimony. And to quote the

> *Swirsky* Ninth Circuit opinion, "Any person untrained in music could conclude that 2-2-2-2-2-1-2-1-3 did not match 2-2-4-3-2-3." It's the same in this case. Any person could conclude that the 0-0-0-1-0-0 does not match 1-0-0-1-1-0. If that was the standard, no expert testimony would be needed and the case would end immediately. There would be no such thing as non-literal copying in the Ninth Circuit if that were the standard. *Swirsky* assures us that that is not the standard. That extrinsic testimony from an expert, a musicologist in that case, is needed.
>
> In this case, expert testimony is needed from someone who is expert in the field of computer software. And that is the testimony that was given. At the end of the day, the jury can make its own intrinsic determination: Did the defendant cross the line? Did the defendant appropriate so much from the work that is pleasing to its intended evidence that it crossed over the line?[199]

During its argument, EA pressed the importance of the jury directly comparing the works at issue.[200] In response, Judge Kleinfeld remarked, "If I were a juror, I would really want an expert, because it is too boring to go across each line and compare. My eyes glaze over . . . ."[201] Judge Hurwitz then concluded:

> [O]ur rule baffles me on this topic for the same reason that Judge Kleinfeld just said which is that the case law seems to say that the ordering and sequence of coding is also part of the copyrightable protectable material and certainly having somebody say they not only read the same number but the sequence makes some difference I think makes some sense to me, but, you know, I don't make the rules here, I just follow them.[202]

Despite that bafflement, on November 22, 2016, the Ninth Circuit affirmed the district court's ruling that Antonick's claim failed as a matter of law.[203] Without addressing the district court's flawed pretrial rulings—severely narrowing Antonick's derivative work claim and improperly requiring "virtual

199. *Id.* at 28:40-34:13.
200. *See id.* at 51:50–52:20, 59:16–1:00:11.
201. *Id.* at 1:01:25–1:01:33.
202. *Id.* at 1:02:40–1:03:09.
203. *Antonick*, 841 F.3d 1062.

identity" of the works as a whole—the appellate court concluded that the plaintiff's failure to place the full source code of both games into evidence made it impossible for the jury to compare the works as a whole.[204]

The court placed primary reliance on *Seiler v. Lucasfilm, Ltd.*,[205] which held based on the best evidence rule[206] that "[t]here can be no proof of 'substantial similarity' and thus of copyright infringement unless Seiler's works are juxtaposed with Lucas' and their contents compared."[207] In *Seiler*, the district judge "found that Seiler had lost or destroyed the originals in bad faith under Fed.R.Evid. 1004(1) and denied admissibility of any secondary evidence."[208]

The circumstances could not have been more different in *Antonick*, yet the Ninth Circuit does not make any effort to apply the clear exceptions to the best evidence rule. Rule 1003 provides that "[a] duplicate is admissible to the same extent as the original unless a genuine question is raised about the original's authenticity or the circumstances make it unfair to admit the duplicate." Rule 1004 provides that

> An original is not required and other evidence of the content of a writing, recording, or photograph is admissible if:
>
> (a) all the originals are lost or destroyed, and not by the proponent acting in bad faith;
>
> (b) an original cannot be obtained by any available judicial process;
>
> (c) the party against whom the original would be offered had control of the original; was at that time put on notice, by pleadings or otherwise, that the original would be a subject of proof at the trial or hearing; and fails to produce it at the trial or hearing; or
>
> (d) the writing, recording, or photograph is not closely related to a controlling issue.

The defendant EA was the copyright owner and remarkably failed to locate original copies of the Madden games, a product that earned EA billions of dollars. Furthermore, Antonick assembled a near complete copy of the Apple II Madden source code and design documents, and the parties were able to provide the jury with a rich understanding of how Apple II Madden and Sega

204. *See id.* at 1066–67.
205. Seiler v. Lucasfilm, Ltd., 808 F.2d 1316 (9th Cir. 1987).
206. *See* FED. R. EVID. 1001–08.
207. *Seiler*, 808 F.2d at 1319.
208. *Id.* at 1317.

Madden compared.[209] As the First Circuit recognized, "if the Best Evidence Rule is satisfied, evidence other than the original may be sufficient to establish the content of a copyrighted work."[210]

The Ninth Circuit cited other cases that focus on the insufficiency of the evidence to prove copyright infringement.[211] Yet Antonick brought a breach of contract case which turned in part on the Copyright Act's definition of "derivative work." The pertinent question was whether it was more likely than not that EA breached its obligation to pay royalties on derivative works as defined by the contract. Antonick provided a wealth of direct and circumstantial evidence to prove that Sega Madden constituted a "derivative work"—as defined by the contract—of Apple II Madden.

The Ninth Circuit's rejection of Antonick's appeal turned on the infamous "nutty" rule[212] and two conclusory assertions. First, that the evidence presented at trial "at most demonstrates access and a possible motive to copy" overlooks the extensive trial record. That record, as explored above[213] and to which the court is required to view in the light most favorable to Antonick, provided the jury ample grounds for finding that EA did not merely copy unprotectable ideas. The jury was entitled to believe substantial evidence showing that under impossibly tight time-to-market pressure, EA and its inexperienced programmer took shortcuts—copying substantial amounts of protectable design and coding elements—to complete in three months what Antonick's experienced team had taken four years to do. EA was caught with

209. *See* Barr Report, *supra* note 102, at Exhibit B (noting that he considered: Mr. Antonick's source code files, as produced on a set of floppy disks labeled as A0001, A0004-06, A0023-24, A0035, A0037-38, A0045-47, A0049, A0054-55, and A0058-66; Source code and technical files recovered from floppy disks (RA0003937); twenty-two optical disks produced by EA on which he identified source code for eight distinct versions of Madden football games for Sega Genesis and Super Nintendo; and four floppy disks from Park Place).

210. Airframe Sys., Inc. v. L-3 Commc's. Corp., 658 F.3d 100, 107 n.9 (1st Cir. 2011).

211. *See* Antonick v. Elec. Arts Inc., 841 F.3d 1062, 1066 (9th Cir. 2016) (citing *Airframe Sys., Inc.*, 658 F.3d at 107 ("Having presented no evidence sufficient to prove the content of its registered source code versions, Airframe cannot show that any of its registered works is substantially similar to the allegedly infringing M3 program.")); Gen. Universal Sys., Inc. v. Lee, 379 F.3d 131, 146 (5th Cir. 2004) (*per curiam*) ("Without providing its own source code for comparison, GUS did not satisfy the requirement that the infringed and infringing work be compared side-by-side."); Olson v. Nat'l Broad. Co., 855 F.2d 1446, 1448, 1451 (9th Cir. 1988) (granting JMOL to copyright defendant because no reasonable jury could have found substantial similarity).

212. "[O]ur law is clear that expert testimony cannot satisfy a plaintiff's burden of proof under the intrinsic test, which 'depend[s] on the response of the ordinary reasonable person.' " *Antonick*, 841 F.3d at 1067 (footnote omitted) (citing Brown Bag Software v. Symantec Corp., 960 F.2d 1465, 1475 (9th Cir. 1992) (quoting Sid & Marty Krofft Television Prods., Inc. v. McDonald's Corp., 562 F.2d 1157, 1164 (9th Cir. 1977))).

213. *See supra* text accompanying notes 130–153.

its hands in the protectable expression cookie jar. They did not merely take unprotectable ideas—they raided the jar.

Second, the Ninth Circuit commented that "the lay testimony was about how the games appeared, not how they were coded—and Antonick does not assert a copyright interest in Apple II Madden's audiovisual appearance, only in its coding." Yet the jury was presented with significant evidence about that coding.[214] The fact that a software expert presented the evidence—of play data and other source code elements—in no way negated the fact that the jury saw actual code. The Ninth Circuit in effect expanded the nuttiness of the "nutty" rule. The colloquy with David Nimmer about how to interpret the "nutty" rule sensibly was for naught.[215]

H. EN BANC AND CERTIORARI PETITIONS: DENIED

The Ninth Circuit's *Antonick* decision offered a glimmer of hope for rectifying the "nutty" rule:

> Antonick is not alone in contending that experts should be allowed to help juries assess the holistic similarity of technical works such as computer programs. *See Brown Bag*, 960 F.2d at 1478 (Sneed, J., concurring); *Comput. Assocs. Int'l, Inc. v. Altai, Inc.*, 982 F.2d 693, 713 (2d Cir. 1992). But, given our precedents, that argument must be addressed to an en banc court.[216]

Antonick decided to take a shot at rectifying the "nutty" rule.[217] Although en banc review is difficult to obtain,[218] several factors weighed in Antonick's favor.[219] The Ninth Circuit panel acknowledged that the applicability of the *Krofft* rule to software code cases was controversial and in conflict with the law in another circuit. In fact, it conflicts with the law of multiple circuits—all that have confronted the issue.[220] Moreover, the computer software industry is of

214. *See supra* text accompanying notes 138–153.

215. *See* 9th Circuit Oral Argument, *supra* note 187, at 29:30–34:13.

216. *Antonick*, 841 F.3d at 1067 n.4.

217. *See* Appellant's Petition for Rehearing En Banc, *Antonick*, 841 F.3d 1062 (No 14-15298) (9th Cir. 2017).

218. *See* Peter S. Menell & Ryan Vacca, *Revisiting and Confronting the Federal Judiciary Capacity "Crisis": Charting a Path for Federal Judiciary Reform*, 108 CALIF. L. REV. 789, 861 (2020) (reporting that the Ninth Circuit granted between 1.26% and 2.17% of en banc petitions in 2013–17).

219. *See* 9TH CIR. R. 35(b)(1)(B) (noting that en banc petitions must begin with a statement that "the proceeding involves one or more questions of exceptional importance, each of which must be concisely stated; for example, a petition may assert that a proceeding presents a question of exceptional importance if it involves an issue on which the panel decision conflicts with the authoritative decisions of other United States Courts of Appeals that have addressed the issue").

220. *See supra* Part III.

tremendous economic significance to the U.S. economy in general and states within the Ninth Circuit. The Ninth Circuit sees a large portion of software copyright cases.

However, the Ninth Circuit unfortunately declined the petition. All of the panel members, despite having written that the "argument must be addressed to an en banc court," voted against review.[221] They might have considered the expert witness issue unnecessary for resolving the *Antonick* case because of the best evidence ruling—which was also wrong,[222] although perhaps not nutty.

With time running down in the fourth quarter, Antonick opted to take a final Hail Mary[223] at the U.S. Supreme Court.[224] The circuit split could not have been clearer and more significant. Alas, the Supreme Court also declined review,[225] bringing this saga to a disconcerting end.

VI. RECTIFYING THE NINTH CIRCUIT'S NUTTY RULE

The *Antonick* case reads like a tragedy of errors, a Dickensian tale for the digital age.[226] Robin Antonick entered into a contract with EA to produce the first realistic football video game, a product that would revolutionize the sports video game industry. His contracts with EA shared the risks. Antonick was paid modestly to produce the game with the prospect of a share of future proceeds from his game and derivative works as defined in the contract if the game succeeded. Antonick saw some of that return from Apple II Madden, but he was allegedly misled into believing that the follow-on Madden games were not derived from his design and source code. When he discovered that he might have been defrauded, he brought suit and painstakingly gathered extensive evidence that enabled him to get to trial. Notwithstanding flawed pretrial rulings that severely restricted his allegations, the jury found in his favor, only to have the district judge overturn the verdict based on

221. Order, *Antonick*, 841 F.3d 1062 (No. 14-15298) ("Judges Rawlinson and Hurwitz voted to deny the petition for rehearing en banc, and Judge Kleinfeld so recommended. The full court was advised of the petition for rehearing en banc and no judge has requested a vote on whether to rehear the matter en banc. Fed. R. App. P. 35. The petition for rehearing en banc is denied.").

222. *See supra* text accompanying notes 205–210.

223. This is drawn from offensive play 99 in Apple II Madden. *See supra* Figure 1 Comparison of Football Play Names and Order in Apple Madden and Sega Madden.

224. *See* Petition for Writ of Certiorari, Antonick v. Elec. Arts Inc., 138 S. Ct. 422 (2017) (No. 17-168); Reply Brief for Petitioner, *Antonick*, 138 S. Ct. 422 (No. 17-168).

225. *Antonick*, 138 S. Ct. 422.

226. *See* CHARLES DICKENS, BLEAK HOUSE 3 (1853). Sadly, Antonick is not the only digital age BLEAK HOUSE. *See* Peter S. Menell, *API Copyrightability Bleak House: Unraveling and Repairing the* Oracle v. Google *Jurisdictional Mess*, 31 BERKELEY TECH. L.J. 1515 (2016).

questionable application of the Rule 50(b) standard and wooden application of a truly "nutty" rule: that expert witnesses cannot be used to aid lay judges and juries in deciphering and analyzing computer source code. On appeal, the Ninth Circuit panel overlooked the serious flaws in the district court's handling of the case, misapplied the best evidence rule, and exacerbated the nuttiness of the "nutty" rule. The larger Ninth Circuit declined to take up the clear circuit split, and the Supreme Court left the national law on the use of expert witnesses in software copyright cases fragmented. Notwithstanding the massive resources devoted to this matter, the judicial system failed to render a coherent or just resolution.

More than four decades ago, and before Congress extended copyright law to protect computer software,[227] the Ninth Circuit ruled that expert testimony was inadmissible to determine whether Mayor McCheese and the merry band of McDonaldland characters infringed copyright protection for Wilhelmina W. Witchiepoo and the other imaginative H.R. Pufnstuf costumed characters.[228] While this judge-made rule made sense in dealing with works that lay judges and jurors can directly perceive, it clearly makes no sense when applied to hexadecimal assembly code for different processors. Although the injustice to Robin Antonick cannot unfortunately be rectified, there remains an urgent need to correct the "nutty" rule that derailed his case and threatens to wreak havoc in future software copyright litigation in the Ninth Circuit.

It is perplexing that Ninth Circuit judges could not see, as judges in other circuits have, the simple path of distinguishing software cases based on the obvious limitations of lay judges and jurors in comprehending the foreign languages of source code. Since the emergence of software copyright infringement cases in the 1980s, substantially all software copyright cases have employed expert witnesses to aid juries in understanding software code. As the Second Circuit wisely recognized in *Computer Associates International, Inc. v. Altai, Inc.*,[229] the ordinary observer standard "may well have served its purpose when the material under scrutiny was limited to art forms readily comprehensible and generally familiar to the average lay person," but as to computer programs, district courts must have "discretion . . . to decide to what extent, if any, expert

227. The Copyright Act of 1976, which went in effect on January 1, 1978, included computer software in the class of "literary works." *See* 17 U.S.C. § 102(a)(1); Menell, *supra* note 40, at 315–18 (discussing Congress's vexed compromise to include computer software, written work that serves functional purposes, within the copyright system).

228. *See* Sid & Marty Krofft Television Prods., Inc. v. McDonald's Corp., 562 F.2d 1157 (9th Cir. 1977).

229. Comput. Assocs. Int'l, Inc. v. Altai, Inc., 982 F.2d 693 (2d Cir. 1992).

opinion, regarding the highly technical nature of computer programs, is warranted in a given case."[230]

The Ninth Circuit's peculiar approach to the role of experts continues to produce head-scratching results. On June 22, 2020, the court reversed a district court's dismissal of a copyright suit filed by the family of screenplay author Paul Zindel alleging that Fox Searchlight Pictures' *The Shape of Water* infringed Zindel's play *Let Me Hear You Whisper*.[231] The court ruled that Zindel was improperly denied the opportunity to present expert testimony regarding the similarities of the works in question as part of the extrinsic test. The Ninth Circuit apparently continues to believe that courts need help in assessing the objective similarities between a play and a film, both of which are expressed in English, but that courts do not need help from experts in understanding the subjective differences in hexadecimal assembly language codes.

The time is long past due for the Ninth Circuit, home to many of the most important software companies and the most significant software copyright cases,[232] to take the *Krofft* expert testimony rule en banc and rectify this "nutty" rule to accord with the other circuits. Short of that, the Supreme Court should either grant certiorari in a case raising this issue or simply remand such a case to the Ninth Circuit for en banc review. Although this issue should not require legislation, that remains an option to rectify and harmonize the national law on this important issue.

230. *Id.* at 713.

231. *See* Zindel v. Fox Searchlight Pictures, Inc., 815 F. App'x. 158 (9th Cir. 2020).

232. *See, e.g.*, Cisco Sys. Inc. v. Arista Networks, Inc., No. 14-cv-05344-BLF, 2016 WL 4440239 (N.D. Cal. Aug. 23, 2016); Oracle Am., Inc. v. Google Inc., 847 F. Supp. 2d 1178 (N.D. Cal. 2012), *aff'd in part, rev'd in part, and remanded*, 750 F.3d 1339 (Fed. Cir. 2014), *cert. denied*, 135 S. Ct. 2887 (2015), *rev'd*, 886 F.3d 1179 (Fed. Cir. 2018), *cert. granted*, 140 S. Ct. 520 (2019); Sega Enters. v. Accolade, Inc., 977 F.2d 1510 (9th Cir. 1992); Apple Comput., Inc. v. Microsoft Corp., 799 F. Supp. 1006 (N.D. Cal. 1992), *aff'd in part, rev'd in part*, 35 F.2d 1435 (9th Cir. 1994).

PATHWAYS TO INFORMATION PRIVACY POLICY: PLURALIST VS EXPERT?

Priscilla M. Regan†

ABSTRACT

This Article examines the dynamics of information privacy policymaking using the pathways framework developed by Timothy J. Conlan, Paul L. Posner, and David R. Beam in 2014. They identify four different pathways for policy—the pluralist, the partisan, the expert, and the symbolic. The Article is particularly interested in exploring why the expert pathway has not been employed in information privacy policymaking, and what conditions might enhance the likelihood of its use in this area. The Article proceeds as follows—first, a brief review of Conlan et al.'s framework and arguments; second, an application of their pathways framework to the development of privacy policy; third, an analysis of expertise in policymaking both generally and then with respect to information privacy policy; and fourth, an explication of why information privacy policymaking has been and is unlikely to take the expert pathway. Although the barriers to more expert input for information privacy policymaking are high, the analysis below identifies three factors which hinder expert input and three complementary changes which could enhance expert influence over information privacy policymaking.

DOI: https://doi.org/10.15779/Z384J09Z01

† Priscilla Regan is a Professor of Politics and Government in the Schar School of Policy and Government at George Mason University. Appreciation to Tim Conlan for comments on an earlier version of this Article and to the editors of the *Berkeley Technology Law Journal* for their thoughtful suggestions. An earlier version of this Article was presented at the 24th Annual BCLT/BTLJ Symposium "The Roles of Technology Expertise in Law and Policy" February 27–28, 2020, Berkeley, CA.

TABLE OF CONTENTS

I. INTRODUCTION 718

II. PATHWAYS TO POWER 720

III. PATHWAYS OF PRIVACY POLICYMAKING 725

IV. EXPERTS IN POLICYMAKING 728

A. SKEPTICISM/AMBIVALENCE 728
B. FORUMS FOR EXPERT INPUT 729
C. POLITICAL DYNAMICS 730

V. EXPERTS IN INFORMATION PRIVACY POLICYMAKING IN THE 2000S AND BEYOND 732

VI. BARRIERS TO EXPERTISE INFLUENCING INFORMATION PRIVACY POLICYMAKING 738

VII. ENHANCING THE ROLE OF EXPERTS 740

VIII. CONCLUSION 743

APPENDIX A – SELECTED INFORMATION PRIVACY CONGRESSIONAL HEARINGS (2010–19) 744

I. INTRODUCTION

Information privacy policymaking has been plagued by the dominance of interests opposed to effective policy. This was true in the earliest rounds of policy debates in the late 1960s and persisted into the 1970s, when business interests opposed omnibus legislation that would have imposed similar fair information principles on both the public and private sectors, and federal agencies opposed the establishment of a new federal agency to protect privacy.[1] This trend continued into the 1980s and 1990s as interests that would have been affected by sectoral privacy legislation successfully weakened original proposals. And this scenario is being replayed once again as advocates of stronger online privacy protections, especially with respect to online platforms, are outspent, outmaneuvered, and overwhelmed by the political strength of online business players.

1. *See generally* PRISCILLA M. REGAN, LEGISLATING PRIVACY: TECHNOLOGY, SOCIAL VALUES, AND PUBLIC POLICY (1995).

In the public policy literature, Timothy J. Conlan, Paul L. Posner, and David R. Beam have identified four different pathways to policymaking—the pluralist, the partisan, the expert, and the symbolic.[2] To date, privacy policy has been firmly embedded in the pluralist pathway. They argue that proponents of a certain policy can strategize to frame their policy problem and their proposals in such a way that policymaking occurs on a pathway that will be most conducive to success. This Article explores the possibility that privacy advocates might achieve success by moving policymaking from the pluralist pathway, where they have been unsuccessful, to the expert pathway, where they might achieve more success. The Article concludes that it is unlikely that privacy advocates will succeed in switching information privacy policymaking to the expert pathway for several reasons, including the current assault on expertise and even on facts themselves, compounded in the privacy area by the question of who the experts are. Such questions have become more contested as privacy issues and technology have evolved. Moreover, congressional hearings tend to privilege a more pluralistic approach to policymaking. Interestingly, the Belfer Center recently issued a report concluding:

> . . . in legislative and high-profile hearings, Congress has appeared unprepared to reckon with emerging technologies and their effects on society. In recent years, Congress has failed to produce substantive legislation on emerging science and technology issues of national import, *like personal data privacy and protections*.[3]

The Article proceeds as follows—first, a brief review of Conlan and Posner's framework and arguments; second, an application of Conlan et al.'s framework to the development of privacy policy; third, an analysis of expertise in policymaking both generally and then with respect to information privacy policy; and fourth, an explication of why information privacy policymaking is unlikely to take the expert pathway. Although the barriers to more expert input for information privacy policymaking are high, the analysis below identifies three factors which hinder expert input and three complementary changes which could enhance expert influence over information privacy policymaking.

---

2. *See generally* TIMOTHY J. CONLAN, PAUL L. POSNER & DAVID R. BEAM, PATHWAYS OF POWER: THE DYNAMICS OF NATIONAL POLICYMAKING (2014).

3. MIKE MIESEN, MAEVE CAMPBELL, CHRIS KUANG, LAURA MANLEY & EMILY ROSEMAN, BELFER CTR. FOR SCI. & INT'L AFFAIRS, BUILDING A 21ST CENTURY CONGRESS: IMPROVING CONGRESS'S SCIENCE AND TECHNOLOGY EXPERTISE 9–12 (2019), https://www.belfercenter.org/sites/default/files/2019-09/ST/Building21stCenturyCongress.pdf (emphasis added).

II. PATHWAYS TO POWER

Conlan et al. identify four distinct pathways that federal policymaking can take and further identify each pathway's primary actors, scale and scope of political mobilization, patterns of formulation and adoption, levels of salience and conflict, and enactment time. Table 1 below provides a summary and overview of these pathways.

Table 1: Comparison of Four Pathways—Conlan, Posner and Beam[4]

	Pluralist	**Partisan**	**Expert**	**Symbolic**
Scope and Form of Mobilization	Specialized/ Organizat'l	Mass/ Organizat'l	Specialized/ Ideational	Mass/ Ideational
Chief Sponsor	Comm. Chairs/ Ranking Members	Pres/Cong Party Leaders	Comm. Chairs/ Ranking Members	Variable – Ind'l Membs/ Leaders
Public Salience	Relatively Low	High	Highly Variable	Relatively High
Incubation Period	Several Years	10+ years	Slow but steady	Quick
Enactment Time	16 months	5 months	22 months	107 days
Degree of Consensus	High	Low	High	High
Partisanship	Low	High	Low	Low
Actors Involved	Interest groups	Party, esp. Pres	Area experts	Media, movements
Issue Definitions	Feedback	Indicators	Indicators	Crisis
Level of Conflict	Low	High	Medium	Low
Magnitude of Policy Change	Incremental	Non-incremental	Non-incremental	Mixed (58%/42%)
Policy Sustainability	77%	66%	44%	50%

4. This table is derived from Chapters 1 and 6 of CONLAN, *supra* note 2.

The *pluralist pathway* is arguably the most common in the U.S. policy system as it involves organized interests bargaining, negotiating, and compromising to reach some agreement, generally of an incremental nature and reflecting the more well-organized interests. The roots of the pluralist pathway, as well as the drawbacks, can be found in James Madison's identification in *Federalist No. 10* of the dangers of "factions," which "are united and actuated by some common impulse of passion, or of interest, adverse to . . . the permanent and aggregate interests of the community."[5] Political scientists originally regarded the policy process as a struggle among competing interest groups, enabling all groups concerned about a particular issue to have influence on the policy outcome, which was seen as the equilibrium point among the groups.[6] Later studies, however, pointed to the unequal influence among groups and the fact that some groups were not organized,[7] as well as the fact that, as E. E. Schattschneider noted, "[t]he flaw in the pluralist heaven is that the heavenly chorus sings with a strong upper-class accent."[8]

Despite the recognized biases in the pluralist system, it remains the dominant mode of policymaking in the United States, in part because the American political systems provides many points of access and many veto points, with politicians acting as advocates for particular groups and brokers to cobble together compromises.[9] Much of the policy work of interest groups today takes place in what Hugh Heclo identified as "issue networks,"[10] similar to John Kingdon's "policy communities,"[11] wherein government actors, special interest groups, public interest groups, and policy specialists in a particular policy area all interact to define problems, vet solutions, and work towards agreement. But, as Frank Baumgartner et al. conclude, this process "works in favor of the status quo."[12] Similarly, Conlan et al. note that coalition-

5. THE FEDERALIST NO. 10 (James Madison).

6. *See generally* ARTHUR BENTLEY, THE PROCESS OF GOVERNMENT (Peter H. Odegard ed., 1967); DAVID TRUMAN, THE GOVERNMENTAL PROCESS: POLITICAL INTERESTS AND PUBLIC OPINION (1951).

7. *See generally* THEODORE J. LOWI, THE END OF LIBERALISM (1969).

8. E.E. SCHATTSCHNEIDER, THE SEMI-SOVEREIGN PEOPLE: A REALIST VIEW OF AMERICAN DEMOCRACY 35 (1960).

9. *See generally* ALLAN J. CIGLER & BURDETT LOOMIS, INTEREST GROUP POLITICS (1990); FRANK BAUMGARTNER & BETH LEECH, BASIC INTERESTS: THE IMPORTANCE OF GROUPS IN POLITICS AND IN POLITICAL SCIENCE (1998); KAY LEHMAN SCHLOZMAN & JOHN T. TIERNEY, ORGANIZED INTEREST AND AMERICAN DEMOCRACY (1986).

10. Hugh Heclo, *Issue Networks and the Executive Establishment, in* NEW AMERICAN POLITICAL SYSTEM (Anthony King ed., 1978).

11. JOHN KINGDON, AGENDAS, ALTERNATIVES, AND PUBLIC POLICIES 122–28 (1984).

12. FRANK BAUMGARTNER, JEFFREY BERRY, MARIE HOJNACKI, DAVID KIMBALL & BETH LEECH, LOBBYING AND POLICY CHANGE: WHO WINS, WHO LOSES, AND WHY 65 (2009).

building strategies in the pluralist pathway "tend to favor relatively modest, noncontroversial, and incremental initiatives."[13]

The *partisan pathway* requires a strong party leader and party unification towards a policy goal and can achieve more dramatic policy change. Political parties, in theory, represent broader social interests and perspectives that can serve as a basis for policy action than do interest groups. This "responsible party model" assumes, however, that party members are unified in agreement and will be disciplined in working towards goals.[14] American political parties rarely achieve such agreement or discipline.[15] When they do, it almost always requires presidential leadership, as illustrated by the policy changes ushered in by President Franklin Roosevelt's New Deal and President Lyndon Johnson' Great Society programs, and partisan support by congressional leadership, as recently evidenced by President Barak Obama's Affordable Care Act and President Donald Trump's tax cuts. However, as Conlan et al. point out, presidential leadership and partisan congressional majorities are often brief and result in countermobilization by the other party.[16] Given the range of viewpoints embraced in the American two-party system, it is unusual for partisan political power to align behind a particular policy position and to sustain that position. Countermobilization is likely to occur from the other party as well as from factions within the party initiating change, both of which often render partisan change fragile.

The *expert pathway* provides visibility and legitimacy to policy experts in academia, bureaucracies, and think tanks whose ideas have been developed and refined in specialized policy communities where consensus has opportunities to develop. Conlan et al. note experts "have come to play growing roles in policymaking" with "professional knowledge and technical feasibility becom[ing] the source of legitimacy against which all proposals are based."[17] They acknowledge that the expert pathway will need to compete with other pathways but as those pathways become more polarized, "analysis and evidence is likely to be prized as much for the ammunition it provides for entrenched interest group, partisan and ideological positions as for its contribution of new and important ideas."[18] They also point out that experts have become more integrated into government bureaucracies, interest groups,

13. CONLAN, *supra* note 2, at 29.

14. Evron M. Kirkpatrick, *Toward a More Responsible Two-Party System*, 65 AM. POL. SCI. REV. 965, 966–67 (1971).

15. SAMUEL P. HUNTINGTON, AMERICAN POLITICS: THE PROMISE OF DISHARMONY (1983).

16. CONLAN, *supra* note 2, at 52–53.

17. *Id.* at 61.

18. *Id.*

and political parties, but they suggest that experts can be distinguished because of "their adherence to professional norms and values of a professional community"[19] rather than institutional loyalty. Experts are active in the policy communities, referred to above in reference to the pluralist pathway, but if they are acting as experts, they would be taking positions more in line with their professional values than with the interests of their organizations. Conlan et al. conclude that the expert pathway "is alive in our system, if not always well"[20] as it has to compete with other pathways for influence and political trends do not necessarily provide continuous support as actors in other pathways will strive to challenge the influence of experts.

The *symbolic pathway* highlights the role of the media and tends to be used for issues that can be simplified and involve values or notions of right and wrong. Goals of policies in the symbolic pathway tend to be abstract, focused on widely held legislative ends rather than complex questions and making coalition building much easier but likely to result in "poorly understood public policies."[21] Although the symbolic pathway may seem to result in quick resolution of a policy, the pathway tends to have negative consequences, including "producing unexpected outcomes . . . and defer[ring] key policy choices and debate until after policy passage or adoption."[22] It is also difficult to control.[23]

Policymaking for a particular issue—be it gun control, climate change, health care reform, or privacy—is not predetermined to take a certain pathway. And once started on a pathway, it is not relegated to continue on that pathway. Indeed one of the lessons of Conlan et al.'s research and analysis is that policy actors should look at the policy process strategically—"policies are often fought over by different actors in the political system who strive to gain control over the process by routing consideration of the policy onto a pathway that maximizes their resources and power in the system."[24] Different types of policy actors are more likely to find success in achieving their goals and building coalitions on different pathways. As alluded to above, interest groups are more likely to succeed on the pluralist pathway, party leaders on the partisan, policy specialists and bureaucrats on the expert, and policy advocates and entrepreneurs on the symbolic. Political parties and interest groups tend to be

19. *Id.* at 67.
20. *Id.* at 82.
21. *Id.* at 92.
22. *Id.* at 97.
23. *Id.*
24. *Id.* at 12.

attracted to aspects of the symbolic pathway in their attempts to frame issues in broad, emotive terms that help to mobilize their members.

An understanding of these pathways can help policy actors to try to direct discussion of a policy to a pathway that is likely to result in an outcome favorable to them. Policy actors who want to be strategic in terms of setting an issue on a particular pathway need to start by *defining the issue*. Definitions, or framing, of policy issues are not predetermined by the issues but instead are matters of interpretation and emphasis and are, in effect, political decisions.[25] Conlan et al. note that "political leaders and policy actors alike are quite opportunistic in reshaping the definition of issues and institutions to manipulate the pathways to favor their position."[26] If an issue can be redefined so that it shifts to a different pathway, those who benefited from the previous definition lose their leverage unless they adapt their strategies to the shift. Conlan et al. caution: "When issues take an expert turn, groups skilled in the pluralistic pathway may further develop their research capabilities to challenge expert-based arguments against their claims."[27]

Not surprisingly, each pathway carries certain political liabilities.[28] Because the pluralist pathway does not consider all interests equally and does not successfully secure broad policy goals, policy actors who are not advantaged by that pathway can strategize to mobilize actors on alternative pathways. This can be accomplished, for example, by encouraging political leaders, such as presidential candidates, to advocate for broader policy change and thus shift policy discussions from the pluralist pathway to the partisan. Similarly, policies decided in a partisan fashion often exclude affected interests that reassert themselves and move policymaking to the pluralist pathway, where their interests are more likely to be recognized and advantaged. Likewise, policy decisions reached through the expert pathway will engender opposition from interest groups if the policy imposes additional costs on the typical operations of these interest groups. The affected interest groups will then respond by trying to transfer policymaking to the pluralist pathway. Policies arrived at through the expert pathway may also disadvantage broader interests and parties may become involved and try to shift policymaking to the partisan pathway. Finally, policy decisions resulting from the symbolic pathway generally are made quickly and may be infeasible over time, allowing interests or experts to shift subsequent policymaking to the pluralist or expert pathway.

25. KINGDON, *supra* note 11.
26. CONLAN, *supra* note 2, at 111–12.
27. *Id.* at 113.
28. *Id.* at 196.

The policy pathway framework envisions a dynamic and fluid environment. Conlan et al. conclude that: "The system is now positioned to encourage more pathway switching in more directions than have traditionally been recognized."[29] Policy actors are more sophisticated and more adept at marshalling issue definitions and resources so that they can cross pathways. The next Part will explore privacy policymaking through the lens of the pathway framework.

III. PATHWAYS OF PRIVACY POLICYMAKING

Using the pathways framework to analyze the history of information privacy policymaking helps to reveal the dynamics of policy decisions and the players who have been most influential in making those decisions. Most information privacy policymaking in the United States has taken the pluralist pathway with well-organized special interests seeking to limit any restrictions on their information practices. Initially, one might have expected that information privacy policy would take the symbolic pathway as the policy issue or problem was framed in rather symbolic terms as reflected in titles of books from the 1960s—*On Record: Files and Dossiers in American Life*, *The Naked Society*, *The Privacy Invaders*, *The Assault on Privacy*, *The Death of Privacy*, and *Privacy and Freedom*.[30] Although media coverage was far different then than now, the media did cover this issue from the perspective of people being defined by what was in their computerized files with a serious diminution of their privacy. In this scenario, technology was seen as the threat and, as Arthur Miller argued, "man must shape his tools lest they shape him."[31]

The discussion in Congress also adopted symbolic language and images and framed the policy issue as privacy threatened by technology. At the earliest congressional hearings on the possible establishment of a Federal Data Center, the chair of the Special Subcommittee on the Invasion of Privacy defined the policy problem of "The Computerized Man" in these terms: "Through the standardization ushered in by technological advance, his status in society would be measured by the computer and he would lose his personal identity."[32] Although symbols, rather than information practices or interests, dominated

29. *Id.* at 198.

30. MYRON BRENTON, THE PRIVACY INVADERS (1964); ARTHUR MILLER, THE ASSAULT ON PRIVACY (1971); VANCE PACKARD, THE NAKED SOCIETY (1964); JERRY ROSENBERG, THE DEATH OF PRIVACY (1969); ALAN WESTIN, PRIVACY AND FREEDOM (1967); STANTON WHEELER, ON RECORD: FILES AND DOSSIERS IN AMERICAN LIFE (1969).

31. MILLER, *supra* note 30, at 8.

32. *The Computer and Invasion of Privacy: Hearings Before a Subcommittee of the Committee on Government Operations*, 89th Cong. 2 (1966).

these early hearings, Congress quickly recognized the need to understand how federal agencies actually handled personal information, and, at that point, the federal agencies' interest in efficiency came into play. The next round of congressional policy formulation involved a four-year study of government data banks,[33] as well as similar studies by the Department of Health, Education and Welfare (HEW)[34] and by the Russell Sage Foundation and the National Academy of Sciences.[35] One might characterize this policy moment as something of a battle over which pathway policymaking would take—the framing of privacy threatened by technology pushed it towards the symbolic, the interests of organizations in controlling their own information practices in a way that kept them efficient steered discussion into the pluralist pathway, and a need to understand the technical capacities of computerization led policy discussion to the expert pathway.

By the time these studies were completed and bills were introduced, interests dominated the policy process as public and private organizations realized that giving individuals control over their personal information would decrease organizational control over a critical resource and increase organizational costs. The details of this are told elsewhere,[36] but the result was the Privacy Act of 1974, which only affected federal agencies and reflected the minimum protection of information privacy that was advocated at that time. The next step in policymaking was the Privacy Protection Study Commission (PPSC), tasked with investigating private sector personal information practices and making recommendations to Congress. The PPSC conducted its investigations on a sector-by-sector basis, hearing from over three hundred private sector witnesses who advocated against government regulation and new laws and, instead, argued that they could best monitor their own information practices and protect privacy.[37] The privileging of the firms who would be affected by policy steered policymaking solidly onto the pluralist pathway, and the PPSC concluded, in line with the interests of the firms, that a voluntary (i.e., self-regulatory) approach rather than a regulatory approach should be the initial approach.

33. *Federal Data Banks, Computers and the Bill of Rights: Hearings Before the Subcommittee on Constitutional Rights of the Committee on the Judiciary United States Senate*, 92nd Cong. (1971).

34. *See* SEC'Y'S ADVISORY COMM. ON AUTOMATED PERS. DATA SYS., RECORDS, COMPUTS. & THE RIGHTS OF CITIZENS, U.S. DEP'T OF HEALTH, EDUC., & WELFARE, (Report of the Secretary's Advisory Committee of Automated Personal Data Systems) (1973).

35. *See* ALAN F. WESTIN & MICHAEL A. BAKER, NAT'L ACAD. OF SCIS., DATABANKS IN A FREE SOCIETY: COMPUTERS, RECORD-KEEPING, AND PRIVACY (1972).

36. REGAN, *supra* note 1, at 77–83.

37. *See* PRIVACY PROT. STUDY COMM'N, PERSONAL INFORMATION IN AN INFORMATION SOCIETY (1977).

In the 1980s, when the symbolism of information privacy highlighted surveillance[38] and the "Shadow of Orwell,"[39] there was a brief opportunity (coinciding with the year 1984) when the symbolic pathway may have become dominant. At the same time, circumstances were favorable for the expert pathway to play a role with a study by the congressional Office of Technology Assessment (OTA) examining how federal agencies were using computers to process and exchange personal information and hearing from experts in computerization, civil liberties and privacy, and government operations. The OTA report warned that "computer networking is leading rapidly to the creation of a *de facto* national database containing personal information on most Americans."[40] However, once the congressional debates on legislation began, interests again prevailed and shifted policy discussion to efficiency and detection of fraud, waste, and abuse. The result was passage of watered-down legislation[41] despite what might have been termed "expert" findings from OTA that there was no firm evidence to support claims of efficiency and cost savings.

Space does not permit a full review of the policy history of information privacy, but the focus on sectoral policy development in the late 1980s and into the 1990s is illustrative of policymaking steered by interests on a pluralist pathway,[42] as is the stakeholder approach taken by the National Information Infrastructure (NII) task forces in the Clinton/Gore administration. Privacy was one of several topics discussed by the NII Task Force and, in April 1997, an options paper was released for public comment raising the question of how best to implement fair information practices "that balance the needs of government, commerce, and individuals, keeping in mind both our interest in the free flow of information and in the protection of information privacy."[43] The Task Force noted the possibility that "demand could foster a robust,

38. *Privacy and 1984: Public Opinions on Privacy Issues: Hearings Before a Subcommittee of the Committee on Government Operations House of Representatives*, 98th Cong. (1984).

39. Symposium, *Information Law and Ethics: In the Shadow of Orwell – the Citizen and Government*, AM. BAR ASS'N (1984), as noted in REGAN, *supra* note 1, at 93.

40. STAFF OF U.S. CONG. OFFICE OF TECH. ASSESSMENT, FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: ELECTRONIC RECORD SYSTEMS AND INDIVIDUAL PRIVACY (1986).

41. *See* Computer Matching and Privacy Protection Act of 1986, Pub. L. No. 100-503.

42. *See*, *e.g.*, Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721 (2018); Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191; Video Privacy Protection Act of 1988, Pub. L. No. 100-618, 102 Stat. 3195 (codified at 18 U.S.C. § 2710 (1988); Cable Communications Policy Act of 1984, Pub. L. No. 98-549, 98 Stat. 2779.

43. Info. Policy Comm. & Nat'l Info. Infrastructure Task Force, *Options for Promoting Privacy on the National Information Infrastructure*, OFFICE OF THE ASSISTANT SEC'Y FOR PLANNING & EVALUATION (Apr. 1, 1997), https://aspe.hhs.gov/report/options-promoting-privacy-national-information-infrastructure.

competitive market for privacy protection. . . . [and] that privacy could emerge as a market commodity in the Information Age," but also discussed the ways in which the government could facilitate the development of a privacy market and enforce self-regulation, and the possibility of the creation of a federal privacy entity.[44] Based in part on the report of the Task Force, the Clinton Administration's *Framework for Global Electronic Commerce* concluded that: "We believe that private efforts of industry working in cooperation with consumer groups are preferable to government regulation, but if effective privacy protection cannot be provided in this way, we will reevaluate this policy."[45]

IV. EXPERTS IN POLICYMAKING

A. SKEPTICISM/AMBIVALENCE

Expert involvement in public policymaking in the United States has generally been somewhat controversial. Although there is broad recognition that policies should be based on facts and evidence, there is a stronger recognition that policymaking is an inherently political process and that policy choices should reflect a political choice. Criticisms of "technocratic" decision-making that surfaced in the 1970s reflected early debates about distinctions between "facts" and "values" and the importance of the latter in policymaking, as well as distinctions between "politics" and "administration."[46] In a 1970 review of four books on public policy, Ted Lowi voiced these concerns: "Being instrumental and technocratic means that the analyst becomes blinded to certain fundamental political patterns that his individualist and informal view defines away."[47]

A parallel development in the 1970s was interest in "evidence-based policymaking," which did not fully take off until the 1990s but brought new attention to the role of experts, not only in administrative decision-making but in congressional policymaking. Evidence-based policymaking has roots in rational decision-making and the recognition that evidence should be used to better understand the nature and extent of social problems, inform decisions about the effectiveness of policy options, and evaluate how well existing

44. *Id.*

45. William J. Clinton & Albert Gore, Jr., *A Framework for Global Electronic Commerce*, WHITE HOUSE, https://clintonwhitehouse4.archives.gov/textonly/WH/New/Commerce/read.html (last visited Aug. 13, 2020) (emphasis added).

46. Woodrow Wilson, *The Study of Administration*, 2 POL. SCI. Q. 197, 197–222 (1887).

47. Theodore Lowi, *Decision Making vs Policy Making: Toward an Antidote for Technocracy*, 30 PUB. ADMIN. REV. 314, 319 (1970).

policies have worked to address problems.[48] In order for evidence-based policymaking to be incorporated into the policy process, a political culture allowing for transparency and rationality in the policy process and a research culture encouraging an analytical commitment to rigorous methodologies for generating policy-relevant evidence are both required.[49] In response to renewed congressional interest in evidence-based policymaking, the Bipartisan Policy Center issued a two-volume report on the use of evidence in Congress. Volume One identified sixteen barriers to congressional use of evidence including: perception barriers such as unclear relevance of evidence; institutional barriers such as lack of collaborative decision-making structures and congressional expertise; and systemic barriers such as challenges related to norms, incentives, and transparency.[50]

As more and more policies involve choices involving knowledge and understanding of science and technology, and as more and more policies become complex and inter-related, the role of experts in policymaking is again receiving new scholarly and public attention. At the same time, however, there is a backlash against facts themselves—resulting in what one commentator has termed the "death of expertise"[51] and another "the age of American unreason."[52] Resistance to intellectual authority and anti-rationalism have been a constant characteristic of American culture as Richard Hofstadter has documented,[53] but what is more novel is the abundance of data allowing policymakers, and people, to cherry-pick facts that confirm their preferred explanations.

B. FORUMS FOR EXPERT INPUT

In addition to some skepticism about the role of experts in policymaking generally, there are questions about when and how experts should be involved. Is expert input possibly most critical, as suggested above, at the early stages of policy formation (issue definition) and policy formulation (consideration of policy options/alternatives)? And if so, is that best conveyed through study reports and congressional testimony? Do experts then recede into the

48. Ian Sanderson, *Evaluation, Policy Learning, and Evidence-Based Policymaking*, 80 PUB. ADMIN. 1, 4 (2002).

49. Brian W. Head, *Reconsidering Evidence-Based Policy: Key Issues and Challenges*, 29 POL'Y & SOC'Y 77, 78–79 (2010).

50. *See* NICK HART, EDWARD DAVIS & TIM SHAW, BIPARTISAN POL'Y CTR., EVIDENCE USE IN CONGRESS: CHALLENGES FOR EVIDENCE-BASED POLICYMAKING (2018), https://bipartisanpolicy.org/wp-content/uploads/2019/03/BPC-Evidence-Use-in-Congress.pdf.

51. TOM NICHOLS, THE DEATH OF EXPERTISE (2017).

52. SUSAN JACOBY, THE AGE OF AMERICAN UNREASON (2008).

53. *See generally* RICHARD HOFSTADTER, ANTI-INTELLECTUALISM IN AMERICAN LIFE (1962).

background during policy adoption, at which point their positions are weighed against interests and values, translated by political actors, and become part of the final decision? Does expert input continue to be important as policies are implemented in executive agencies, and do those forums become another critical point where experts might reassert influence lost during policy adoption? And similarly, is expert opinion on how well policies are working as intended taken seriously during policy evaluation through either agency reports, congressional hearings, or outside studies? Arguably, expert input is important throughout the stages of the policy process although in different forums and with slightly different purposes.

Conlan et al. identify four circumstances where the roles of experts are likely to be most significant.[54] The first is *rationalizing changes to established policies* (not new) that have not been working as intended.[55] The second is for *low-conflict, low salience issues* on which other policy actors see minimal effect on their own interests.[56] The third area is *highly complex issues* where other actors recognize that they do not understand the risks involved.[57] The fourth are issues on which other policy actors are not engaged or only limitedly engaged, which is most likely to occur at the *initial stage of defining a policy problem*.[58] However, if experts are not able to reach and sustain a consensus based on their professional knowledge and research, they are likely to be viewed as political operatives and have limited influence.

C. POLITICAL DYNAMICS

There are at least two different views of how seriously Congress is likely to consider expert analyses and policy preferences. Kevin Esterling's research suggests that the uncertainty that is attendant with policy proposals presents risks for members of Congress, and the level of risk that members perceive from interest groups affects to what extent members consider expert input.[59] Drawing on an examination of policymaking for emissions trading, school choice, and the adoption of health maintenance organizations, Esterling finds that interest groups, under conditions of ambiguity and uncertainty, do provide neutral expertise and not merely information that enhances their positions.[60] But others point out that on any number of issues "expertise and strong

54. *See* CONLAN, *supra* note 2, at 75–78.
55. *Id.*
56. *Id.*
57. *Id.*
58. *Id.*
59. *See generally* KEVIN ESTERLING, THE POLITICAL ECONOMY OF EXPERTISE (2004).
60. *See generally id.*

consensus on factual matters have been trumped by ideology."[61] Other research suggests that Congress relies upon its own congressional staff agencies—the Congressional Budget Office, Government Accountability Office, Congressional Research Service, and formerly the Office of Technology Assessment—for policy advice, somewhat independent of the level of interest group consensus. David Whiteman, for example, finds that, although congressional members and staff have formed initial policy preferences, they use expert analysis in development of the conceptual framing of the policy debate and in the concrete details of policy proposals.[62] His research reveals that for many policy issues there is a core group of legislators who are heavily involved in policy deliberations and whose offices interact regularly with experts in congressional agencies.[63]

There also appear to be two dynamics at play as experts get involved in policymaking.[64] The first is that if an issue is solidly on the expert pathway, then professional knowledge and technical feasibility are privileged and become the lodestar against which proposals are evaluated. Experts dominate and are viewed as legitimate because their knowledge is critical to successful policy. The second is that experts can be co-opted to lend support for the policy positions of interest groups or parties or ideological groups. Conlan et al. recognize this possibility, noting that "the proliferating range of scientists, economists, and policy analysts employed by contending interests . . . challenges the credibility of expert communities."[65] In this case, an issue is not on the expert pathway but one of the other three pathways, and the influence of experts is limited to how their expertise supports others. The question then becomes: for what issues are experts likely to be viewed as so critical to policy resolution that an issue can ride the expert pathway?

Conlan et al. examined forty-two legislative policies within eight different policy areas to identify the main policy pathway used for getting an issue on the agenda and securing its passage for each legislative decision.[66] The only one of the eight policy areas which never used the expert pathway was gun control, for which the pluralist, partisan, and symbolic pathways were instead used. In some cases, it is fairly obvious why experts would play a major role in policy development and passage. For example, tax policy requires a detailed understanding of existing tax laws, the implications of those laws on different

61. Burdett Loomis, Book Review, 34 PERSP. ON POL. SCI. 125, 173 (2005).

62. *See generally* DAVID WHITEMAN, COMMUNICATION IN CONGRESS (1995).

63. *See generally id.*

64. CONLAN, *supra* note 2, at 61.

65. *Id.* at 9, 198.

66. *See generally* CONLAN, *supra* note 2 (the eight areas are health care, gun control, farm policy, tax legislation, welfare policy, financial regulation, federal mandates, and budget policy).

groups, and the effects of proposed changes. However, only two of seven laws passed from 1981 to 2001 rode the expert pathway.[67] One might similarly expect budget policy to take the expert pathway, but only one of five laws from 1985 to 2011 did so.[68]

Factors other than the substance of the issue must, therefore, play a role in the choice of pathways. Conlan et al. suggest that members of Congress inject considerations pertaining to their reelection prospects when evaluating whether to involve experts.[69] They identify four factors that members are likely to consider in the choice to involve experts in a meaningful way in the policy process: *shame* or the fact that experts have gained public status and credibility on an issue which allows politicians to align with them against narrow interests that had controlled an issue; *competition* when one set of political actors is making expert-based claims and those opposed initiate the involvement of other experts to counter those claims; *conflict management* for issues where agreement on empirical facts can establish a baseline and control the scope of conflict; and *blame avoidance* for issues on which political actors want to insulate themselves from political opposition on hard choices.[70]

The following sections will examine the likelihood that, and circumstances under which, experts will play a dominant role in information privacy policymaking.

V. EXPERTS IN INFORMATION PRIVACY POLICYMAKING IN THE 2000S AND BEYOND

Before examining policymaking in the 2000s, it is important to describe the policy environment and arenas that previous policy initiatives had established as the working environment for information privacy development and implementation. With respect to federal agencies, the locus of policy responsibility was primarily the Office of Management and Budget (OMB). With respect to private sector organizations, the locus was the Federal Trade Commission (FTC) with its jurisdiction over unfair and deceptive trade practices. With respect to organizations operating at the state level, state Attorneys General (AG) had varying level of authority. Looking at these three arenas from an expert perspective, the primary actors at the OMB are government bureaucrats who are often lawyers, at the FTC are lawyers and

67. *See id.* at 110–11
68. *See id.*
69. *See id.* at 81–82.
70. *Id.*

economists,[71] and at AG offices are lawyers.[72] Although it may well be the case that these lawyers have backgrounds in other areas, their shared expert orientation to an issue would be legal, and they are likely to adopt a fairly narrow policy perspective based on an interpretation of the current law and precedents.

During this time, however, three factors were changing the policy landscape in ways that did not fundamentally reflect a legal perspective and that necessitated different types of expertise. The first factor was *technological changes* in computer, information, and communications technologies, and the concomitant development of "big data" and the Internet of Things.[73] The experts needed to understand the changes, as well as the likely implications of the changes, were computer and data scientists—some of whom were in academia, a few in government agencies such as the National Telecommunications and Information Administration (NTIA), but most employed by the companies spearheading the innovations. The second factor was *industry changes* and the rise of large internet platforms and multiplication of both small, start-up, internet-based companies and consolidation of large internet companies.[74] The experts needed here were financial and industry analysts with backgrounds in economics or business administration—some of whom were in government agencies such as the FTC and Department of Commerce, but many of whom were again employed by the companies involved. The third was *international policy actions* by other countries and regional bodies, which affected the range of legitimate information practices by the U.S.-based companies. The necessary experts here are less well-defined but likely to include foreign policy actors and international lawyers—some of whom are in government agencies including the State Department, Commerce Department, and the Office of the U.S. Trade Representative.

During the early 2000s, public interest in online privacy increased initially because of concerns about identity theft and online tracking of activities, then

71. *See generally* CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY (2016).

72. Danielle K. Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747 (2017), https://scholarship.law.nd.edu/ndlr/vol92/iss2/5.

73. *See generally* David Gewirtz, *Technology that Changed Us: The 2000's, from iPhone to Twitter*, ZDNET (May 29, 2018), https://www.zdnet.com/article/technology-that-changed-us-the-2000s/.

74. Makada Henry-Nickie, Kwadwo Frimpong & Hao Sun, *Trends in the Information Technology Sector*, BROOKINGS INST. (Mar. 29, 2019), https://www.brookings.edu/research/trends-in-the-information-technology-sector/; Bryan Martin, *Tech Boom 2.0: Lessons Learned from the Dot-Com Crash*, WIRED (Aug. 2013), https://www.wired.com/insights/2013/08/tech-boom-2-0-lessons-learned-from-the-dot-com-crash/.

because of concerns about data breaches, and more recently because of concerns about mobile tracking, flows of personal data through apps, and organizational uses of artificial intelligence.[75] During this time, there are three significant trends in congressional interest in privacy policymaking. The first is that more congressional committees or subcommittees exerted jurisdiction over information and data privacy issues reflecting the complexity and interrelatedness of the issue. During earlier congressional deliberations, the locus of responsibility was generally with judiciary committees or subcommittees but, as can be discerned from Appendix A, commerce committees and subcommittees dominate, taking both a consumer protection and a technology perspective, with decreased interest from the judiciary.[76] Second is that, regardless of the subject of the congressional hearings, most of the witnesses were from industry. Of the 286 witnesses testifying at thirty-eight major congressional hearings on information privacy from 2010 to 2019, over half (174) were from technology companies or industry-related organizations while twenty-six witnesses were from public interest groups, twenty-eight were academics or lawyers, thirty-five were government officials, and five were from other entities (e.g., international).[77] Finally, despite the number of bills introduced, no legislation passed, which could signal a lack of consensus among experts or the dominance of interests.

This leaves us with a critical question about whether one can distinguish who the experts are and whether they can be differentiated from the interests. The 2012 Obama Administration's policymaking around its proposed Consumer Privacy Bill of Rights and around its Big Data report can both be analyzed to explore an answer. Instead of leaving deliberations on the proposed bill to congressional committees, the White House tasked the NTIA, part of the Commerce Department and last involved with information privacy during the Clinton Administration's stakeholder processes addressing the NII, with "convening interested stakeholders—including companies, privacy advocates, consumer groups, and technology experts—to develop and implement enforceable codes of conduct that specify how the principles in the

75. Alex Hern, *Internet Privacy: The Apps that Protect You from Your Apps*, GUARDIAN (Feb. 16, 2020, 2:00 AM), https://www.theguardian.com/technology/2020/feb/16/internet-privacy-settings-apps-to-protect-you- [https://perma.cc/V7YF-8KZQ]; Timothy L. O'Brien, *Identity Theft Is Epidemic. Can It Be Stopped?*, N. Y. TIMES (Oct. 24, 2004), https://www.nytimes.com/2004/10/24/business/yourmoney/identity-theft-is-epidemiccan-it-be-stopped.html [https://perma.cc/R9HJ-N3JH].

76. *Infra* app. A.

77. *Id.*

Consumer Privacy Bill of Rights apply in specific business contexts."[78] The NTIA also issued a request for public comment on the proposed bill. The NTIA specifically defined this initiative as a "multistakeholder process," and the NTIA was designated as the forum for discussion with a role to mediate or facilitate consensus building among stakeholders.[79] To some extent, one can interpret the Obama Administration's strategy as a testing of all four pathways—symbolic because of the use of "bill of rights"; pluralist because of the "stakeholder" perspective; partisan because of an exertion of executive control; and expert because of the specified inclusion of "technology experts," the only stakeholders explicitly accorded the expert label.[80]

The Obama Administration's approach yielded eighty-seven comments,[81] overwhelmingly from industry groups. Comments were submitted by major internet-related businesses, including Facebook, Visa, Mozilla, Microsoft, AT&T, eBay, Verizon and Intel. Additionally, comments were submitted by key industry associations including the Retail Industry Leaders Association, Software and Information Industry Association, Application Developers Alliance, Marketing Research Association, Interactive Advertising Bureau, National Cable and Telecommunications Association, Direct Marketing Association, Internet Commerce Coalition, and CTIA-The Wireless Association. Privacy and consumer groups also submitted comments, including from the Electronic Privacy Information Center (EPIC), ACLU, Privacy Rights Clearinghouse, Center for Digital Democracy and Consumer Watchdog, but they were far outnumbered by industry groups. NTIA also held a multistakeholder meeting, which also yielded no concrete results and was not surprisingly dominated by industry groups.[82] Although a mere accounting of the number of groups commenting is not sufficient to determine the policy pathway, it does shed light on the fact that industry related groups were in the majority. Although these groups may indeed have expertise on technological

78. Lawrence E. Strickling, *Moving Forward with the Consumer Privacy Bill of Rights*, NTIA (Feb. 29, 2012), https://www.ntia.doc.gov/blog/2012/moving-forward-consumer-privacy-bill-rights. On February 23, 2012, the White House released *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy*, https://obamawhitehouse.archives.gov/sites/default/files/privacy-final.pdf.

79. *Comments on Multistakeholder Process*, NTIA (Apr. 3, 2012), https://www.ntia.doc.gov/federal-register-notice/2012/comments-multistakeholder-process?page=1 (comments received by Apr. 3, 2012).

80. *Id.*

81. *Id.*

82. Jeff Chester, CTR. FOR DIG. DEMOCRACY, HEAD IN THE DIGITAL SAND: HOW THE OBAMA ADMINISTRATION'S NTIA-LED MULTISTAKEHOLDER EFFORT DOESN'T DELIVER ITS PROMISED PRIVACY BILL OF RIGHTS (2013), https://www.democraticmedia.org/sites/default/files/CDDPrivacyObamaAdmReportAugust2013.pdf.

capacities and consumer behavior, that expertise is in the context of the industry and most likely framed in terms of the interests of the industry, and not professional norms and values. The proposed consumer privacy bill made little headway.

Likewise, the process during the Obama Administration around big data employed a multistakeholder process with industry groups again playing a major role but with more input from technology experts and public interest groups. This time the process was co-managed by several executive departments, including the Department of Commerce, Department of Energy, Office of Science and Technology Policy (OSTP), and National Economic Council, and involved outreach to academic experts, industry representatives, privacy advocates, civil rights groups, law enforcement agents, and other government agencies.[83] Three university conferences were organized around the topics of privacy; social, cultural, and ethical dimensions; and governance and values. Stakeholder meetings were convened with over a hundred groups, including major industries, industry associations, and public interest groups.[84] A request for public comment drew over seventy comments, with more balance among stakeholders, though industry-related associations were the largest group of commenters.[85]

As the Executive Office process was underway, the President's Council of Advisors on Science and Technology (PCAST) also undertook a parallel study to assess the technological dimensions of the intersection of big data and privacy. PCAST is explicitly an expert advisory group of scientists and engineers convened in order to better inform the President about policy choices in the area of science, technology, and innovation. Of the sixteen PCAST members, eleven are from universities and four from industry (Google, Microsoft, United Technologies Corporation, Zetta Venture Partners), and one from a non-profit (National Quality Forum).[86]

Both reports raised privacy concerns, particularly regarding fairness and discrimination, as well as acknowledging the societal benefits from appropriate uses of big data and provided policy options for such uses. The White House report identified a number of specific policy recommendations, including

83. EXEC. OFFICE OF THE PRESIDENT, WHITE HOUSE, BIG DATA: SEIZING OPPORTUNITIES, PRESERVING VALUES 3–4 (2014), https://obamawhitehouse.archives.gov/sites/default/files/docs/big_data_privacy_report_5.1.14_final_print.pdf.

84. *Id.* at 70–72.

85. *Id.* at 77–78.

86. PRESIDENT'S COUNCIL OF ADVISORS ON SCI. & TECH., EXEC. OFFICE OF THE PRESIDENT, BIG DATA AND PRIVACY: A TECHNOLOGICAL PERSPECTIVE (2014), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_big_data_and_privacy_-_may_2014.pdf.

passing a Consumer Privacy Bill of Rights and National Data Breach Legislation, as well as amending the Electronic Communications Privacy Act.[87] However, again, no legislative change resulted. Although this multistakeholder process was unsuccessful in generating congressional action, the process itself was more inclusive partly as a result of the university conferences and the inclusion of PCAST, both of which allowed for contribution from experts.

With respect to information privacy policy, the Trump Administration has continued the multistakeholder approach of the Clinton and Obama Administrations. The Commerce Department created an Internet Policy Task Force "to conduct a comprehensive review of the nexus between privacy policy, copyright, global free flow of information, cybersecurity, and innovation in the Internet economy."[88] The Task Force was intended to "leverage expertise" and emphasized the importance of trust in the digital environment. The National Institute of Standards and Technology (NIST) was charged with developing a voluntary privacy framework to help organizations manage risk while NTIA was charged with modernizing U.S. data privacy policy and proposed focusing on outcomes of organizational data practices rather than specifying requirements for those practices.[89] NTIA's request for public comment on the proposed outcomes yielded 217 comments.[90] More individuals commented than in response to previous requests, but, again, comments from companies and industry-related groups dominated.

From this brief review of development of information privacy policy in the 2000s in congressional committees, the FTC, the NTIA, and task forces, two conclusions can be drawn. The first is that current policymaking continues to occur primarily in the pluralist pathway as interests tend to dominate policy narratives and decisions. The second is that, although there is recognition that "technology experts" are included in lists of "stakeholders," their input and appearance often occurs as industry employees and voices, not as independent actors with credibility and legitimacy as a result of their technological knowledge and experience. Expertise, and the leverage accorded to expertise,

87. *See* STRICKLING, *supra* note 78.

88. *Internet Policy Task Force*, NTIA, https://www.ntia.doc.gov/category/internet-policy-task-force (last visited Aug. 13, 2020).

89. Press Release, NTIA, NTIA Seeks Comment on New Approach to Consumer Data Privacy (Sep. 25, 2018), https://www.ntia.doc.gov/press-release/2018/ntia-seeks-comment-new-approach-consumer-data-privacy.

90. Press Release, NTIA, NTIA Releases Comments on a Proposed Approach to Protecting Consumer Privacy (Nov. 13, 2018), https://www.ntia.doc.gov/press-release/2018/ntia-releases-comments-proposed-approach-protecting-consumer-privacy.

thus may be undercut or compromised because of their affiliation with an industry or public interest group.

VI. BARRIERS TO EXPERTISE INFLUENCING INFORMATION PRIVACY POLICYMAKING

As noted immediately above, the first barrier is the hegemonic control that affected interests have had on information privacy and their capacity at keeping this issue in the pluralist pathway—an ability that derives from the fact that this is, to a very large extent, the default pathway in U.S. policymaking and is reinforced by the political and economic power of the affected interests. The second barrier is that expertise, particularly technological expertise, is to a large extent embedded in, and integral to, the industries that would be affected by more effective policy. One might, however, expect that as technological factors become a more critical component of information privacy issues, technology experts in particular would be able to exert more independent influence. Three additional factors, which to this point have also been barriers to expertise input but which could be corrected, come into play: the lack of technology expertise in Congress and the FTC; the complexity of information privacy as a policy problem; and the current deferral of policymaking to private entities collecting and using information about people.

The first factor is a barrier which, in theory, could be overcome and which, in practice, has been addressed to some extent. This factor involves the lack of technology expertise in congressional committees and the FTC, which has had primary jurisdiction over information privacy policy. Both relevant congressional committees and the FTC have recognized that their lack of knowledge has weakened their ability to evaluate claims made by industry actors and have taken steps to increase their technological expertise. For example, the FTC has added a Chief Technologist, an Office of Technology Research and Investigation, staff technologists in the Division of Privacy and Identity Protection, and, most recently, a Technology Task Force[91] in the Bureau of Competition (with seventeen lawyers and a number of technology fellows). Latanya Sweeney, during her tenure as Chief Technologist, established positions for Summer Research Fellowships in Technology and Data Governance to bring students with technology backgrounds to the FTC with opportunities to spend a summer "exploring ways to design, create, assess, and analyze technology at its intersection with business, society and

91. Press Release, FTC, FTC's Bureau of Competition Launches Task Force to Monitor Technology Markets (Feb. 26, 2019), https://www.ftc.gov/news-events/press-releases/2019/02/ftcs-bureau-competition-launches-task-force-monitor-technology.

policy."[92] Additionally, the FTC saw this program as an opportunity "to broaden its ability to understand and respond to current topics in technology."[93] Given the academic focus of these programs, it is likely that they will serve as an effective way to bring expertise to the FTC and to inform experts about the operating culture of the FTC.

The second factor appears to be a larger barrier moving forward and involves the complexity of the information privacy environment. As alluded to directly above, the technology in question intersects "with business, society and policy," necessitating not just expertise in technology but also in the dynamics of those intersections. The effect of this is that claims of expertise can (and are) contested, as one cannot draw a clear line from one type of disciplinary expertise to a claim of expertise about the effects of an information practice on privacy. For example, a *lawyer*, based on prior legal precedents in similar areas, can speak to whether a claim about a mobile app's privacy policies raises questions about unfair and deceptive trade practices; a *computer technologist* can explain the technological underpinnings of the app; a *data scientist* can outline how information flows to make the app work and what information flows beyond the app itself; a *behavioral economist* can make predictions about how individuals will respond to the app; a *financial analyst* can evaluate the market effects; a *sociologist* can opine on the larger social and political effects of the app; and an *ethicist* can suggest moral questions posed by uses of the app. In this case, *seven* different professional groups can claim some expertise in policy discussions about the effects of the mobile app on privacy.

The multiplicity of claims to expertise is not entirely unique to privacy. Many policy areas draw on multiple types of experts, but this problem appears relatively greater in privacy policy. Tax policy, for example, draws heavily on three different types of expertise—law, accounting, and economics—each of which makes relevant and unique contributions to policy discussions without being fundamentally at odds. Given the overlap in these areas of expertise and a somewhat common language, it is more likely that an expert consensus can develop.[94] For an issue like privacy, experts are more likely to disagree as they approach the issue with divergent, not complementary, perspectives. As an example, law enforcement often calls for access to encrypted devices and weakening encryption, while people who are experts in the technology understand that it is difficult to do this while maintaining strong encryption and lawyers see Fourth Amendment concerns. Experts with particularized

92. Latanya Sweeney, Save the World, NTIA (Apr. 17, 2014, 4:05 PM), https://www.ftc.gov/news-events/blogs/techftc/2014/04/save-world.

93. *Id.*

94. CONLAN, *supra* note 2, at 121.

areas of expertise are less likely to consider factors outside their area of knowledge, while those with more breadth and depth in their backgrounds are more likely to be able to recognize and negotiate competing claims.

To overcome this barrier of diverse claims of expertise, two possibilities present themselves. The first is to provide academic programs for students in interdisciplinary, or transdisciplinary, studies so that they have both depth and breadth to understand the complexity of the information privacy environment. A number of universities have launched graduate programs along these lines—UC Berkeley, New York University, Carnegie Mellon, and Cornell come immediately to mind.[95] A second is to provide forums that prioritize expert discussion in a manner that will not devolve into interest-group-dominated deliberation. Difficult as it may be to separate the two, an effort to provide some space that queries the technological capacities and implications in an objective manner appears essential if technological experts are to play a meaningful role in public policymaking.

A third factor providing a barrier is the nature of the current policy regime, which gives organizations—both public and private—a great deal of latitude to, in effect, set their own privacy policies. The self-regulatory regime for the private sector in particular provides private companies with control over developing their own privacy notices, including language that can be so vague and obtuse as to be relatively meaningless to a consumer, in addition to control over both enforcement and administration of those policies as well as any grievances arising from them.

VII. ENHANCING THE ROLE OF EXPERTS

The above analysis leads to the conclusion that three complementary changes would reduce the barriers discussed above and enable experts to play a larger role in information privacy policy.

First, the establishment of a source of expertise outside of or independent of industry is critical for experts to have the professional standing to offer advice that is not seen as being in some way affected by industry interests. As mentioned above, there is an academic pipeline that is producing students who are well-versed in the various intersecting expertise central to understanding the implications of various technologies and practices on privacy. But producing experts is not enough to place them in positions where they not

95. *E.g.*, UC Berkeley's Law and Technology certificate program or its graduate programs in Information Management Systems, Carnegie Mellon's Master of Science in Information Technology – Privacy Engineering, and the certificate programs at Princeton's Center for Information Technology Policy.

only can influence policymaking but also exert influence as a recognized professional community. This does not mean that such experts cannot be affiliated with industry, but it does require first that their identity is rooted in their profession and their professional reputation rather than their current position in industry. It also requires that these experts exist in a variety of institutions—public, private, and nonprofit.

If these two requirements were met, it would enable such experts to be recognized as such and to exert professional influence within policy communities discussing options for information privacy. Ken Bamberger and Deirdre Mulligan's research on privacy act officers within companies suggest that this may be occurring, at least at some of the largest companies.[96] Although the results of their research is limited by the small number of their respondents, they did find the emergence of a professional identity informed in part by attendance at conferences and workshops such as the Privacy Law Scholars Conference, the annual meeting of data protection commissioners, and the Computers Freedom and Privacy conference.[97] Bamberger and Mulligan note the role of the International Association of Privacy Professionals (IAPP) in meeting the informational, training, and networking needs of privacy "professionals" through educational programs, conferences, and a credentialing program.[98] Conferences and networking opportunities help privacy experts build and maintain a professional identity, as well as recognized credentialing, that provides not only a shared language and understanding of the issues across organizations, but also a sense of confidence in one's professionalism within the organization with which they are affiliated.

The second change to enable experts to play a more central role in policy development would be a congressional forum that privileges more expert input into the policy process for information privacy than is available through the more political congressional hearing process. Both the Belfer Center on Science and Technology and the National Academy of Public Administration (NAPA) have recently recommended that Congress increase its capacity in science and technology areas, and that it provide more forums for mid-level and long-term identification of policy issues and options. The NAPA report recommended that Congress both enhance the technological expertise and capacity of existing entities, such as the Congressional Research Service (CRS)

96. *See generally* KENNETH A. BAMBERGER & DEIRDRE K. MULLIGAN, PRIVACY ON THE GROUND: DRIVING CORPORATE BEHAVIOR IN THE UNITED STATES AND EUROPE (2015).

97. *See* Kenneth A. Bamberger & Deirdre K. Mulligan, *New Governance, Chief Privacy Officers, and the Corporate Management of Information Privacy in the US: An Initial Inquiry*, 33 L. & POL'Y 477 (2011), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1701087.

98. *See* Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy on the Books and on the Ground*, 63 STAN. L. REV. 247, 262 (2011).

and the Government Accountability Office (GAO), as well as create a new advisory office to increase the capacity of Congress itself.[99] Creating this new office would entail recruiting and hiring science and technology advisors for House and Senate committees with relevant oversight responsibilities.[100] The Belfer Center on Science and Technology similarly concluded that Congress had not given itself the resources needed to efficiently and effectively absorb new information.[101] The study pointed out that, "in legislation and high-profile hearings, Congress has appeared unprepared to reckon with emerging technologies and their effects on society. In recent years, Congress has failed to produce substantive legislation on emerging [science and technology] issues of national import, *like personal data privacy and protections*."[102]

Finally, a serious prospect of legislative action would entice industry to pay attention and provide an opportunity for experts to play a larger role. As Cameron Kerry pointed out, within Congress and within the information privacy community, there is agreement on the key principles; nonetheless, "it is a challenge to articulate these in ways that are concrete without being too prescriptive or too narrow."[103] The shortcomings of the current information privacy approach, relying on Fair Information Principles of notice, choice, and consent, are broadly recognized and necessitate a shift in policy thinking to obligate organizations to responsibly handle personal information. In setting such obligations or duties, Margot Kaminski's conclusion that "both the current penalties and the current levels and kinds of uncertainty in the U.S. privacy regime are not enough to drive industry to the table in efficiency-maximizing ways" is important to consider.[104] She argues that effective policy will require broad standards backed by enforcement, ensuring that that there is uncertainty over what the standards require and, therefore, driving companies to negotiate with the enforcement agency.[105] Bamberger and

99. *See* SCIENCE AND TECHNOLOGY POLICY ASSESSMENT: A CONGRESSIONALLY DIRECTED REVIEW, NAT'L ACAD. OF PUB. ADMIN 51–55 (2019), https://web.archive.org/web/20200405173323/https://www.napawash.org/uploads/Academy_Studies/NAPA_FinalReport_forCRS_110119.pdf.

100. *Id.* at 54–55.

101. *See* MIESEN, *supra* note 1, at 9–12 (2019), https://web.archive.org/web/20200405174107/https://www.belfercenter.org/sites/default/files/2019-09/ST/Building21stCenturyCongress.pdf.

102. *Id.* at 1 (emphasis added).

103. Cameron F. Kerry, *Will This New Congress Be the One to Pass Data Privacy Legislation?*, BROOKINGS INST. (Jan. 7, 2019), https://www.brookings.edu/blog/techtank/2019/01/07/will-this-new-congress-be-the-one-to-pass-data-privacy-legislation/.

104. Margot E. Kaminski, *When the Default Is No Penalty: Negotiating Privacy at the NTIA*, 94 DENVER L. REV. 925, 946 (2016).

105. *Id.*

Mulligan's research further supports the value of such uncertainty. They credit the success of the FTC's divergence from "command-and-control governance" and a " 'reticent regulator' approach," and instead its embrace of regulatory and legal ambiguity which has, in effect, kept companies uncertain and aware of the potential privacy risks of their practices, incentivizing them to take the advice of information privacy experts more seriously.[106]

VIII. CONCLUSION

Although the current policymaking regime for information privacy is dominated by the organizations with interests in a more unrestrained flow of information about individuals and is not conducive to effective and objective input by experts, the above analysis identifies some changes that would help experts to gain footing in policy discourse for this issue. Specifically, this analysis identifies the importance of providing a source of expertise independent of industry, establishing a congressional forum that privileges expert advice over interest group influence, and initiating legislative action that would lead industry to attend more seriously to concerns about information privacy. These changes would provide experts with a reliable forum to operate from, enhanced abilities to cross examine competing claims of expertise, and appropriate recognition in the formulation of policy. As demonstrated by the last fifty years of information privacy policymaking, the current system encourages ineffective political outcomes, marginalized experts, and interest-based loyalty. By enabling a more robust expert pathway for information privacy policymaking, we can begin to chip away at the dominant pluralist pathway and, in the process, make more effective policy choices.

106. BAMBERGER & MULLIGAN, *supra* note 98, at 308.

APPENDIX A – SELECTED INFORMATION PRIVACY CONGRESSIONAL HEARINGS (2010–19)*

Date	Committee	Purpose	Witnesses
December 4, 2019	Senate Committee on Commerce, Science, and Transportation	Examine legislative proposals to protect consumer data privacy, including giving FTC more resources and authority	• Julie Brill, Former Commissioner of the FTC, now at Microsoft • Maureen Ohlhausen, Former Acting-Chair of the FTC, now at 21st Century Privacy Coalition • Laura Moy, Georgetown Law Center on Privacy & Technology • Nuala O'Connor, Walmart • Michelle Richardson, Center for Democracy and Technology
July 16, 2019	Senate Committee on Banking, Housing, and Urban Affairs	Examine Facebook, Inc. proposed development of a new cryptocurrency, called Libra, and a digital wallet to store this cryptocurrency, called Calibra, and to review implications for consumers and potential risks associated with Libra	• David Marcus, Facebook

* Compiled by author and Caroline Ball, GMU MPA student and Graduate Research Assistant. The table includes most of the major information privacy hearings held over the last twenty years. It does not include hearings on communication privacy, student privacy, privacy of health records, or specific issues in one government agency. The primary sources were GovInfo (www.govinfo.gov), Congress.Gov (www.congress.gov), and websites of relevant congressional committees.

Date	Committee	Purpose	Witnesses
May 8, 2019	House Energy and Commerce Committee	Oversight of the Federal Trade Commission: Strengthening Protections for Americans' Privacy and Data Security	• Joseph Simmons, FTC • Noah Joshua Phillips, FTC • Rohit Chopra, FTC • Rebecca Kelly Slaughter, FTC • Christine Wilson, FTC
May 7, 2019	Senate Committee on Banking, Housing, and Urban Development	Privacy Rights and Data Collection in a Digital Economy	• Peter Chase, German Marshall Fund • Jay Cline, PWC • Maciej Ceglowski, Pinboard
May 1, 2019	Senate Committee on Commerce, Science, and Transportation	Examine consumers' expectations for data privacy in the Digital Age and how those expectations may vary based on the type of information collected and processed by businesses.	• Helen Dixon, Republic of Ireland • Neema Singh Guliani, ACLU • Jules Polonetsky, Future of Privacy Forum • Jim Steyer, Common Sense Media
March 26, 2019	Subcommittee on Manufacturing, Trade, and Consumer Protection of Senate Commerce Committee	Data privacy issues that impact small businesses and the unique challenges they face with laws designed for larger companies	• Mr. Justin Brookman, Consumer Reports • Ms. Nina Dosanjh, National Association of Realtors • Mr. Jefferson England, Silver Star Communications • Mr. Evan Engstrom, Engine Advocacy and Research Foundation • Mr. Ryan Weber, KC Tech Council

Date	Committee	Purpose	Witnesses
February 27, 2019	Senate Committee on Commerce, Science, and Transportation	Examine what Congress should do to address risks to consumers and implement data privacy protections for all Americans	• Jon Leibowitz, 21st Century Privacy Coalition • Michael Beckerman, Internet Association • Brian Dodge, Retail Industry Leaders Association • Victoria Espinel, The Software Alliance • Woodrow Hartzog, Professor, Northeastern University • Randall Rothenberg, Interactive Advertising Bureau
February 26, 2019	House Energy and Commerce Committee	Protecting consumer privacy in an era of Big Data	• Brandi Collins-Dexter, Media, Democracy 7 Economic Justice • Dave Grimaldi, IAB • Rosalyn Layton, AEI • Nuala O'Connor, CDT • Denise Zheng, Business Roundtable
September 26, 2018	Senate Committee on Commerce, Science, and Transportation	Examine current privacy policies in top companies, review current privacy laws, discuss possible new safeguards	• Len Cali, AT&T • Andrew DeVore, Amazon • Keith Enright, Google • Damien Kieran, Twitter • Guy Tribble, Apple • Rachel Welch, Charter Communications

Date	Committee	Purpose	Witnesses
August 16, 2018	Senate Committee on Commerce, Science, and Transportation	Examine policy issues before the Commission and review the FCC's ongoing duties and activities	• Ajit Pai, FCC • Michael O'Rielly, FCC • Brendan Carr, FCC • Jessica Rosenworcel, FCC
June 19, 2018	Senate Committee on Commerce, Science, and Transportation – Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security	Follow-up to Zuckerberg hearing, focused on privacy concerns in the wake of Cambridge Analytica	• John Battelle, NewCo • Aleksandr Kogan, University of Cambridge Department of Psychology • Ashkan Soltani, Soltani LLC (formerly FTC)
June 14, 2018	House Committee on Energy and Commerce	Understanding the digital advertising ecosystem	• Robert Glasser, Wunderman • Mike Zaneis, Trustworthy Accountability Group • Justin Brookman, Consumers Union • J. Howard Beales, GW School of Business
April 11, 2018	House Committee on Energy and Commerce	Facebook: Transparency and Use of Consumer Data (Cambridge Analytica)	• Mark Zuckerberg, Facebook
April 10, 2018	Senate Commerce, Science, and Transportation and Judiciary Committees (joint)	Facebook, social media, privacy and the use and abuse of data (Cambridge Analytica)	• Mark Zuckerberg, Facebook

Date	Committee	Purpose	Witnesses
February 6, 2018	Senate Committee on Commerce, Science, and Transportation – Subcommittee on Consumer Protection, Product Safety, Insurance, and Data Security	Examine the Uber breach including coverups, review the value of "bug bounty" programs	• Justin Brookman, Consumers Union • John Flynn, Uber • Mårten Mickos, HackerOne • Katie Moussouris, Luta Security
November 29, 2017	House Committee on Energy and Commerce – Subcommittee on Communication and Technology – Subcommittee on Digital Commerce and Consumer Protection	Discuss companies' use of algorithms to personalize content, review concerns about protecting consumer information, outlining platform privacy policy disclosures	• Catherine Tucker, MIT School of Management • Omri Ben-Shahar, University of Chicago Law School • Kate Klonick, Yale Law School • Michael Kearns, University of Pennsylvania Department of Computer and Information Science • Laura Moy, Georgetown Law Center on Privacy and Technology • Frank Pasquale, University of Maryland Law

Date	Committee	Purpose	Witnesses
November 8, 2017	Senate Committee on Science and Transportation	Protecting consumers in era of major data breaches	• P. Barros, Jr., Equifax • Richard Smith, former Equifax • Marissa Mayer, Yahoo • Karen Zacharia, Verizon • Todd Wilkinson, Entrust Datacard
March 22, 2017	Senate Committee on Commerce, Science, and Transportation	Examine benefits and risks of innovative technologies to combat cyber threats and secure critical infrastructure	• Caleb Barlow, IBM Security • Venky Ganesan, National Venture Capital Association • Steve Grobman, Intel Security Group • Malcolm Harkins, Cylance Corp. • Eric Rosenbach, DOD
March 21, 2017	House Committee on Energy and Commerce – Subcommittee on Communication and Technology	Examine challenges facing broadband infrastructure deployment efforts, review proposals to promote broadband infrastructure development and investment and efforts to improve permitting process	• Steven K. Berry, Competitive Carriers Association • Michael Conners, Saint Regis Mohawk Tribe • Thomas Murray, Community Wireless Structures • Joanne S. Hovis, CTC Technology and Energy • LeRoy T. Carlson, U.S. Cellular • James W. Stegeman, CostQuest Associates • Bryan Darr, Mosaik Solutions

Date	Committee	Purpose	Witnesses
September 8, 2016	Senate Committee on Homeland Security and Governmental Affairs – Subcommittee on Regulatory Affairs and Federal Management	Examine Federal independent agencies regulatory review activities and processes, review proposals for potential improvements to regulatory process	• Adam J. White, Hoover Institution • Cary Coglianese, University of Pennsylvania Law School
July 12, 2016	Senate Committee on Commerce, Science, and Transportation	How will FCC's proposed privacy regulations affect consumers and competition	• Jon Leibowitz, 21st C Privacy Coalition • Dean Garfield, Info Tech Industry Coalition • Paul Ohm, Georgetown Law • Matthew Polka, Am Cable Assoc • Peter Swire, Georgia Inst of Tech
June 14, 2016	House Committee on Energy and Commerce – Subcommittee on Communication and Technology	Reviewing FCC proposed rules to establish consumer privacy requirements for broadband internet access service providers	• Doug Brake, Information Technology and Innovation Foundation • Jon Leibowitz, 21st Century Privacy Coalition • Paul Ohm, Georgetown University Law Center

Date	Committee	Purpose	Witnesses
July 29, 2015	House Committee on the Judiciary – Subcommittee on Courts, Intellectual Property, and the Internet	Examine the Internet of Things, focusing on privacy issues and government regulation	• Gary Shapiro, Consumer Electronics Association • Dean D. Garfield, Information Technology Industry Council • Mitch Bainwol, Alliance of Automobile Manufacturers • Morgan Reed, ACT\The App Association
July 28, 2015	House Committee on Energy and Commerce – Subcommittee on Communication and Technology	Summarizing current FCC activities and policy issues	• Tom Wheeler, FCC • Ajit Pai, FCC
April 29, 2015	House Committee on Oversight and Government Reform – Subcommittee on Information Technology	Examine digital data encryption and options to maintain proper balance between public safety and privacy	• Amy Hess, FBI Science and Technology Branch • Daniel F. Conley, Suffolk County District Attorney • Kevin D. Bankston, New America Open Technology Institute • Jon Potter, Application Developers Alliance • Matthew Blaze, University of Pennsylvania Department of Computer and Information Science

Date	Committee	Purpose	Witnesses
February 11, 2015	Senate Committee on Commerce, Science, and Transportation	Examine Internet of Things (IoT) Internet-connected devices, focusing on concerns over privacy and network security	• Mike Abbott, Kleiner Perkins Caufield and Byers • Douglas Davis, Intel Corp. • Lance Donny, OnFarm Systems • Adam Thierer, George Mason University • Justin Brookman, Center for Democracy and Technology
May 15, 2014	Senate Committees on Homeland Security and Governmental Affairs	Online advertising and hidden hazards to consumer privacy and data privacy	• Alex Stamos, Yahoo • George Salem, Google • Craig Spiezle, Online Trust Alliance • Maneesha Mithal, FTC • Lou Mastria, Digital Advertising Alliance
June 28, 2012	Senate Committee on Commerce, Science, and Transportation	Examine need for Federal privacy regulations to protect consumers from collection of personal information through commercial tracking of individual Internet activities, focusing on status of industry self-regulation efforts and mechanisms	• Bob Liodice, Association of National Advertisers • Alex Fowler, Mozilla Corp. • Peter Swire, Ohio State University • Berin Szoka, TechFreedom

Date	Committee	Purpose	Witnesses
January 31, 2012	Senate Committee on Judiciary	The Video Privacy Protection Act: protecting viewer privacy in the 21st Century	• Melvin Watt, Rep from NC • David Hyman, Netflix • William McGeveran, U of Minn Law • Marc Rotenberg, EPIC • Christopher Wolfe, Hogan Lovells LLP
October 13, 2011	Subcommittee on Commerce, Manufacturing, and Trade of House Committee on Energy and Commerce	Privacy and the collection and use of online and offline consumer information	• Barbara Lawler, Intuit • Mike Hintze, Microsoft • Scott Meyer, Evidon • Linda Woolley, DMA • Allessandro Acquisti, Carnegie Mellon Univ • Pam Dixon, World Privacy Forum
October 5, 2011	House Committee on Energy and Commerce – Subcommittee on Commerce, Manufacturing, and Trade	Examine child privacy issues on the Internet, focusing on adequacy of existing protections under the Children's Online Privacy Protection Act (COPPA) of 1998 and FTC-proposed changes to COPPA	• Mary Engle, FTC • Hemanshu Nigam, SSP Blue • Morgan Reed, Association for Competitive Technology • Stephen Balkam, Family Online Safety Institute • Kathryn Montgomery, American University • Alan Simpson, Common Sense Media

Date	Committee	Purpose	Witnesses
September 15, 2011	House Committee on Energy and Commerce – Subcommittee on Commerce, Manufacturing, and Trade	Examine European Union (EU) regulatory efforts to protect online consumer data, focusing on unintended consequences of EU Data Protection and e-Privacy Directives for commerce, consumers, and businesses	• Catherine Tucker, MIT • Stuart Pratt, Consumer Data Industry Association • Paula Bruening, Hunton and Williams, LLP • Peter Swire, Ohio State University
July 14, 2011	House Committee on Energy and Commerce – Subcommittee on Commerce, Manufacturing, and Trade	Examine consumer Internet privacy issues, and to review Federal efforts to protect consumer privacy	• Edith Ramirez, FTC • Julius Genachowski, FCC • Lawrence Strickling, National Telecommunications and Information Administration
June 29, 2011	Senate Committee on Commerce, Science, and Transportation	Privacy and data security: protecting consumers in the modern world	• Julie Brill, FTC • Cameron Kerry, Dept of Commerce • Austin Schlick, FCC • Stuart Pratt, Consumer Data Industry Assoc • Iona Rusu, Consumers Union • Tim Schaaff, Sony • Thomas Lenard, Tech Policy Inst • Scott Taylor, Hewlett-Packard

Date	Committee	Purpose	Witnesses
May 19, 2011	Senate Committee on Commerce, Science, and Transportation	Consumer privacy and protection in the mobile marketplace	• David Vladeck, FTC • Bret Taylor, Facebook • Morgan Reed, Assoc for Competitive Tech • Catherine Novelli, Apple • Alan Davidson, Google • Amy Guggenheim, Common Sense Media
March 16, 2011	Senate Committee on Commerce, Science, and Transportation	State of online consumer privacy	• Jon Leibowitz, 21st Century Privacy Coalition • Lawrence Strickling, NTIA • Erich Anderson, Microsoft • Ashkan Soltani, Privacy Consultant • Barbara Lawler, Intuit • Chris Calabrese, ACLU
July 27, 2010	Senate Committee on Commerce, Science, and Transportation	Examine online consumer privacy issues and developments, focusing on Government and private industry efforts to protect consumers and assist consumer understanding of and control over privacy protection rights, policies, and mechanisms	• Guy Tribble, Apple • Bret Taylor, Facebook • Alma Whitten, Google • Jim Harper, Cato Institute • Dorothy Attwood, AT&T • Joseph Turow, University of Pennsylvania

Date	Committee	Purpose	Witnesses
April 29, 2010	Senate Committee on Commerce, Science, and Transportation – Subcommittee on Consumer Protection, Product Safety, and Insurance	Examine online safety and privacy issues impacting children, focusing on new technological developments and efficacy of the Children's Online Privacy Protection Act (COPPA) of 1998	• Jessica Rich, FTC • Timothy Sparapani, Facebook • Michael Hintze, Microsoft • Kathryn Montgomery, American University • Marc Rotenberg, Electronic Privacy Information Center • Berin Szoka, Progress and Freedom Foundation

PERFORMING CYBERSECURITY EXPERTISE: CHALLENGES FOR PUBLIC UTILITY COMMISSIONS

Rebecca Slayton†

ABSTRACT

Regulators have evolved organizational processes, capacities, and expertise that aim to balance public goods such as reliability, affordability, and environmental protection. However, cybersecurity is a different kind of good. It requires continual vigilance by experts and continual advancements in their practices as cybersecurity involves intelligent adversaries that seek to undermine it. Regulators have thus expressed concern that neither they nor the companies they regulate have the expertise to ensure that critical infrastructure remains uncompromised. This Article examines such expertise as an authoritative relationship between individuals claiming specialized skills and those without such training. In particular, it considers how public utility commissions help produce critical infrastructure cybersecurity expertise. It argues that the commissions have not merely accessed expertise but have worked with skilled individuals to actively produce expertise. The analysis highlights three contexts and processes for producing such expertise. First, after breaches occur in utility networks, commission experts highlight industry-accepted best practices and standards—not only to explain the breaches, but to emphasize that they possess specialized knowledge that could have prevented such breaches. Second, commission experts maintain ongoing discussions with utilities, such that utility requests for rate recovery associated with cybersecurity investments rarely need to be publicly challenged—a process which might reveal disagreement among experts and undermine authority. Third, when experts are called upon to help establish cybersecurity standards, they have attempted to remain neutral and facilitate agreement among industry experts. However, in the midst of public controversy about appropriate standards, regulators have at times struggled to maintain their authority.

DOI: https://doi.org/10.15779/Z380R9M47Q

† Rebecca Slayton is Associate Professor jointly in the Science & Technology Studies Department and Judith Reppy Institute for Peace and Conflict Studies, both at Cornell University. She is currently working on a book about the history of cybersecurity expertise. This paper is based upon research supported by the National Science Foundation under grant number 1553069.

TABLE OF CONTENTS

I. INTRODUCTION 758

II. THE ORIGINS OF POWER GRID CYBERSECURITY REGULATION 763

A. MAKING THE GRID "SMART"—AND VULNERABLE 763
B. THE INDETERMINACY OF FEDERAL CYBERSECURITY REGULATIONS 766
C. ORGANIZING EXPERTISE AT THE NEW YORK PUBLIC SERVICE COMMISSION 768

III. EXPERTISE IN THE BREACH 770

IV. RATE RECOVERY AMID PERPETUALLY EVOLVING THREATS 773

A. REJECTING THE RHETORIC OF CONTINUALLY EVOLVING THREATS 776

V. CYBERSECURITY STANDARDS FOR A RAPIDLY EVOLVING INDUSTRY 779

A. CYBERSECURITY STANDARDS IN DISPUTE 782
B. CALLS FOR MORE EXPERT DIALOGUE 785
C. FINAL RULING 790

VI. CONCLUSION 791

I. INTRODUCTION

In the past twenty years, growing dependence on cyberspace has made national security a concern of relatively small, subnational organizations ranging from private companies to provincial, state, and local governments. Small businesses with no obvious relation to national security have found themselves in the crosshairs of state-sponsored campaigns designed to infiltrate national critical infrastructure and undermine national security. A recent report revealed that Russian hackers infiltrated the U.S. electrical power grid by targeting tiny, seemingly insignificant contractors in at least twenty-four states, exploiting trust networks.[1] The hackers targeted at least sixty

1. Rebecca Smith & Rob Barry, *America's Electric Grid Has a Vulnerable Back Door - and Russia Walked Through It*, WALL ST. J. (Jan. 10, 2019, 11:18 AM), https://

utilities, breached about two dozen of them, and gained access to the control rooms of eight or more—where they could have turned off the power had they wished to do so.[2] This suggests a success rate of over ten percent, but the potential impact of such compromises is much greater because of complex interdependency in the electrical power grid, where relatively small local disturbances can cascade into much larger failures if not managed well.[3]

In this context, federal, state, and local regulators have all expressed anxiety about how they can ensure the security of critical utility infrastructures, such as the power grid.[4] Regulators have evolved organizational processes, capacities, and expertise that aim to balance public goods such as reliability, affordability, and environmental protection, but cybersecurity is a different kind of good. Whereas reliability and efficiency have traditionally been understood as relatively deterministic, predictable characteristics, security implies an intelligent adversary that seeks to undermine it. No technological fix can provide assurance of cybersecurity; it requires continual vigilance by experts and continual advancements in their practices and knowledge. Indeed, cybersecurity can be understood as a race between experts on opposite sides of the law; white hats seek to defend systems while black hats seek to compromise them.

Thus, regulators have expressed concern that neither they nor the companies they regulate have the expertise needed to ensure that critical infrastructure remains uncompromised. A recent article by public utility commissioners notes that "[a]s the range and specialization of cyber threats grow, it will become increasingly difficult for companies to maintain sufficient in-house expertise to detect and manage penetrations."[5] A working paper from

www.wsj.com/articles/americas-electric-grid-has-a-vulnerable-back-doorand-russia-walked-through-it-11547137112.

2. *Id.*

3. *See* U.S.-CAN. POWER SYS. OUTAGE TASK FORCE, FINAL REPORT ON THE AUGUST 14, 2003 BLACKOUT IN THE UNITED STATES AND CANADA: CAUSES AND RECOMMENDATIONS (2004), https://www.energy.gov/sites/prod/files/oeprod/DocumentsandMedia/BlackoutFinal-Web.pdf (discussing the source of the 2003 Northeast Blackout).

4. *See, e.g.*, MILES KEOGH & SHARON THOMAS, NAT'L ASS'N OF REGULATORY UTIL. COMM'RS, CYBERSECURITY: A PRIMER FOR STATE UTILITY REGULATORS VERSION 3.0 (2017), https://pubs.naruc.org/pub/66D17AE4-A46F-B543-58EF-68B04E8B180F; Lynne Holt & Mary Galligan, *State Public Utility Commissions' Role in Cybersecurity and Physical Security Issues: Trade-Offs and Challenges* (Pub. Utl. Research Ctr. at Univ. of Fla., Working Paper, Dec. 12, 2017), https://bear.warrington.ufl.edu/centers/purc/docs//papers/1707_STATE_PUC_ROLE_Cybersecurity_12_12_17.pdf.

5. Sherina Maye Edwards, Caitlin Shields, Anne McKeon & Nakhia Crossley, *Cybersecurity, Part II: Opportunities and Challenges for State Utility Regulators*, PUB. UTIL.

the Public Utilities Research Center similarly notes that commissions "face many of the same challenges as utilities in attracting and retaining employees with cybersecurity expertise," but must also "compete with utilities for skilled employees with the added disadvantage of inadequate state pay-scales."[6] Organizations such as the National Association of Regulatory Utility Commissioners (NARUC) recently created a cybersecurity primer with five steps for state utility regulators, starting with "[c]reate expertise within their own organizations" and pointing to training opportunities offered by NARUC and other organizations.[7] In short, a variety of studies have examined the question of how regulators can acquire expertise and have suggested training in-house employees, hiring new cybersecurity experts, contracting with external consultants, or some combination of all three.

This Article focuses on a related but distinct set of questions. What constitutes cybersecurity expertise in the context of critical infrastructure? How do regulators adjudicate between conflicting claims to expertise? And, given the frequency of breaches and the absence of any security guarantees, how is the authority of cybersecurity experts produced?

Addressing this broader set of problems requires theorizing *expertise*. As the brief discussion above suggests, most analyses of regulation implicitly define expertise in terms of specialized knowledge and skills that are possessed by individuals or groups of people. From this perspective, the primary challenge is to acquire objective and disinterested expertise, thereby enabling regulators to provide a check on private interests and ensure the provision of public goods.

A somewhat different conception of expertise has emerged from work in Science and Technology Studies (STS) and related fields such as anthropology, sociology, and history.[8] Scholars in these fields have argued that expertise should be understood as a set of relationships between experts, laypersons, and culturally valued objects of expertise—e.g., secure computer networks.[9] Thus, expertise entails more than the possession of specialized knowledge or

FORTNIGHTLY, (Mar. 2017), https://www.fortnightly.com/fortnightly/2017/03/cybersecurity-part-2.

6. HOLT & GALLIGAN, *supra* note 4, at 13.

7. KEOGH & THOMAS, *supra* note 4, at 20.

8. *See, e.g.*, Rebecca Slayton & Aaron Clark-Ginsberg, *Beyond Regulatory Capture: Coproducing Expertise for Critical Infrastructure Protection*, 12 REG. & GOVERNANCE 115 (2018). This review is heavily influenced by the framing of E. Summerson Carr*, Enactments of Expertise*, 39 ANN. REVS. ANTHROPOLOGY 17 (2010). For more on security expertise, see generally TRINE VILLUMSEN BERLING & CHRISTIAN BUEGER, SECURITY EXPERTISE: PRACTICE, POWER, RESPONSIBILITY (2015).

9. For an overview of this literature, see generally Carr, *supra* note 9.

skills by a group of people; it also entails a relationship between people who claim to possess specialized skills and those who do not. These relationships are constructed through several kinds of activities, including a process of training and socialization, wherein aspiring experts learn to "pass" as legitimate members of an expert culture; demonstrating intimacy and mastery over rare but culturally valued objects; authorizing experts through institutions such as professional certification bodies; and obscuring the contingency and incompleteness of expert evaluations through naturalization. Drawing on dramaturgical approaches to understanding everyday social interaction, STS scholars have argued that expert advice can be understood as a kind of performance; experts selectively highlight aspects of their work that enhance its authority while obscuring or minimizing uncertainties, disagreements, and other features that might undermine it.[10] Expertise thus entails more than possessing knowledge or skills. It entails persuading an audience of the veracity of specific claims and the effectiveness of particular actions.

In general, cybersecurity expertise is a tough act to perform. Institutional markers, such as certifications and college degrees, confer only limited authority. It is widely recognized that such markers are no guarantee of efficacy, and very prominent experts may have no credentials at all. Instead, cybersecurity experts gain authority by demonstrating mastery over culturally valued objects—computers, networks, and the data flowing through them—the details of which seem arcane to the average person. However, this is often a perverse kind of mastery: breaking into systems that are believed to be secure. Furthermore, cybersecurity experts do not promise that they can prevent all breaches. Cybersecurity experts agree that virtually all practical computer systems can be breached by a sufficiently determined adversary. Furthermore, since breaches may remain hidden for years at a time, and there are no comprehensive metrics with which to gauge the security of a system, cybersecurity experts can never be certain that a system has not already been breached. This offers a limited basis for demonstrating expertise.

All of this raises the question of how regulators know what experts to trust. Moreover, because improvements in security often entail tradeoffs with other public goods, regulators must often negotiate between different and conflicting kinds of expertise. The NARUC primer notes the need for "a nimble and complex balance of security, functionality, and cost," pointing out that "a 'perfect' defense against cyberattacks has a cost that may, and often does, outweigh the value of the information it protects . . . . [T]he energy sector

10. *See, e.g.*, STEPHEN HILGARTNER, SCIENCE ON STAGE: EXPERT ADVICE AS PUBLIC DRAMA (2000).

cannot expect to 'gold plate' the grid."[11] Crucially, the logics that drive cybersecurity investments may be at odds with the logics grounding traditional investments in critical infrastructure. For example, as discussed further below, cybersecurity experts often invoke the need to keep pace with ever-changing threats—a need that can drive endless technological change and associated expense. However, this conflicts quite directly with regulators' goal of keeping rates associated with public goods such as electricity, gas, and water affordable and stable. Deciding what specific actions are appropriate thus requires both knowledge of technologies and practices used for security and value judgments about the relative importance of multiple goals.

How then, do regulators assure themselves and the public that they have achieved an appropriate balance between cybersecurity and other public goods? This paper argues that regulators have not merely accessed expertise but also worked with skilled and knowledgeable individuals to actively produce expertise. These findings have relevance not only for the cybersecurity of the electrical power grid, but for studies of regulation in complex technological industries more broadly.

The remainder of this Article consists of four main parts and a conclusion. The first overviews regulation for electrical grid cybersecurity, discussing how the grid became vulnerable to cyberattack, how federal regulators responded to these vulnerabilities, and how one state regulatory organization—the New York Public Services Commission (NYPSC or "Commission")—began to organize security expertise after the terrorist attacks of September 11, 2001.

The next three sections discuss three specific contexts in which the Commission's security experts have performed their expertise. First, Commission staff have been called upon to assess security in the wake of breaches. Although a security breach effectively means that experts working against the law have gotten the best of experts attempting to secure systems, there is little evidence that security breaches at utilities have undermined the public authority of either the utilities' or the Commission's security experts. Instead, the Commission's experts have responded to such breaches by identifying failures in the utilities' security practices, often with the help of consulting companies hired by the utilities. In so doing, the breaches have ironically reinforced the authority of cybersecurity experts by emphasizing that breaches are avoidable if organizations simply follow the best practices established by experts.

Second, the Commission's staff are often called upon to assess utilities' requests for rate recovery. These requests have grown, not only in response to

11. KEOGH & THOMAS, *supra* note 4, at 20.

North American Electric Reliability Corporation Critical Infrastructure Protection (NERC CIP) requirements, but also in response to perceptions of rapidly evolving threats. It is here that the cooperative relationship between the Commission's experts and the utilities experts seems more apparent, for I have yet to find any example of the Commission staff criticizing or rejecting security initiatives proposed by utilities. This is not to suggest that any specific proposals should have been rejected. Rather, ongoing conversation among the utilities and the Commission's staff likely produces a high degree of convergence before rate cases are filed. The readiness of the Commission's staff to embrace arguments about perpetually evolving threats stands in contrast to the approach taken by regulatory experts in other states. I present one example from a similar rate case in Massachusetts.

And third, the Commission's staff has been called upon to help establish cybersecurity standards for smart grids. This is perhaps the most challenging site for performing expertise, because competition among a growing number of actors in electricity markets has led to conflict over appropriate standards of security. Although the Commission's staff attempted to defer to industry experts and a business-to-business process, they were not able to completely stay out of the fray.

II. THE ORIGINS OF POWER GRID CYBERSECURITY REGULATION

A. MAKING THE GRID "SMART"—AND VULNERABLE

The grid's vulnerability to cyberattacks has emerged as part of a broader shift in ways of producing, selling, and using electrical power. In the late 1980s and early 1990s, engineers and entrepreneurs began to contend that microprocessors and computer networking would enable free-market solutions to many problems. For example, utilities were increasingly wary of investing in large sources of new power generation which might sit idle for long periods of time. Accordingly, they developed an interest in what came to be known as Advanced Metering Infrastructure (AMI), which can be used to implement hourly billing plans that incentivize consumers to shift electricity use from times of high demand to times of low demand. Microprocessors could also be used to help integrate Distributed Energy Resources (DER) such as rooftop solar, wind, and demand response programs, wherein customers might agree to stop using energy at certain times in exchange for more favorable rates.[12]

12. Rebecca Slayton, *Efficient, Secure Green: Digital Utopianism and the Challenge of Making the Grid "Smart*," 48 INFO. & CULTURE 448, 455–57 (2013).

In the 1990s, advocates of market restructuring also argued that computer networking could enable the creation of more competitive spot markets, or markets where financial instruments are traded for immediate delivery of services or goods. At the time, electricity production followed a model in which vertically integrated utilities provided electricity generation, transmission, and distribution as regulated monopolies. Spot markets would have utilities primarily provide transmission and distribution as regulated monopolies, while companies competed to supply generation. The 1992 Energy Policy Act authorized the Federal Energy Regulatory Commission (FERC) to require that utilities make their transmission lines available to electricity generators that wanted to sell wholesale power to distributors. FERC acted aggressively on its new authority, and some state commissions went further by requiring utilities to divest their generation assets.[13]

FERC encouraged utilities to form non-profit Independent System Operators (ISOs) or Regional Transmission Operators (RTOs) to manage centralized spot markets and coordinate grid operations.[14] Here again, information technology (IT) played a key role in the new regime. The ISOs/RTOs used computer networks (including the internet) to create a centralized spot market on a day-ahead and hourly basis. Electricity generators bid to supply electricity at specific times, and the ISOs/RTOs used these bids to manage economic dispatch for the system.[15] Today, approximately two-thirds of the electricity supply in North America is coordinated by nine different ISO/RTOs.[16]

Thus, the rise of distributed energy resources, along with the creation of spot markets and associated unbundling of generation and distribution, entailed a transformation in the information infrastructure running the electrical grid in the final decades of the twentieth century. The infrastructure transformed from a system controlled primarily by special-purpose and centralized computers towards one controlled by a complex network of standardized and distributed microprocessors.

---

13. *See* THE ELECTRIC ENERGY MARKET COMPETITION TASK FORCE, REPORT TO CONGRESS ON COMPETITION IN WHOLESALE AND RETAIL MARKETS FOR ELECTRIC ENERGY, 33–34 (2006).

14. Promoting Wholesale Competition Through Open Access Non-discriminatory Transmission Services by Public Utilities; Recovery of Stranded Costs by Public Utilities and Transmitting Utilities, 61 Fed. Reg. 21540, 21596–97, (May. 10, 1996) (codified at 18 C.F.R. pts. 35, 385) (encouraging the formation of ISOs).

15. Seth A. Blumsack, Jay Apt & Lester B. Lave, *Lessons from the Failure of U.S. Electricity Restructuring*, 19 ELECTRICITY J. 15, 17–19, 26 (Mar. 2006).

16. ISO/RTO COUNCIL, https://isorto.org (last visited Feb. 24, 2020).

Around the turn of the millennium, this transformation was accelerated by growing enthusiasm for a smart grid—a label incorporating a vast range of technologies such as advanced metering infrastructure, electric vehicle charging stations that can also provide battery storage and related services, satellite-based, wide-area measurement systems, and many more computer-managed systems.[17] The U.S. Energy Independence and Security Act of 2007 committed the nation to developing a smart grid, defined first and foremost as the "increased use of digital information and controls technology to improve reliability, security, and efficiency of the electric grid," followed by the "[d]ynamic optimization of grid operations and resources, with full cybersecurity," the "[d]eployment and integration of distributed resources and generation, including renewable resources," and a list of other goals.[18] In sum, the smart grid is typically depicted as something that will simultaneously increase efficiency, reliability, security, and the integration of renewable resources.

However, there are tradeoffs between these goals in practice.[19] While some smart devices may improve security, the proliferation of "smart" devices—particularly through the distribution systems that local and state regulators oversee—also greatly increases opportunities for attack. Accordingly, the 2007 Act also gave the National Institute of Standards (NIST) responsibility for coordinating the development of a framework to ensure the interoperability and security of these many devices. NIST published this framework in August 2010, including a set of high-level cybersecurity guidelines.[20] However, these were not mandatory requirements, and they left considerable room for discretion to experts in the industry to determine what constituted appropriate risk. As the framework explained, "[e]ach organization will need to perform a risk assessment to determine the applicability of the requirements to their specific situations."[21]

The NIST guidelines were partly based on federal cybersecurity standards, which were mandatory for the bulk electric grid—i.e., generation and transmission assets. Yet, as the following sections discuss, these federal standards were also risk-based and left considerable room for experts to exercise discretion.

17. *See* Slayton, *supra* note 12, at 464–65.

18. Energy Independence and Security Act of 2007 § 1301, 42 U.S.C. § 17381 (2018).

19. Slayton, *supra* note 12, at 460–68.

20. *See* CYBER SEC. WORKING GRP., NAT'L INST. OF STANDARDS & TECH., INTRODUCTION TO NISTIR 7628: GUIDELINES FOR SMART GRID CYBER SECURITY 2 (2010) https://permanent.access.gpo.gov/gpo1900/nistir-7628_total.pdf.

21. *Id.* at 10.

B. THE INDETERMINACY OF FEDERAL CYBERSECURITY REGULATIONS[22]

Though engineers began to warn of computer-related security risks as early as the 1970s, regulators paid relatively little attention to what came to be known as cybersecurity until the late 1990s. The Oklahoma City bombings focused federal attention on critical infrastructure protection, which only intensified after the 2001 terrorist attacks on the World Trade Center. FERC announced that it would be including cybersecurity standards in its 2002 Notice of Proposed Rulemaking on a Standardized Market Design, which was intended to provide a "level playing field" for competitive wholesale electric markets.[23] It asked an industry group—the North American Electric Reliability Corporation (NERC)—to help draft standards. Over the next year, NERC helped to manage an often-controversial standards drafting process. On August 13, 2003, it approved an "Urgent Action Standard" intended to serve as a temporary guide until more permanent standards could be agreed upon.[24]

The very next day, the largest blackout in U.S. history left fifty-five million people without power across eight U.S. states and Ontario, Canada. A task force charged with examining the causes of the blackout implicated software: a glitch caused an alarm malfunction after a transmission line hit a tree branch, leading to a cascading failure with widespread consequences.[25] The task force's final report further noted that "there are terrorists and other malicious actors who have the capability to conduct a malicious cyberattack with potential to disrupt the energy infrastructure."[26] Consequently, it recommended including physical and cybersecurity requirements in a set of reliability standards which were to be "mandatory and enforceable, with penalties for noncompliance."[27]

The Energy Policy Act of 2005 began implementing these recommendations by tasking FERC with designating an electric reliability organization (ERO), which would work with the industry to develop and enforce the new standards. NERC was the only entity to file for ERO consideration and was appointed as ERO in July 2006.[28]

However, the process of developing enforceable Critical Infrastructure Protection (CIP) standards was slow, partly because of significant tensions between the expert practices needed for maintaining the reliability of the grid's

22. Much of the discussion in this Section is based on research presented in Slayton & Clark-Ginsberg, *supra* note 8. More detailed discussion and citations can be found there.

23. *Id.* at 120.

24. *Id.* at 121.

25. U.S.-CAN. POWER SYS. TASK FORCE, *supra* note 3, at 135.

26. *Id.*

27. *Id.* at 163.

28. Energy Policy Act of 2005 § 1211, 16 U.S.C. § 824o (2018).

operational technology (OT)—physical machinery such as electricity generators, circuit breakers, transformers—and those that have traditionally been used for securing IT. OT engineers have achieved tremendous levels of reliability through a slow and evolutionary process of change, deploying technology for decades at a time. By contrast, IT is secured through frequent software updates, and systems are often outdated within five years.[29] Software updates can often produce unexpected consequences and interactions. While such unexpected behavior is an inconvenience in an office environment, it can be deadly when the computers control physical machinery. The companies making control systems for OT have not always provided software patches and may not support capabilities such as encryption. Password protection and other common forms of authentication may be dangerous if they lock out an operator in an emergency. Thus, OT and IT have struggled to agree upon what the CIP standards should entail or what constitutes best practices in critical infrastructure cybersecurity.

These tensions led to exceptions within the NERC CIP standards which allowed organizations to use "reasonable business judgment" in determining whether or not to apply security controls[30] Utilities were particularly concerned about the potentially prohibitive cost of replacing equipment that had been expected to last for decades, simply because that equipment did not allow for the implementation of certain controls. However, exceptions based upon "technical feasibility" and "business judgment" gave industry experts more discretion than regulators wanted.[31] When FERC approved the standard in January 2008, it also required NERC to remove "language that allowed variable implementation of standards based on 'reasonable business judgment' " and to create "a new framework of accountability surrounding exceptions based on technical feasibility."[32] Nonetheless, federal regulators continue to be challenged by the inevitable need for industry experts to use some discretion in implementing standards, as well as the need to adjudicate when experts do not agree.

---

29. JOSEPH WEISS, PROTECTING INDUSTRIAL CONTROL SYSTEMS FROM ELECTRONIC THREATS 34 (2010).

30. *FERC Approves New Reliability Standards for Cyber Security*, POWERGRID INT'L, Jan. 17, 2008, https://www.power-grid.com/2008/01/17/ferc-approves-new-reliability-standards-for-cyber-security/#gref; *see also*, Mandatory Reliability Standards for Critical Infrastructure Protection, 17 Fed. Reg. 7368, 7370 (Feb. 7, 2008) (codified at 18 C.F.R. pt. 40).

31. *Id.*

32. *See* Mandatory Reliability Standards for Critical Infrastructure Protection, *supra* note 30, at 7370; POWERGRID INT'L, *supra* note 30. Under the approved standards, organizations would be required to self-certify compliance more than once a year, and to "achieve 'auditable compliance' no earlier than mid-2009." Mandatory Reliability Standards for Critical Infrastructure Protection, 17 Fed. Reg., *supra* note 30, at 7371.

State and local authorities face these challenges to an even greater degree. For example, public utility commissions must regularly assess whether utilities' requests for rate recovery related to NERC CIP compliance requirements is justified. Furthermore, NERC CIP standards were designed to protect electricity generation and transmission infrastructure, not the distribution networks that fall under the jurisdiction of state and local authorities. Indeed, the reliability and security of distribution networks are regulated through a patchwork of state and local organizations. Investor-owned utilities are regulated by state utility commissions, while municipal utilities are owned by cities and are held accountable by elected officials, and cooperatives are owned and governed by their members.

Decision-makers in this patchwork of governing bodies may have little or no knowledge of cybersecurity. Nor do they always have the resources needed for assessing tradeoffs between security and other public goods. Yet they are responsible for overseeing some of the most vulnerable and exposed portions of the electric power grid. The remainder of this Article examines how one such organization—the New York Public Services Commission (NYPSC)—has responded to this challenge. It then briefly compares that to the response of another organization—the Massachusetts Department of Public Utilities.

C. ORGANIZING EXPERTISE AT THE NEW YORK PUBLIC SERVICE COMMISSION

The NYPSC is a particularly interesting case because the terrorist attacks of September 11, 2001, put the Commission literally at ground zero of debate about critical infrastructure security. One month after the terrorist attacks on the Twin Towers, the Commission established a security assessment team within its staff arm, the Department of Public Service.[33] This team began meeting with the dozens of companies within its jurisdiction to develop a better understanding of the security measures in place.[34] In 2003, the Commission hired John Sennett, who had been a special agent with the FBI since 1980, to direct a new utility security section.[35] Over the next several years, the security section hired individuals specializing in physical security—many of whom had a background in law enforcement—as well as individuals with training in information security.

33. Lori A. Burkhart, *A Fight Over Market Design*, PUB. UTIL. FORTNIGHTLY (Nov. 15, 2002), https://www.fortnightly.com/fortnightly/2002/11-0/regulators-forum-fight-over-market-design.

34. *Id.*

35. Neither Sennett nor the security section has a public profile associated with the commission, but Sennett's background appears on his professional website. *See* John Sennett, LINKEDIN, https://www.linkedin.com/in/john-sennett-25a16529 (last visited Aug. 1, 2020).

However, the Department did not wait until it had hired in-house security experts to begin evaluating the utilities' security. Instead, staff immediately urged the energy and telecommunications utilities to "retain third-party consultants or experts to evaluate the adequacy of their physical equipment and computer system security arrangements."[36] Most of the companies did so, but two of the twelve—New York State Electric & Gas (NYSEG) and MCI Communications Corporation (originally Microwave Communications Inc.)—balked. Accordingly, in August 2002, the Commission ordered the NYSEG and MCI to retain consultants to evaluate their security. Additionally, noting that the Commission staff and utilities "have not faced a threat of this magnitude and scope in the past," the Commission argued that "outside expertise is needed to ensure that preparations to meet the new threats are adequate."[37] Accordingly, the Commission contracted with two consulting firms—one firm to evaluate the adequacy of the cybersecurity evaluations and the utilities' response to recommendations in those evaluations, and another firm to do the same with the physical security evaluations.

The two firms ultimately found that, while the utilities were diligent about contracting for third-party security assessments, those assessments sometimes overlooked issues such as the need for separation of duties and policies for managing personnel and third-party vendors. In September 2003, the Commission ordered the utilities to prepare management plans explaining how they would respond to the issues raised in the reports that the utilities had contracted, in addition to those contracted by the Commission.[38]

In June 2004, it issued a press release announcing that the energy utilities had implemented or were in the process of implementing "a total of almost 800 initiatives designed to strengthen physical and cyber-system security," while telecommunications companies were implementing 275 such initiatives.[39] Furthermore, it explained:

---

36. Order Instituting Proceeding and Establishing Procedures for Preparation of Security Evaluations at 1, Telephone and Energy Utility Arrangements for Safeguarding the Security of Their Physical Equipment and Cyber Systems, No. 02-M-0953 (N.Y. Pub. Serv. Comm'n Aug. 2, 2002), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={C2E5B25F-CDFB-42DB-A405-6647EDD6AD33}.

37. *Id.* at 2.

38. *See generally* Order Directing Further Action, Telephone and Energy Utility Arrangements for Safeguarding the Security of Their Physical Equipment and Cyber Systems, No. 02-M-0953 (N.Y. Pub. Serv. Comm'n Sep. 30, 2003), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={4E6EC1D8-227D-4C6B-A741-D2D668DEACB4}.

39. Press Release, N.Y. Pub. Serv. Comm'n, Strengthening of Physical and Cyber-System Security of Energy/Telecommunications Utilities Protects Public (June 2, 2004), http://

> The Commission's Office of Utility Security staff has conducted its own analysis of the utility efforts, with assistance from selected independent security experts, and determined that physical and cyber-system security involving utility facilities in the state is greatly improved. Moreover, Commission staff, in concert with the utilities, will continue to evaluate emerging technologies for continually improving security.[40]

As these words suggest, the Commission's security experts aimed to accomplish their work in a collaborative rather than an adversarial manner, working "in concert" with the utilities.[41] Below, I will argue that this collaborative approach was sometimes conducive to achieving a persuasive public performance of expertise because ambiguities about how to apply standards could be resolved behind closed doors, rather than in a public forum where the contingent and value-laden nature of expert judgments can be questioned. Nonetheless, experts' ability to perform persuasively has varied across different contexts. The following parts discuss three such contexts: responding to security breaches at the utilities, evaluating requests for rate recovery of cybersecurity expenses, and establishing standards for an increasingly complex and divided industry.

III. EXPERTISE IN THE BREACH

Despite the Commission's efforts to bolster both physical and cybersecurity at its regulated utilities in the early 2000s, these organizations were not free of breaches over the following decade. The most significant known breach was discovered in January 2012, after IT staff at NYSEG and Rochester Gas & Electric (RG&E) noticed suspicious network traffic that used the access credentials of one of the companies' contractors. They soon concluded that the confidential information of approximately 1.8 million customers—including social security numbers, birthdates, and financial account information—had been compromised. They consequently issued notifications to customers, along with offers of credit monitoring services.[42] The companies retained Verizon Business to conduct an investigation, which

www3.dps.ny.gov/pscweb/WebFileRoom.nsf/Web/1D5D816E2F80B95D8525729D00655 96C/$File/pr04042.pdf?OpenElement.

40. *Id.*

41. *Id.*

42. *See* Staff Report at 4, Order Directing a Report on the Implementation of Recommendations, N.Y. State Elec. & Gas Corp./Rochester Gas & Elec. Corp. Sec. Breach, No. 12-M-0282 (N.Y. Pub. Serv. Comm'n July 18 2012), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={94D18677-4E68-4549-88FD-6FCB29703A03}.

discovered that the contractors had subcontracted work to persons working outside of the United States. It found no wrongful intent on the part of the contractor or the subcontractor and no evidence that any of the information had been used. Nonetheless, the Commission ordered its security staff to investigate the cybersecurity practices of NYSEG, RG&E, and other regulated utilities.[43]

In July, the security specialists issued a report identifying five areas in which NYSEG and RG&E had failed to follow "best practices" as defined in NIST standards for protecting personally identifiable information.[44] They also noted that they had completed on-site reviews of four companies—Consolidated Edison, Orange and Rockland, National Grid, and National Fuel Gas—and would soon complete a comparable review of Central Hudson.[45] They had not discovered any "significant vulnerabilities requiring immediate corrective action," but they had identified some "areas for improvement," and they expected the utilities to implement their recommendations.[46] In September, the staff sent out a questionnaire to all the utilities for an on-site review by the Commission staff, which would be scheduled no later than October 31, 2012.[47]

If the Commission staff found major problems at Central Hudson, it did not mention them in any public documents. Yet on February 16, 2013, IT staff at Central Hudson found evidence of anomalous activity on their networks.[48] Over the next three days, they discovered an active worm in their system.[49] Moreover, a computer connected to a cash and check processing system was trying to log on to other company computers using local accounts.[50] The staff notified the utility security section of the Department of Public Services and

43. *See* Press Release, N.Y. Pub. Serv. Comm'n, PSC Investigates Consumer Data Breach at NYSEG, RG&E (Jan. 23, 2012), http://www3.dps.ny.gov/pscweb/WebFileRoom.nsf/Web/1986D5ECA1917A8A8525798E005F81DD/$File/pr12007.pdf?OpenElement.

44. The staff's report is appended to the Commission's order issued six days later. *See* Staff Report, *supra* note 42, at 3.

45. *Id.* at 13.

46. *Id.* at 14.

47. *See* Letter from Jaclyn A. Brilling, N.Y. State Elec. & Gas Corp./Rochester Gas & Elec. Corp. Sec. Breach, No. 12-M-0282 (N.Y. Pub. Serv. Comm'n Sep. 20, 2012), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={09628D61-47C9-43D6-97D5-3606771E6170}.

48. Order Directing the Creation of an Implementation Plan at 1, Security for the Protection of Personally Identifiable Customer Information, No. 13-M-0178 (N.Y. Pub. Serv. Comm'n Aug. 19, 2013) (rev. of Cent. Hudson Gas & Elec. Corp. Breach Incident), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={28CDF9EB-8661-491C-B2C2-E6E527297EE0}.

49. *Id.* at 1–2.

50. *Id.* at 1.

contracted with Dell to investigate further.[51] Experts from Dell concluded that the malware had been present for at least six months prior to discovery but could not determine how it had been introduced or how much data it might have extracted from the system.[52] Central Hudson had no choice but to regard the checking information of its customers as compromised, and on February 22, 2013, it began to notify the public and approximately 110,000 affected customers.[53] Dell ultimately made thirteen recommendations to Central Hudson.[54]

The Commission's security staff met with Central Hudson and Dell's representatives and reported on the process to the Commission, which ordered Central Hudson to file an implementation plan outlining how it would respond to the issues raised by Dell. Meanwhile, the Commission's security experts continued to review the utilities and ultimately made nine recommendations for improving security, including several "best practices"—preparing for breaches by conducting drills and contracting with forensic experts and credit monitoring companies, improving training, improving management of personally identifiable information, upgrading both physical and cyber defensive measures such as "next-generation intrusion detection systems," and conducting a regular third-party vulnerability assessment.[55]

In August 2013, the Commission ordered each of the utilities to prepare plans outlining how they were implementing these recommendations.[56] Furthermore, arguing that the final measure—regular vulnerability assessments—was the most important of the nine recommendations, the Commission ordered each utility to undertake an annual vulnerability assessment, the first of which was to be completed by July 1, 2014.[57] The Commission emphasized that it was important "that any third-party consultants retained for this purpose have a high level of experience and expertise," and noted that its staff had recommended "certification by the Payment Card Industry Security Standards Council" as "the best available

51. *Id.* at 2.
52. *Id.* at 2–3.
53. *Id.* at 3.
54. *Id.* at 6.
55. Order Directing the Creation of an Implementation Plan at 5–6, Security for the Protection of Personally Identifiable Customer Information, No. 13-M-0178 (N.Y. Pub. Serv. Comm'n Aug. 19, 2013), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={5986D197-87DB-4D21-A89B-95DC45E05061}.
56. *See, e.g.*, *id.* at 8.
57. *Id.* at 7.

assurance of competence for this type of audit work."[58] The Commission's security staff would then review the implementation plans.

In sum, the breaches at NYSEG and Central Hudson led the Commission to establish new oversight practices, most notably an annual third-party audit. Since no major breaches have come to light since the Commission instituted annual audits and investigations never found evidence of data misuse, the incidents appear to have been publicly resolved. Nonetheless, perhaps it is remarkable that the breaches were never used to question the expertise of either the utilities' or the Commission's security staff. After all, why was it that even after specifically investigating security practices at the utilities, the Commission's staff did not publicly identify and correct the shortcomings that led to the breach at Central Hudson? But this question does not appear to have been asked publicly. Instead, the breach provided an opportunity for the Commission's experts to perform expertise by citing best practices, certifications, and other institutionalized markers of cybersecurity expertise. Rather than demonstrating a lack of expertise among these professionals, the Commission took these incidents as proof that their expertise was needed.

IV. RATE RECOVERY AMID PERPETUALLY EVOLVING THREATS

A second context in which the Commission's staff have performed expertise is in the evaluation of requests to recover expenses associated with cybersecurity. In this context, we must note a significant tension between two needs—the need for continual investment in cybersecurity to counter continually evolving threats and the need to keep rates affordable and stable over time.

In the past decade, utilities have repeatedly rationalized requests to recover expenses associated with cybersecurity by highlighting new and changing threats to the grid. Most of these requests have been buried in much larger and more comprehensive rate cases, some of which proved quite controversial, with some of the Commission's in-house experts challenging proposed utility expenditures. Nonetheless, the Commission's cybersecurity staff have generally embraced arguments for increased spending on security, citing rapidly changing threats.

For example, in June 2013, six months after initiating a comprehensive rate case, Con Edison increased its request for cybersecurity investment. In prepared testimony, Con Edison's in-house experts argued that "cyber threats are becoming more persistent, more sophisticated, more widespread, with a

58. *Id.* at 7–8.

greater focus on the utility industry and with potentially severe consequences . . . ."[59] They highlighted recent attacks on utilities, including the compromise of the control systems of a northeast utility, and an ongoing targeted attack on Con Edison's internal computer networks from internet addresses in Iran. While emphasizing that they did not believe the attack on Con Edison had been successful, they noted that "[t]here is no reason to assume these attacks will abate . . . [i]n fact, all recent evidence indicates they will continue to occur with increasing sophistication and as attack vectors change, the Company's responses to them must be swift and definitive."[60] Accordingly, they requested rate recovery for capital investments as well as operational and maintenance expenses associated with the hiring of sixteen new cybersecurity experts. Many aspects of Con Edison's rate case proved contentious, with the Commission staff rejecting portions of Con Edison's requested revenue increases. However, the Commission's security staff did not oppose these new investments in cybersecurity.[61]

Three years later, when Con Edison again requested new revenues associated with cybersecurity, the Commission's security staff not only accepted that such expenses were necessary, they also repeated the rationale of evolving threats in their prepared testimony. Their rationale was that:

> [t]he field of cybersecurity is one in which the risks, threat actors/vectors, and technologies involved are constantly changing and increasing in complexity at a breakneck pace. . . . This ever-escalating cyber threat to business and critical infrastructure information requires that utilities remain constantly vigilant and seek new and innovative ways to bolster their cybersecurity posture.[62]

Both utility and Commission cybersecurity experts repeated similar arguments in a recent rate case filed by NYSEG and RG&E. In May 2019, testimony from the company's electric reliability and operations panel argued that

59. Prepared Testimony of the Shared Services Panel at 14, In the Matter of Consolidated Edison Co. of N.Y., Inc., Nos. 13-E-0030, 13-G-0031, 13-S-0032 (N.Y. Pub. Serv. Comm'n June 21, 2013), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={C69D0A46-1A04-461A-A25D-6B5BD131984F}.

60. *Id.* at 14.

61. *See* Staff Initial Brief, In the Matter of Consolidated Edison Co. of N.Y., Inc., Nos. 13-E-0030, 13-G-0031, 13-S-0032 (N.Y. Pub. Serv. Comm'n Aug. 30, 2013), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={BBA1148B-18D6-4A85-BEAD-B6C6FB042E37}.

62. Keith Haugen & Dennis C. Murray, Prepared Testimony of the Department of Public Service Staff Security Panel at 19, In the Matter of Consolidated Edison Company of New York, Inc., Nos. 16-E-0060, 16-G-0061 (N.Y. Pub. Serv. Comm'n 2016), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={DBE70276-BD3C-46F6-80E9-A8B878BC3D8A}.

"continual and extensive changes to the security landscape require these security upgrades to protect against physical and cyber intrusions. . . . As threats evolve and become more sophisticated, the Companies must keep pace."[63] It also noted that growing cybersecurity expenses were needed "to ensure data protection, privacy and compliance with regulatory and legal mandates."[64]

The Commission's cybersecurity experts echoed these arguments in prepared testimony.[65] When asked to explain the importance of cybersecurity, they argued that "[t]he field of cyber security is one in which the risks, threat actors/vectors, and technologies involved are constantly changing and increasing in complexity."[66] They used similar rhetoric to recommend approval of proposals for increased spending for a previously funded project, the "Net Sec[urity] Lifecycle," noting that "the projects that comprise the multiple layers of security need to be constantly maintained and upgraded, and both software and hardware need periodic replacement."[67]

To be sure, staff evaluating these proposals cited more than just evolving threats. They also pointed to NERC's mandatory cybersecurity standards, along with other best practices. Yet as discussed above, existing standards of grid security leave considerable room for discretion. Perhaps remarkably, I have yet to find any examples of the New York Public Service Commission security staff critiquing the utilities' grid cybersecurity proposals. This suggests that they are either spending too much on cybersecurity or failing to adequately secure the grid. This substantial agreement between the utilities' and Commission's experts may largely be due to a tacit and informal coordinating process that takes place as the Commission staff conduct their regular oversight work.

---

63. Direct Testimony of Electric Reliability & Operations Panel at 33–34, No. 19-E-0378 (N.Y. Pub. Serv. Comm'n May 20, 2019), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={21DC1333-30C6-4989-9C76-E2617E2D96EC}.

64. *See id.* at 34.

65. Specifically, testimony was provided by Brian O'Keefe, who held a BS in political science and extensive experience in managing physical security at National Grid, and Philip Tabor, a cybersecurity analyst who held a BS in psychology and a Security+ certification from the Computing Technology Industry Association (Comp TIA), a certifying body. Keith Haugen Dennis C. Murray, Prepared Testimony of the Department of Public Service Staff Security Panel, before the State of New York Public Service Commission, In the Matter of Consolidated Edison Company of New York, Inc. Cases 16-E-0060 and 16-G-0061 (2016)

66. Prepared Testimony of Staff Security Panel at 15, Office of Resilience and Emergency Preparedness, No. 19-E-0378, 19-G-0379, 19-E-0380, 19-G-0381 (N.Y. Pub. Serv. Comm'n Sept. 20, 2019), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={BF742238-7AF2-478D-A6E1-88C58477EF76.

67. *Id.* at 17.

A. REJECTING THE RHETORIC OF CONTINUALLY EVOLVING THREATS

In states where public utility commissions have devised other means to gather expert advice, the same kinds of arguments for increased investment in cybersecurity have not always proven persuasive. This becomes very clear from a recent case in Massachusetts. Unlike the New York Public Services Commission, the Massachusetts Department of Public Utilities does not appear to have an in-house team of security experts. Instead, the Massachusetts Attorney General's Office (AGO) has a section devoted to ratepayer advocacy. This section represents the ratepayers in any proceeding and can hire consultants and charge back the costs to the companies.[68] The AGO recently played a significant role in challenging proposals for rate recovery related to IT, including cybersecurity.

In 2019, Massachusetts Electric Company and Nantucket Electric Company, two subsidiaries of the multinational National Grid Services Company, filed a comprehensive rate case with the Massachusetts Department of Public Utilities. One of seventeen sets of testimony submitted by National Grid focused on IT.[69] The Information Technology Panel explained that the company's Digital Risk and Security team provided "the requisite consultancy and expertise needed to meet the escalating threats to the Company's networks and systems."[70] It further explained that it had recently "revisited its strategy and associated project roadmaps to ensure that the roadmaps were in alignment with the current threat landscape," and that this review "resulted in a refreshed multi-year investment program needed to ensure continued and evolving protection of National Grid's cyber and information assets."[71] The panel outlined eight new initiatives in an attached exhibit, arguing that these would "deliver new capabilities focused on ensuring the reliability and availability of our infrastructure, while delivering capability to keep pace with

68. MASS. GEN. LAWS ch. 12, § 11E (2020).

69. The panel included three employees: Stephen Olive, Chief Information Officer, who holds a bachelor's degree in electrical engineering and an MBA; Daniel J. DeMauro, NGSC's director of U.S. information technology regulatory compliance, who holds a bachelor's degree in accounting; and Mukund Ravipaty, NGSC's Director of Global Head Security Services, Design, and Architecture, who holds a bachelor's degree in computer science and an MBA. Ravipaty described his responsibilities as including "overseeing the development of cyber-security strategy and architecture to ensure that National Grid's cyber and security protections are developed to keep pace with the evolving threats and capabilities of hostile individuals, groups, and nations." Pre-Filed Direct Testimony of the Information Technology Panel at 184, Mass. Elec. Co. & Nantucket Elec. Co. each d/b/a Nat'l Grid, D.P.U. 18-150 (Mass. Dep't of Pub. Util. Nov. 15, 2018), https://fileservice.eea.comacloud.net/FileService.Api/file/FileRoom/10043017.

70. *Id.* at 192.

71. *Id.* at 194.

emerging threats and continued evolution towards a risk based, proactive, intelligence led cyber security program."[72]

In November 2018, the AGO responded to the National Grid filing by requesting approval to spend up to $550,000 on consultants, citing the high complexity of the case and a substantial rate increase.[73] This request was quickly granted, and both the AGO and Department of Public Utilities were soon issuing dozens of information requests to National Grid. This included queries about proposed cybersecurity programs, including "whether each project or investment enhances current IT assets/capabilities, or replaces existing IT assets/capabilities" and "if the existing assets have reached the end of their useful life and how the Company has adjusted its associated cost accounting."[74]

National Grid's expert panel responded that all the proposed investments "are either new or enhanced capabilities."[75] It further explained: "[d]ue to the nature and sophistication of the continuing cyber threats, National Grid is continually developing its cyber capabilities to stay one step ahead of these emerging threats."[76] National Grid also attached a February 2019 IT strategy document, prepared by a consultant to the company, which emphasized the need for continual change:

> In today's global ecosystem, the threat of cyber-attacks has continued to intensify and grow in complexity. This ever-changing landscape requires continued focus and attention to safeguard the critical national infrastructure . . . .
>
> National Grid must continue to develop its cyber capability, at a faster pace than the emerging threats, and this is becoming

72. *Id.*

73. The Attorney General's Notice of Retention of Experts and Consultants, Mass. Elec. Co. & Nantucket Elec. Co. each d/b/a Nat'l Grid, D.P.U. 18-150 (Mass. Dep't of Pub. Util. Nov. 27, 2018), https://fileservice.eea.comacloud.net/FileService.Api/file/FileRoom/10071059.

74. Attorney General's Thirtieth Set of Document and Information Requests at 1, Mass. Elec. Co. & Nantucket Elec. Co. each d/b/a Nat'l Grid, D.P.U. 18-150 (Mass. Dep't of Pub. Util. Mar. 15, 2019), https://fileservice.eea.comacloud.net/FileService.Api/file/FileRoom/10479171.

75. Information Request AG-30-1 at 2, Mass. Elec. Co. & Nantucket Elec. Co. each d/b/a Nat'l Grid, D.P.U. 18-150 (Mass. Dep't of Pub. Util. Mar. 29, 2019), https://fileservice.eea.comacloud.net/FileService.Api/file/FileRoom/10546443.

76. *Id.* at 2.

> increasingly critical as the energy sector evolves and accelerates the digitisation of energy infrastructure . . . .[77]

National Grid also responded to a range of other information requests, such as which projects would address compliance with NERC CIP requirements, and what costs were allocated to National Grid's subsidiaries operating in different regions. As we have seen, similar arguments about the need to keep pace with growing threats satisfied the New York Public Service Commission when faced with such a request.

However, the Massachusetts Attorney General deemed these responses deficient. In a brief filed in mid-June 2019, the AGO criticized National Grid's "high level description of projects," continuing:

> The Company's investment "plan" constitutes an accumulation of disjointed documents without a comprehensive planning document to pull them all together. The Company's documents show an investment process that is subject to continual adjustments, unstructured relative to long-term initiatives and spending…and contains no performance measurements or benchmarks. . . . [T]he Company's approach of producing an annual portfolio of projects subject to continual change is unacceptable given the significant and increasing level of IT investment.[78]

For its part, National Grid argued that criticism about continual change was inappropriate since changes were responsive to real needs and were thoroughly reviewed.

In its final order, the Massachusetts Department of Public Utilities ultimately concluded that National Grid's proposed costs associated with IT investments were "reasonable" and actually slightly increased the proposed IT rent expense.[79] Nonetheless, it found "some merit in the Attorney General's argument that the Company's approach to IT investment is reactive, uncoordinated, and has not been vetted to determine benefits Massachusetts ratepayers receive for the costs allocated to them."[80] This was just one of several concerns that spurred the Massachusetts Department of Public Utilities

77. Attachment AG-30-1-2 at 8, Mass. Elec. Co. & Nantucket Elec. Co. each d/b/a Nat'l Grid, D.P.U. 18-150 (Mass. Dep't of Pub. Util. Mar. 29 2019), https://fileservice.eea.comacloud.net/FileService.Api/file/FileRoom/10546446.

78. Initial Brief of the Office of the Attorney General at 48, Mass. Elec. Co. & Nantucket Elec. Co. each d/b/a Nat'l Grid, D.P.U. 18-150 (Mass. Dep't of Pub. Util. June 14, 2019), https://fileservice.eea.comacloud.net/FileService.Api/file/FileRoom/10831974.

79. Order at 71, 269, 271 Mass. Elec. Co. & Nantucket Elec. Co. each d/b/a Nat'l Grid, D.P.U. 18-150 (Mass. Dep't of Pub. Util. Sept. 30, 2019), https://fileservice.eea.comacloud.net/FileService.Api/file/FileRoom/11262053.

80. *Id.* at 499.

to open an investigation into the company's strategic planning processes, staffing decisions, and "potential management problems through to the highest levels of the organization."[81]

As this suggests, arguments that rapidly evolving threats necessitate increased cybersecurity funding are not always persuasive to government authorities charged with protecting ratepayer interests. The outcomes of the cases cited here are underdetermined by the arguments of experts and likely reflect the different processes by which experts mediate between the utilities and regulators. In sum, the AGO hiring of consultants to scrutinize the utilities' proposals as needed is an intrinsically more adversarial process, whereas the New York Public Service Commission's in-house cybersecurity experts are likely to develop cooperative relationships with the utilities' experts.

V. CYBERSECURITY STANDARDS FOR A RAPIDLY EVOLVING INDUSTRY

A third context in which the New York Department of Public Services security section has performed expertise is in helping to establish standards for a rapidly changing industry. As noted above, efforts to achieve a variety of regulatory goals—including the increased integration of renewable resources and the introduction of more retail competition and lower energy prices—have driven investments in IT that inevitably create new security vulnerabilities. The New York Public Service Commission was proactive about industry restructuring and began pushing retail competition in energy supply in the 1990s. In the restructured market, Energy Service Companies (ESCOs) began competing to purchase and sell energy resources, such as demand-side response capabilities (programs which incentivized users to not use energy at times of high demand), tailoring the specific mix to the needs or interests of particular customers.[82] ESCOs were seen as important to achieving goals for integrating more renewable energy into the grid because they could, for example, give consumers the option to pay more for energy from renewable resources. Utilities became providers of infrastructure, but no longer held monopoly power to sell electricity.

81. *Id.* at 502.

82. ESCOs also may offer many other services, such as helping large energy consumers reduce their consumption. But for purposes of this discussion, I am focusing on their role in competitive energy markets. For an early discussion of the role of ESCOs in restructured markets, see Opinion and Order Concerning Uniform Business Practices, Retail Access Business Rules, No. 98-M-1343 (N.Y. Pub. Serv. Comm'n Feb. 16, 1999), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={8543A612-83DD-45E3-9262-EB1CBF591743}.

Enabling this restructured market entailed the creation of an Electronic Data Interchange (EDI) that the utilities, ESCOs, direct customers, and marketers could use to exchange data. In the late 1990s, the Commission started an EDI working group to establish standards.[83] Creating market incentives and signals also entailed the deployment of Advanced Metering Infrastructure to enable time-of-use billing. In 2006, the Commission ordered utilities to file plans for deploying AMI.[84] As the utilities began submitting their plans, the Commission concluded that the utilities did not share a common understanding of what features AMI should include. Accordingly, on October 10, 2007, the Commission requested comment on what minimum functional requirements should be included in AMI.[85] And in April 2008, the Commission held a technical conference on the topic.[86]

It was only at this technical conference that the Commission staff finally began to devote significant attention to the security of AMI. They formed a "utility AMI security task force" which began to work "intensively."[87] However, by February 13, 2009, when the Commission issued minimum technical requirements, the task force reported that it had "much work yet to do before producing technical specifications that may be used by utilities to assess and procure security related functionality."[88] It noted "[s]ecurity must be built in from the beginning to be truly effective, but often it is the lowest consideration as all of the other competing demands are being pursued."[89] While acknowledging that they had "only begun to scratch the surface of addressing security issues" and that requirements would need to be revisited, they articulated nine security capabilities that they reviewed as necessary; these included authenticating users, maintaining data integrity and confidentiality, and providing audit logs and administration tools.[90]

---

83. *Id.* at 9–10.

84. *See* Notice Seeking Comment at 1, Competitive Metering, No. 00-E-0165 (N.Y. Pub. Serv. Comm'n Oct. 10, 2007), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={F81FB762-3011-4AB9-949B-EF73D78B88C1}.

85. *See id.* at 1–2.

86. *See* Notice of Technical Conference on Advanced Metering Infrastructure, Competitive Metering, No. 00-E-0165 (N.Y. Pub. Serv. Comm'n Mar. 3, 2008), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={4DC3DCBF-0974-44FC-BA74-003E9D1FCDFE}.

87. Order Adopting Minimum Functional Requirements for Advanced Metering Infrastructure Systems and Initiating an Inquiry into Benefit-Cost Methodologies at 16, Advanced Metering Infrastructure, No. 09-M-0074 (N.Y. Pub. Serv. Comm'n Feb. 13, 2009), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={16310751-0A41-401D-BFE5-7E95F5B3869D}.

88. *Id.*

89. *Id.*

90. *Id.*

The Commission issued these guidelines just one week before the passage of the American Recovery and Reinvestment Act of 2009 (ARRA), which included federal funding for smart grid research and development. Through conversations with federal officials, the Commission staff learned that applications would have greater chances of success if they also obtained supporting funds from non-federal sources. Accordingly, in April 2009 the Commission invited the utilities to submit their proposals for federal funding along with any requests for rate recovery.[91] All applicants for ARRA smart grid funding were required to describe how they would design cybersecurity into new systems, and the staff effectively deferred to the judgments of federal officials in evaluating the proposals. In July, the Commission authorized several utilities to recover costs associated with specific project proposals, explaining that they "rely on the DOE criteria . . . and [they] commend the cyber security and interoperability requirements contained in [their] AMI minimum functional requirements as a reference for the utilities' final planning and design phases of their smart grid projects."[92]

Five years later, the Commission again confronted questions about cybersecurity when considering Governor Andrew Cuomo's "Reforming the Energy Vision" initiative.[93] Spurred by the infrastructural weaknesses demonstrated during Hurricane Sandy, the vision essentially affirmed and accelerated efforts to develop a smart electrical grid. It emphasized using IT to create market-based incentives for increasing the integration of distributed energy resources (DER) into the grid. This increased the importance of distributed energy resource suppliers (DERS), organizations that provided a wide range of resources, such as demand response (i.e., reducing electricity demand at times of peak usage), distributed generation and storage, and more. And it also raised questions about how the Commission should exercise oversight over a growing number of actors.

In 2014, the Commission opened a proceeding to consider its oversight responsibilities under "Reforming the Energy Vision," and the following year

91. Letters were sent on April 2, 2009 and can be found in the docket for American Recovery and Reinvestment Act of 2009 - Utility Filings for New York Economic Stimulus, No. 09-E-0310 (N.Y. Pub. Serv. Comm'n), http://documents.dps.ny.gov/public/MatterManagement/CaseMaster.aspx?MatterCaseNo=09-E-0310.

92. Order Authorizing Recovery of Costs Associated with Stimulus Projects at 39, American Recovery and Reinvestment Act of 2009 - Utility Filings for New York Economic Stimulus, No. 09-E-0310 (N.Y. Pub. Serv. Comm'n July 27, 2009), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={60420742-E365-4DF5-8499-2F578BF4A74F}.

93. REFORMING THE ENERGY VISION (REV), www.rev.ny.gov (last visited Feb. 28, 2020).

it initiated a proceeding to consider oversight of DERS.[94] Both of these proceedings acknowledged the increased challenges for cybersecurity. In a 2015 ruling, the Commission noted, while most cybersecurity standards had been developed for generation and transmission assets, the increased integration of DER presented increased risks to distribution systems. Furthermore, it noted:

> There is no single set of security standards that we can simply direct utilities to comply with. It is unlikely that any definitive set of standards will ever exist, given the dynamic nature of the threat. . . . [S]ecurity methods, systems and protocols will always require constant vigilance and reassessment, with new vulnerabilities being discovered and exploited, and new countermeasures developed and implemented.[95]

While acknowledging that most efforts at cybersecurity focused on the bulk electric system, the Commission nonetheless highlighted smart grid standards developed by NIST. Ultimately, it chose not to issue new standards, citing "the many other efforts going on within the industry and . . . the constantly evolving nature of both the system and the threats."[96] Instead, it continued to evaluate the utilities' readiness based on existing standards, and it gave utilities the "primary responsibility for ensuring that DER providers selling services into the DSP [(Distributed System Platform)] are in compliance with all applicable standards."[97] However, this guideline soon brought the utilities into conflict with ESCOs, EDIs, and other companies using electricity data.

A. CYBERSECURITY STANDARDS IN DISPUTE

On March 29, 2018, an Electronic Data Interchange (EDI) platform provided by Energy Services Group LLC and in use by Energy Transfer Partners—a company operating pipelines for gas, oil, and related

94. These were respectively Reforming the Energy Vision, No. 14-M-0101 (N.Y. Pub. Serv. Comm'n), http://documents.dps.ny.gov/public/MatterManagement/CaseMaster.aspx?MatterCaseNo=14-M-0101; and Regulation and Oversight of Distributed Energy Resource Providers and Products, No. 15-M-0180 (N.Y. Pub. Serv. Comm'n), http://documents.dps.ny.gov/public/MatterManagement/CaseMaster.aspx?MatterCaseNo=15-M-0180.

95. Order Adopting Regulatory Policy Framework and Implementation Plan at 100, Reforming the Energy Vision, No. 14-M-0101, (N.Y. Pub. Serv. Comm'n Feb. 26, 2015), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={0B599D87-445B-4197-9815-24C27623A6A0}.

96. *Id.*

97. *Id.* at 101.

commodities—was hacked.[98] Energy Transfer Partners was able to continue its operations by "handling all scheduling in house," and resumed use of the platform on April 2nd.[99] However, five major utilities in New York—Central Hudson Gas and Electric, Consolidated Edison Gas and Electric, NYSEG, RG&E, Niagara Mohawk (d/b/a National Grid), and National Fuel Gas Distribution Corporation—were also using the EDI to communicate with energy service companies. When they learned of the breach—somewhat belatedly—they immediately stopped using the platform and demanded that Energy Services Group provide information about the security of its systems, test them again for security, and sign an agreement to undertake certain measures to improve security, including purchasing cybersecurity insurance.[100]

Each of these utilities also demanded that Energy Service Entities (ESEs)—a broad category which included ESCOs, Distributed Energy Resource providers, EDI providers, Direct Customers, and New York State organizations such as New York Power Authority (NYPA)—enter into a Digital Services Agreement (DSA) with each utility. In addition to an agreement related to the confidentiality of data, some of the utilities' DSAs included a set of cybersecurity requirements and an associated vendor risk assessment, which the utilities had already been using to determine whether their contractors were implementing appropriate security controls.[101]

However, ESCOs and many other organizations objected that they did not pose the same risks to the utilities as did their vendors, and that the DSA was inappropriate. Importantly, the ESCOs cited NIST standards, arguing that the DSA failed to account for the different levels of risk posed by specific entities. For instance, a group joining forces as "the ESCO Coalition" quoted from the NIST Cybersecurity Framework, stating that the Framework was "not designed 'as a one-size-fits-all approach to managing cybersecurity risk for critical infrastructure,' " and instead recognized that

98. Doug Olenick, *Update: Cyber-Attack knocks US Energy Services Group Offline,* SC MEDIA UK (Apr. 9, 2018), https://www.scmagazineuk.com/update-cyber-attack-knocks-us-energy-services-group-offline/article/1472917.

99. Ryan Collins & Meenal Vamburkar, *Cyber Attack Shuts Pipeline Data System, Energy Transfer Says*, WORLD OIL (Apr. 2, 2018), https://www.worldoil.com/news/2018/4/2/cyber-attack-shuts-pipeline-data-system-energy-transfer-says.

100. Joint Utilities DSA Petition at 8–9, Regulation and Oversight of Distributed Energy Resource Providers and Products, No. 15-M-0180 (N.Y. Pub. Serv. Comm'n Feb. 4, 2019), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={6F6929DD-DC16-45C8-AD41-14B2609B34BE}.

101. The DSA was based upon one previously approved by the Commission for Community Choice Aggregation (CCA) programs, with three significant additions: a data security rider with requirements for cybersecurity, a self-attestation form, and a requirement for the energy service entities to purchase cybersecurity insurance. *Id.* at 9.

> [o]rganizations will continue to have unique risks – different threats, different vulnerabilities, different risk tolerances. They will also vary how they customize practices described in the Framework. Organizations can determine activities that are important to critical service delivery and can prioritize investments to maximize the impact of each dollar spent.[102]

Accordingly, they argued that the utilities should not "have the power to unilaterally dictate specific security measures without first showing that the proposed requirements are appropriately tailored to the risk."[103] They argued that allowing the utilities "to unilaterally dictate specific security measures creates an unfair potential that the Joint Utilities will transfer a disproportionate amount of cyber risk to ESCOs and other market participants."[104] For example, ESCOs were particularly opposed to the proposed requirement that they and any third-party representatives purchase cybersecurity insurance with minimum liability limits of $10 million per event and annually.[105] They argued that any insurance requirement "should be based not on any arbitrary amount (as is the current $10 million requirement), but instead should be based on an assessment of the actual risks faced by each ESCO."[106] They also noted that the requirement "likely would make it impossible for ESCOs to deal with many third-parties, resulting in less competition and unnecessarily increased costs for consumers."[107]

Rather than taking a strong position on how national standards should be interpreted, the Commission's cybersecurity experts attempted to facilitate a business-to-business dialogue. On May 31, 2018, the Department of Public Service staff held a stakeholder meeting between the five utilities (which came to be known as the "Joint Utilities"), representatives of the energy service companies, EDI providers, and some DERS.[108] Over the next week, the utilities revised the five separate DSAs and associated risk assessments into a single uniform DSA and Self Attestation Form in which the entities were to affirm that they had implemented particular security controls. In early June, they circulated the revised forms requesting additional comment by June 22,

102. Comments of the New York Retail Choice Coalition and Supporting ESCOs on Proposed Data Security Agreement and Proposed Self-Attestation Form at 5, Cyber Security Protocols and Protections in the Energy Market Place, No. 18-M-0376 (N.Y. Pub. Serv. Comm'n June 22, 2018), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={9EB7F160-3AF6-483F-A5A7-23DFCD94005A}.

103. *Id.* at 7.

104. *Id.*

105. *Id.* at 3.

106. *Id.* at 12.

107. *Id.* at 10.

108. *Id.* at 1.

2018, but mandating the signing of the Self-Attestation Form by the end of June. In the meantime, on June 14th, the NYPSC initiated a proceeding on Cybersecurity Protocols in the Marketplace, directing its staff to monitor the business-to-business discussions and report back to the Commission by the end of the summer.[109]

However, there was no speedy resolution to the conflict over appropriate security requirements. Two additional days of technical conferences on July 26–27, 2018, yielded some progress, as did a follow-up conference call on August 1st. Nonetheless, many ESCOs requested further discussions, arguing that substantial problems remained. The utilities, however, argued that there was not enough time for further conversation, as they needed to reach closure by the end of the month to comply with the Commission's order. Accordingly, the utilities circulated a revised draft of the Self-Attestation Form on August 2nd, and a revised DSA on August 16th, mandating that they be signed by August 24th and 31st, respectively. As they emphasized in subsequent filings, the revised Self-Attestation Form consisted of sixteen security controls drawn from NIST standards for critical infrastructure security.[110] Accordingly, they argued that these represented a reasonable set of minimum standards.[111]

B. CALLS FOR MORE EXPERT DIALOGUE

However, the ESCOs and related companies continued to highlight problems with the requirements. At stake was not only whether the security requirements proposed by the utilities were an appropriate interpretation of national standards was at stake, but whether they were feasible. For instance, the self-attestation form required that data be encrypted in transit, but the companies noted that this was "impossible for unknown third-parties."[112] Although the companies continued trying to resolve various issues before the August deadlines mandated by the utilities, they failed to reach an agreement. Some companies signed under protest, while others refused to sign.

---

109. *See* Order Establishing Minimum Cybersecurity and Privacy Protections and Making Other Findings at 5, Regulation and Oversight of Distributed Energy Resource Providers and Products, No. 15-M-0180 (N.Y. Pub. Serv. Comm'n Oct. 17, 2019), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={99401E73-404B-4A4B-A0CA-6C2585DB7EFF}.

110. *See id.* at 6.

111. *See id.* at 7.

112. Comments of New York Retail Choice Coalition and Supporting ESEs in Opposition to Joint Utilities Petition for a Declaratory Ruling at 11, Cyber Security Protocols and Protections in the Enegery Market Place, No. 18-M-0376 (N.Y. Pub. Serv. Comm'n Nov. 30, 2018), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={4D20690A-1619-4DBD-846F-B986734AA6B1}.

The companies objected to the utilities' requirements and the process of negotiating those requirements, arguing that additional negotiation among experts was necessary. As early as June, Starion Energy argued that "the DSA fails to serve the Commission's worthy objective of data security protection. . . . [T]he DSA needs to be entirely reconceived, not merely redrafted, and a broader group of industry and technical experts needs to be engaged in the process."[113] In August and September, several companies and coalitions of companies called for the Commission to establish a cybersecurity working group akin to what had earlier been established for EDI.[114] Thus, by the end of the summer, the Commission's experts had neither resolved the technical challenges posed by the proposed requirements, nor ensured that a satisfactory level of expert dialogue occurred in the business-to-business process.

The Commission staff's report on the business-to-business process, filed in September, did little to ameliorate these grievances. The report commended the dialogue as "a nimble process by which the parties could develop cyber protections that address the significant concern facing New York's distribution utilities," and concluded that "the revised DSA strikes a fair balance between the Joint Utilities' concerns of both protecting the utility systems from infiltration and against customer data breaches, and the ESEs' concerns of overreaching and over-burdensome cyber security requirements."[115] They noted that roughly eighty percent of ESCOs had executed the DSA, and seventy-five percent had executed the Self-Attestation. Additionally, about half of the EDI providers had executed the DSA, and only about thirty-five percent had executed the Self-Attestation. They further stated that most of the "active ESEs that have not complied with the August deadlines or filed under protest,

113. Initial Comments of Starion Energy, Inc. at 2, Cyber Security Protocols and Protections in the Energy Market Place, No. 13-M-0376, (N.Y. Pub. Serv. Comm'n June 22, 2018), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={B1D2F816-6D9D-4723-A139-32D731703F4D}.

114. Retail Energy Supply Association's Motion to Form a Cybersecurity Working Group, Cyber Security Protocols and Protections in the Energy Market Place, No. 18-M-0376 (N.Y. Pub. Serv. Comm'n Aug. 28, 2018), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={D5E5B0A7-F775-45AB-9AB5-C972D2AB5B8E}; Final Comments of DSA Coalition Members on Proposed Data Security Agreement and Proposed Self-Attestation, Cyber Security Protocols and Protections in the Energy Market Place, No. 18-M-0376 (N.Y. Pub. Serv. Comm'n Sept. 24, 2018), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={679B4AFE-20E8-459C-A4E3-3BD9C9A4451F}.

115. Staff Report on the Status of the Business-to-Business Collaborative to Address Cyber Security in the Retail Access Industry at 3, Cyber Security Protocols and Protections in the Energy Market Place, No. 18-M-0376 (N.Y. Pub. Serv. Comm'n Sept. 24, 2018), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={46C17240-E3D1-4088-B45E-9E04C5A5886F}.

have not fully articulated the basis for not complying."[116] They speculated that this was because of the lack of Commission action, as well as what they called "inadequate justification for cyber insurance"—yet they did not recommend eliminating that justification.[117]

Despite tilting towards the utilities' position, in one sense the staff validated the ESEs' argument that security requirements should be tailored to the risks of the organization. It noted, for example, that "some DERS utilize different forms of electronic communication with the utilities and/or may receive different customer data points as compared to an ESCO."[118] Accordingly, it recommended establishing a business-to-business process for DERS and went on to facilitate multiple stakeholder meetings on this topic.[119] But overall, the staff report attempted one kind of closure—accepting the terms of the DSA and self-attestation—while acknowledging that requirements could never be entirely finalized. They noted calls for the Commission to establish a working group to discuss cybersecurity requirements and expressed support for such a group as a means of adapting the requirements "to an everchanging cyber landscape going forward."[120]

The utilities were emboldened by the staff report, citing its conclusions about the quality of the proceedings and fairness of the resulting requirements. Frustrated by what they viewed as the intransigence of the organizations refusing to sign the DSA, in November 2018, the utilities petitioned the Commission to rule that they could disconnect organizations from accessing their systems if they refused to sign the DSA and meet other security standards.[121]

However, ESEs protested, reiterating the problems with the DSA and objecting to the process by which it was drafted. For example, the Retail Energy Supply Association (RESA) objected to the staff's conclusion that the business-to-business process had been fair and produced a "balanced DSA," arguing that, "because of the superior bargaining power held by the Joint Utilities, the agreements provide the Joint Utilities with a significant amount

116. *Id.* at 5.

117. *Id.* at 6.

118. *Id.* at 8.

119. *See* Order Establishing Minimum Cybersecurity and Privacy Protections and Making Other Findings, *supra* note 109, at 5–6.

120. Staff Report on the Status of the Business-to-Business Collaborative to Address Cyber Security in the Retail Access Industry, *supra* note 115, at 7.

121. *See* Petition of the Joint Utilities for Declaratory Ruling, Retail Access Business Rules, No. 98-M-1343 (N.Y. Pub. Serv. Comm'n Nov. 9, 2018), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={13DAEE84-EF37-49D9-A67B-BCE38A46C041}.

of control over their ESCO competitors."[122] They continued to object to a number of provisions, including the utilities' assertion of the right to audit the ESCOs and the imposition of the cybersecurity insurance requirement, for the same reasons discussed above.

The Joint Utilities responded to such criticism by petitioning the Commission to affirm the business-to-business process and their right to require that the ESE's comply with several minimum standards, including requirements that the industry continued to dispute, such as purchasing cybersecurity insurance.[123] However, the ESCOs continued to object to the process, their objections being both what they saw as the superior bargaining power of the utilities and the lack of full and open dialogue among technical experts. The Mission:Data coalition went so far as to accuse the utilities of acting in bad faith, stating that they "seek to exploit the current climate of fear surrounding cybersecurity risks in order to inappropriately seize certain powers over distributed energy resource ("DER") suppliers."[124] The DSA coalition argued:

> The business-to-business process utilized thus far to develop the DSA and SAF was neither fair nor reasonable, because ESE's have always been under threat of repercussions by the Joint Utilities for not signing these agreements. Moreover, the Joint Utilities have virtually excluded any interactive dialogue between the respective information technology experts of ESEs and the Joint Utilities on the DSA and SAF, except for a single two-hour call on August 1, 2018, which only came about after vociferous complaints . . . of the Joint Utilities' non-responsiveness for weeks to repeated ESE requests for such integral, technical dialogue.[125]

122. Retail Energy Supply Association's Response to the Joint Utilities Petition for Declaratory Ruling at 3, Cyber Security Protocols and Protections in the Energy Market Place, No. 18-M-0376 (N.Y. Pub. Serv. Comm'n Dec. 21, 2018), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={3EDD440A-6A94-47BF-9697-C9E6189CE949}.

123. Joint Utilities DSA Petition, Cyber Security Protocols and Protections in the Energy Market Place, No. 18-M-0376 (N.Y. Pub. Serv. Comm'n Feb. 4, 2019), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={597AA41A-73AE-4C3B-8FBF-CB001F00A765}.

124. Case 18-M-0376—Proceeding on Motion of the Commission Regarding Cyber Security Protocols and Protections in the Energy Market Place, New York Public Service Commission, Response of Mission:data Coalition to the Commission's February 20, 2019 Notice Soliciting Comments at 2 (Apr. 29, 2019), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={07F2522E-390B-4669-939A-C05FCE80CF34}.

125. DSA Coalition Response to Joint Utilities II at 3, Regulation and Oversight of Distributed Energy Resource Providers and Products, No. 15-M-0180 (N.Y. Pub. Serv.

Similarly, the ESEs took issue with the findings of the Commission's experts. For example, the DSA coalition argued that the staff report "failed to recognize the Joint Utilities' superior bargaining position" and also failed to provide "independent analysis" of issues that the Commission had instructed it to address, such as vulnerabilities in the Joint Utilities' systems, "whether the Joint Utilities' mandated practices under the DSA and SAF would actually protect utilities' systems and confidential and sensitive customer information," or "analysis on whether insurance is an efficient and effective vehicle for mitigating financial risks."[126]

Similarly, RESA argued that the utilities' demands would not actually reduce risk, but simply transfer risk from the utilities to the ESEs. RESA argued: "[T]he DSA is nothing more than a contractual agreement governing liability and does not actually ensure that the utility network is not compromised by EDI transactions. The DSA itself does not increase or decrease any perceived risk to a utility's system, nor does executing the agreement mitigate any such perceived risk."[127]

The ESE's continued to raise questions about technical feasibility which could only be assessed by technical experts. For instance, they objected that some of the requirements—such as encrypting all data in transit—were not technically feasible for some kinds of communication, such as email communications with customers.[128]

Thus, by the spring of 2019, the Commission was failing to perform cybersecurity expertise. The problem was not that the Commission did not have access to knowledgeable and skilled individuals; the technical competence of the Commission's security team was not in question. Rather, the problem was that the Commission's experts were unable to forge a public consensus about what cybersecurity measures should be required of ESEs. This was largely because they were unable to facilitate an adequate level of dialogue among experts in different sectors of the industry, as demonstrated by the growing mistrust between the ESEs and the utilities.

In this context, the Commission staff could no longer simply defer to the experts in the industry, in particular the utility industry.

Comm'n Apr. 29, 2019), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={969DBFB3-F1B3-4BB9-84CF-E0BD298138CF}.

126. *Id.* at 8.

127. Retail Energy Supply Association's Response to the Joint Utilities ESE Petition at 10, Cyber Security Protocols and Protections in the Energy Martket Place, No. 18-M-0376 (N.Y. Pub. Serv. Comm'n Apr. 29, 2019), http://documents.dps.ny.gov/public/Common/ViewDoc.aspx?DocRefId={AF7FB9AE-0113-4CBA-96D3-349ED01A8DE5}.

128. *See* DSA Coalition Response to Joint Utilities II, *supra* note 119, at 13–14.

C. FINAL RULING

The Commission attempted to strike this balance on October 17, 2019, when it finally issued an "Order Establishing Minimum Cybersecurity and Privacy Protections and Making other Findings."[129] The order grounded its epistemic authority in cybersecurity standards such as those promulgated by NIST, by accepting the argument that cybersecurity requirements should be based upon risks. It distinguished between risks to the misuse of data and risks to information systems. Further, it noted that some organizations did not pose the same level of risk to information systems. Accordingly, while the Commission required nearly all of the ESEs to implement appropriate protections to protect customer privacy, it ruled that "only entities that electronically receive or exchange customer information from a direct connection with the utilities' IT systems, except by email, will need to adopt the cybersecurity requirements established in [the] Order."[130]

The Commission also acknowledged technical feasibility concerns raised by the ESEs, for example by exempting email communications from requirements that all confidential customer information be encrypted in transit. The Commission also allowed the utilities to require audits but ruled that such audits must be conducted by a third party rather than the utilities, as originally proposed, a provision which raised concerns about the protection of proprietary information. And perhaps in the biggest triumph for the ESEs, the Commission ruled that the organizations would not be required to purchase cybersecurity insurance.[131] The Commission ruled that "a cybersecurity insurance requirement, which is mainly intended to address damages after an incident occurs," would not reduce risk and "would serve to act as little more than a market barrier to entry."[132]

This order appears to have salvaged what was nearly a failed performance of expertise. The Mission:Data coalition praised the ruling as "a big win for innovation" and highlighted several aspects of the DSA and self-attestation form that the Commission had rejected.[133] The utilities moved forward with revising the forms as directed by the Commission. In the context of this increasingly competitive and fractious industry, performing cybersecurity

129. *See* Order Establishing Minimum Cybersecurity and Privacy Protections and Making Other Findings, *supra* note 109.

130. *Id.* at 36.

131. *Id.* at 58.

132. *Id.*

133. Robert Walton, *New York Adopts Utility-ESCO Cybersecurity Standards, Rejects Insurance Requirements*, UTILITY DIVE (Oct. 18, 2019), https://www.utilitydive.com/news/new-york-adopts-utility-esco-cybersecurity-requirements-rejects-insurance/565333/.

expertise required that the Commission's staff make detailed judgments about how to balance security against other goals, such as innovation and the integration of renewable energy resources.

VI. CONCLUSION

As the cases discussed above demonstrate, state and local regulators do not merely face the challenge of sourcing expertise; they must also help to perform authoritative expertise in a rapidly evolving technological landscape where consensus is often nowhere to be found. The New York Public Services Commission was very proactive about hiring both consultants and in-house experts in the wake of 9/11. Yet, performing cybersecurity expertise required more than simply hiring people; it also entailed making authoritative assessments of various proposals for improving cybersecurity, assessments which entailed balancing goals such as security, innovation, affordability, and more. This was no easy feat.

By most measures, the Commission's cybersecurity staff have successfully performed expertise. They have articulated cybersecurity standards that the electric sector has largely accepted, and there is little evidence that members of the public question the security assurances offered by the Commission, even after public breaches. While security is difficult, if not impossible, to measure, there is every reason to believe that the Commission's experts have improved security at the regulated utilities. But understanding how the Commission's experts have improved security requires attending to more than just hiring practices; it also requires analysis of how the Commission's experts cultivate relationships with the regulated utilities, related companies, and the artifacts that they seek to secure.

This Article has highlighted at least three contexts in which the Commission's staff cultivate these relationships. First, the Commission's experts have been called upon to investigate security breaches. In these contexts, they have typically highlighted best practices and industry standards By critiquing companies for failing to implement best practices and standards, the staff reinforce the notion that they possess the specialized knowledge and skills needed to avoid breaches in the future, and thereby enhance their own authority, even in the face of evidence that oversight has failed.

Second, the Commission's experts are often called upon to assess the legitimacy of requests to recover the costs of new cybersecurity initiatives. Here again, they often invoke standards and best practices, yet the implementation of standards often leaves much to the discretion of organizations. In everyday rate cases, ambiguities about how to apply standards are generally not discussed. Instead, both the utilities' and the Commission's

cybersecurity experts generally appear to agree on the need for specific investments, and both emphasize the need to keep pace with rapidly changing threats. The near-universal convergence of the Commission's experts and the utilities' experts suggest that a process of tacit coordination is likely at work. Ultimately, a substantial part of the Commission's experts' job is to maintain ongoing dialogue with the industry. Indeed, NARUC's recent guidelines note that "[a]s a regulator, if you can engage with the companies on [cybersecurity] informally, as a discrete issue separated from the baggage of a regulatory proceeding, you're likely to get better information."[134] This is particularly important in the context of cybersecurity, where the traditional regulatory emphasis on transparency may need to be balanced against the demands of security. The key point of this Article is that ongoing contact between the Commission's and utilities' experts not only allows for oversight, but it also allows for the coordination of cybersecurity planning behind closed doors, minimizing the potential for public disagreement about how to interpret and apply standards. This then enhances the authority of the Commission's expert recommendations.

However, the Commission's experts were unable to refer to best practices or coordinate planning behind closed doors in the third context discussed here: helping to adjudicate standards for a rapidly changing and divided industry. Although the Commission's experts attempted to simply facilitate the negotiation of cybersecurity requirements for organizations accessing utility data, they ultimately were forced to make specific recommendations to the Commission. These recommendations entailed judgments about not only technical feasibility, but also about how to balance security requirements against the desire to lower barriers to entry in a new and rapidly growing market for energy services. Performing cybersecurity expertise ultimately required more than just knowledge. It entailed earning trust in an increasingly competitive industry.

134. KEOGH & THOMAS, *supra* note 4, at 18.

ILLUSORY CONFLICTS: POST-EMPLOYMENT CLEARANCE PROCEDURES AND THE FTC'S TECHNOLOGICAL EXPERTISE

Lindsey Barrett[†], *Laura Moy*[††], *Paul Ohm*[†††] *& Ashkan Soltani*[‡]

ABSTRACT

The federal government restricts what former employees can work on after they leave the government, and for good reason. These post-employment conflict restrictions attempt to address the "revolving door" problem, where employees take information learned from their position in government to unfairly advantage industry. But an unintended consequence of overbroad conflict rules is that they impede well-meaning, former federal employees from providing their knowledge and general expertise to other enforcement agencies with similar missions, such as those at the state level. This is playing out right now with FTC technologists, at a time when the agency—and, indeed, consumer protection agencies more broadly—desperately needs greater technical expertise. Three problems result: (1) former FTC technologists find themselves unable to contribute to the enforcement efforts of other agencies and plaintiffs' attorneys aligned with the mission of the FTC, (2) some current FTC technologists are unwilling to work on important issues before the agency out of fear that doing so will limit their ability to work on related matters in the future, and (3) would-be technologists may be unwilling to take a position at the agency due to these concerns.

We explore the impact of federal conflict rules on technologists working with the FTC, consider how this impact has changed alongside changing circumstances and enforcement practices, and discuss policy implications. We conclude that unless the FTC reforms the way it administers its conflict rules, it risks losing the assistance of technological expertise—expertise of which it badly needs more, rather than less.

DOI: https://doi.org/10.15779/Z38901ZG6Z

† Adjunct Professor of Law and Fritz Family Fellow, Georgetown University Law Center.

†† Associate Professor of Law and Director of the Communications & Technology Law Clinic, Georgetown University Law Center.

††† Professor of Law and Associate Dean, Georgetown University Law Center. From 2012–13, Professor Ohm served as a Senior Policy Advisor for Privacy in the FTC's Office of Policy Planning.

‡ Distinguished Fellow, Institute for Technology Law & Policy and Center on Privacy & Technology at Georgetown University Law Center. From 2010–11, Mr. Soltani served as a staff technologist for the Division of Privacy and Identity Protection at the FTC. And from 2014–16, Mr. Soltani was appointed as the Chief Technologist of the FTC, wherein he helped in creating the Office of Technology Research and Investigation in order to expand the FTC's roster of technologists. The authors are grateful to Harsimar Dhanoa and Jeffrey Brown for excellent research assistance. They are also grateful to Chris Hoofnagle, Jessica Rich, and David Vladeck for helpful comments.

TABLE OF CONTENTS

I. INTRODUCTION 794

II. FEDERAL POST-EMPLOYMENT RESTRICTIONS 796

A. HISTORY AND GOALS OF FEDERAL POST-EMPLOYMENT RESTRICTIONS 796
B. POST-EMPLOYMENT CONFLICT OF INTEREST RESTRICTIONS UNDER 18 U.S.C. § 207 800
C. POST-EMPLOYMENT CONFLICT OF INTEREST RESTRICTIONS UNDER FTC RULES 802

III. POST-EMPLOYMENT RESTRICTIONS IN FTC PRACTICE TODAY 804

A. IMPACT OF POST-EMPLOYMENT RESTRICTIONS ON TECHNOLOGISTS 805
B. INCREASED MARKET CONSOLIDATION 807
C. TECHNOLOGISTS ACT AS UTILITY PLAYERS 810
D. LENGTHY AND BROAD CONSENT DECREES 813
E. RISK-AVERSE AGENCY CULTURE 815
F. POSSIBLE POLITICAL CONFLICT BETWEEN FTC AND STATE ATTORNEYS GENERAL 818

IV. IMPLICATIONS FOR AGENCY EFFICACY 822

V. POLICY RECOMMENDATIONS 826

VI. CONCLUSION 833

I. INTRODUCTION

The Federal Trade Commission's (FTC) laudable decade-long experiment to hire in-house technologists may be in jeopardy from an unexpectedly bureaucratic source: federal conflict of interest law. Post-employment restrictions for federal employees are designed to ensure that government officials avoid corruption and to slow the revolving door into industry. In their current application to former technologists, however, they have the counterproductive effect of preventing people with technical expertise from engaging in work that creates no meaningful conflicts.

Preventing technologists from accepting unproblematic post-government work through the conflicts clearance process harms the consumer protection and pro-competition missions of the agency. Overbroad conflicts clearance policies harm the direct mission of the agency by limiting the ability of experts

to aid fellow enforcers such as state attorneys general, who should be seen as force multipliers or fellow travelers in policing technology companies. These policies also make it more difficult for the FTC to hire and retain technological experts, which hampers the agency's ability to adequately fulfill its competition and consumer protection missions. Prospective technologists think twice about working for the agency when they hear about the way the clearance process has limited the activity of others. FTC employees also limit the cases they can work on in order to avoid potential post-employment conflicts.

This paper builds on the direct experience of two of the authors, one a former Chief Technologist and the other a former Senior Policy Advisor for privacy at the FTC. Since leaving the agency, we have encountered numerous obstacles in our experience with the FTC's clearance process, which we find to be unnecessarily broad in design and perhaps also in execution. We have bolstered this firsthand experience through interviews with numerous former FTC officials who confirm and expand upon our observations.

We begin with an outline of our methodology. We interviewed eight former FTC consumer protection attorneys and technologists and two attorneys in the offices of state attorneys general in order to assess the extent of the problem. The goal of the interviews was to determine whether the experience of two of us being denied the ability to work on certain matters post-FTC employment was representative, whether technologists and other specialists were treated differently for the purpose of conflicts, and whether there was any consensus as to why the FTC was applying the conflicts rules the way it was and still is.

Preserving anonymity to allow our interviewees to discuss sensitive topics was and is a key concern, given how few former technologists there are and how easily certain details would reveal the identity of the interviewees. For the reader's edification, we have tried to provide as much context as possible without compromising the anonymity of the interviewees, such as by highlighting when statements were contradicted by other interviewees, not contradicted by any interviewees, supported by interviewees, supported by only some interviewees, or when they were supported indirectly. Indeed, the difficulty of preserving the anonymity of our interviewees underscores the very problem enumerated in this essay—there are simply too few FTC technologists for the answers we describe here to allow each subject to get lost in a crowd.

We focus on the FTC because that is the agency with which we have direct experience, but the lessons of our analysis may also apply to other government agencies seeking to hire and retain technological experts, which ought to describe nearly every agency in this technological age. The way an agency

interprets the conflict of interest laws and the way it administers its clearance procedures can have an important, underappreciated impact on the way it fulfills its mission—and the ability of other enforcers to fulfill theirs.

Part II of this Article explains why the federal conflict rules were created and how they affected current and former agency employees at that time. Part III discusses how changes in technology, economy, market, and agency practices have altered the impact of these conflict rules on technologists working with the FTC. Part IV explores the implications of this changing impact on agency efficacy and on the FTC's ability to handle technical and other specialized subject matters. Part V offers policy recommendations to address this problem to help pave the way for the FTC and other federal agencies to increase their technical capacity, in part by hiring technical specialists.

II. FEDERAL POST-EMPLOYMENT RESTRICTIONS

Federal law restricts post-government employment opportunities for all federal government employees. The primary source of these restrictions across the federal government comes from one federal ethics statute, 18 U.S.C. § 207. In addition to § 207, former FTC employees must comply with post-employment restrictions set forth in the FTC Rules of Practice (i.e., 16 C.F.R. § 4.1(b)). As a starting point, it is helpful to understand more about the history, origin, and intent of these restrictions, as well as what they do and who interprets and enforces them.

A. HISTORY AND GOALS OF FEDERAL POST-EMPLOYMENT RESTRICTIONS

Both the federal conflict statute and the FTC's conflict rules were established in the 1960s.[1] Legislative and administrative history show that restrictions on where a former federal employee may work and what matters they may work on are intended to combat the "revolving door" problem and to prevent both actual government corruption and the appearance thereof.[2]

1. 18 U.S.C. § 207 was established in 1962 alongside several other federal anti-corruption provisions. Act to Strengthen the Criminal Laws Relating to Bribery, Graft, and Conflicts of Interest, and for Other Purposes, ch. 11, §§ 201–09, 218, 76 Stat. 1119–25 (1962). 16 C.F.R. § 4.1(b) was established in 1967. Commercial Practices, 32 Fed. Reg. 8444, 8456–59 (June 13, 1967).

2. *See* S. REP. NO. 95-170, at 32 (1977) ("18 USC 207, like other conflict of interest statutes, seeks to avoid even *the appearance* of public office being used for personal or private gain. In striving for public confidence in the integrity of government, it is imperative to remember that what appears to be true is often as important as what is true. Thus government

The rules are nevertheless intended to be somewhat restrained, balancing the need to combat these problems with the need to preserve the government's ability to attract and retain top-notch expertise.[3] Striking the right balance between these competing objectives—preventing corruption and facilitating expertise—is key to optimizing government function.

The federal statute designed to prevent actual and perceived conflict by former federal employees, § 207, was developed on the belief "that a public servant owes undivided loyalty to the Government."[4] The statute addresses two primary ways in which potential conflicts might occur. First, former federal employees could "switch sides" upon leaving the government, going on to provide other parties with an agency's proprietary information in an adversarial proceeding, which would limit the agency's ability to protect the public interest.[5] Second, if federal employees anticipate using their federal experience to help secure lucrative post-agency employment at a regulated entity, they might temper their behavior while employed by the agency.[6] Lax rules for post-agency employment conflicts would invite federal employees to mold their conduct at the agency to make themselves more appealing candidates for employment at a regulated entity after leaving the agency. The

in its dealings must make every reasonable effort to avoid even the appearance of conflict of interest and favoritism." (emphasis in original)).

3. *See id.* ("But, as with other desirable policies, it can be pressed too far. Conflict of interest standards must be balanced with the government's objective in attracting experienced and qualified persons to public service. Both are important, and a conflicts policy cannot focus on one to the detriment of the other. There can be no doubt that overly stringent restrictions have a decidedly adverse impact on the government's ability to attract and retain able and experienced persons in federal office.").

4. H.R. REP. NO. 87–145, at 3 (1961).

5. *Id.* at 4 ("[A]n official should be prohibited from resigning his position and 'switching sides' in a matter which was before him in his official capacity."); *see also* United States v. Nasser, 476 F.2d 1111, 1116 (7th Cir. 1973) (describing § 207 restrictions as serving to protect the government from use of agency information against the government); JACK MASKELL, CONG. RESEARCH SERV., POST-EMPLOYMENT, "REVOLVING DOOR," LAWS FOR FEDERAL PERSONNEL 1–2 (2014), https://fas.org/sgp/crs/misc/R42728.pdf ("One of the initial and earliest purposes of enacting the 'revolving door' laws was to protect the government against the use of proprietary information by former employees who might use that information on behalf of a private party in an adversarial type of proceeding or matter against the government, to the potential detriment of the public interest.").

6. MASKELL, *supra* note 5, at 2 ("Another interest of the government in revolving door restrictions was to limit the potential influence and allure that a lucrative private arrangement, or the prospect of such an arrangement, may have on a current federal official when dealing with prospective private clients or future employers while still with the government, that is, 'that the government employee not be influenced in the performance of public duties by the thought of later reaping a benefit from a private individual.' ") (quoting Brown v. D.C. Bd. of Zoning Adjustment, 413 A.2d 1276, 1282 (D.C. App. 1980)).

legislative history and subsequent cases interpreting the statute and rules also reflect a concern about the appearance of conflict, in addition to actual conflicts, because even the perception of corruption can erode public faith in the rule of law.[7]

Federal post-employment restrictions also aim to avoid being overly rigid. Overly rigid conflict rules might make it impossible to draw top talent to agencies where employees with needed expertise could easily find employment with other agencies or the private sector.[8] Indeed, in enacting and revising § 207, Congress was acutely aware that restrictive rules could hamstring the government's ability to attract and retain technical experts. For example, in a 1960 House hearing on federal conflict of interest legislation, a representative of the Department of Defense expressed concern that the proposed § 207 "would greatly narrow the opportunity for [people who came to government from private industry] to seek employment outside the Government if they were precluded thereafter from rendering any assistance to anyone in connection with any subject matter concerning which they had any responsibility."[9] The Defense Department representative also pointed out that "[w]e have had considerable difficulty in recruiting engineers and scientists."[10]

As Congress deliberated over the structure and wording of conflicts restrictions in the year before passage of the bill that established § 207, President Kennedy sent a letter to Congress urging accommodations for temporary, part-time, and technical experts:

> The fundamental defect of [conflict] statutes as presently written is that: On the one hand, they permit an astonishing range of private interests and activities by public officials which are wholly incompatible with the duties of public office; on the other hand, they create wholly unnecessary obstacles to recruiting qualified people for government service. This latter deficiency is particularly serious in the case of consultants and other temporary employees, and has

7. *Id.*; *see also* Adam Samaha, *Regulation for the Sake of Appearance*, 125 HARV. L. REV. 1563, 1599 (2011) (discussing ethics rules designed to facilitate public trust by diminishing the possible appearance of corruption).

8. MASKELL, *supra* note 5, at 2 ("These purposes in adopting limitations on former employees' private employment opportunities must, however, also be balanced against the deterrent effect that overly restrictive provisions on career movement and advancement will have upon recruiting qualified and competent persons to government service."); S. REP. NO. 95–170, at 32 (1977).

9. *Federal Conflict of Interest Legislation: Hearing on H.R. 1900, H.R. 2156, H.R. 2157, H.R. 6556, and H.R. 10575 Before the H.R. Antitrust Subcomm. of the Comm. on the Judiciary*, 86th Cong. 144 (1960) (statement of Stephen S. Jackson, Deputy Assistant Secretary of Defense for Manpower, Personnel, and Reserve).

10. *Id.*

> been repeatedly recognized by Congress in its enactment of special exemption statutes . . .
>
> But if the statutes often leave important areas unregulated, they also often serve as a bar to securing important personal services for the government through excessive regulation when no ethical problem really exists. Fundamentally, this is because the statutes fail to take into account the role in our government of the part-time or intermittent adviser whose counsel has become essential but who cannot afford to be deprived of private benefits, or reasonably requested to deprive themselves, in the way now required by these laws. Wherever the government seeks the assistance of a highly skilled technician, be he scientist, accountant, lawyer, or economist, such problems are encountered.[11]

The following decade, after the Watergate scandal, Congress passed the Ethics in Government Act, which revised and crafted new post-employment restrictions as part of a wave of reforms.[12] Before the new restrictions went into effect, however, a number of parties raised concerns that the restrictions might interfere with the hiring of high-caliber employees.[13] In a report on the legislation, the Subcommittee on Oversight and Investigations of the House Committee on Interstate and Foreign Commerce explained that ethics restrictions should "accommodate the need to attract and retain a qualified and experienced work force."[14] The report also stated that "hearings reflected the grave concern of agency heads" that the "balance between maintaining integrity and ensuring an able work force has not been properly struck."[15] For example, the Secretary of Health, Education, and Welfare characterized the revisions as likely to cause "the greatest brain drain of talent in the history of Federal service."[16] Recognizing the need to strike a balance between preventing

11. President's Special Message to the Congress on Conflict-of-Interest Legislation and on Problems of Ethics in Government, 1961 PUB. PAPERS 327–329 (Apr. 27, 1961).

12. SAM BERGER & ALEX TAUSANOVITCH, CTR. FOR AM. PROGRESS, LESSONS FROM WATERGATE: PREPARING FOR POST-TRUMP REFORMS 3–6 (2018), https://cdn.americanprogress.org/content/uploads/2018/07/27101947/WatergateReformsReport-3.pdf (discussing the Ethics in Government Act and other "extensive" post-Watergate government reforms). Among other things, the 1978 Ethics in Government Act established "a mechanism for the appointment of an independent special prosecutor"; created the Office of Government Ethics; and "imposed the first mandatory financial disclosures for members of Congress, candidates, and some high-level executive branch officials." *Id.*

13. STAFF OF THE SUBCOMM. ON OVERSIGHT & INVESTIGATIONS OF THE H. COMM. ON INTERSTATE & FOREIGN COMMERCE, 96TH CONG., CONG. REP. ON IMPACT OF THE ETHICS IN GOV'T ACT 5 (Comm. Print 1979).

14. *Id.*

15. *Id.*

16. *Id.*

conflicts and attracting top talent, Congress ultimately softened the new limitations before they went into effect.[17]

B. POST-EMPLOYMENT CONFLICT OF INTEREST RESTRICTIONS UNDER 18 U.S.C. § 207

The federal statute defining post-employment conflicts, § 207, is both a criminal and a civil statute; those who violate it could end up in prison or be subject to a hefty civil penalty.[18] The statute is enforced by the Department of Justice (DOJ),[19] but the Office of Government Ethics (OGE) has regulatory authority to promulgate rules, providing further details on the application of § 207 beyond what is provided in the statute.[20] In addition, the FTC provides direct guidance to former employees regarding § 207.[21] Under § 207, former federal employees are not prohibited from taking a job with any other potential employer but are prohibited from engaging in certain activities.[22] For former FTC employees, there are two types of conduct prohibited under the federal statute of which they should be aware.

First, the federal statute essentially prohibits a former federal employee from switching sides on a matter on which they previously represented the federal government.[23] If a former FTC employee communicates to, or appears

17. OFFICE OF GOV'T ETHICS, REPORT TO THE PRESIDENT AND TO CONGRESSIONAL COMMITTEES ON THE CONFLICT OF INTEREST LAWS RELATING TO EXECUTIVE BRANCH EMPLOYMENT 14 (2006) ("Before these new restrictions even became effective, Congress amended section 207 to lighten the new restrictions, in response to expressions of concern about the expected impact on recruitment and retention.").

18. An offense can result in up to a year in prison, and a willful offense can result in up to five years. 18 U.S.C. § 216(a) (2018). In addition, a person who violates § 207 can be subject to a civil penalty up to fifty-thousand dollars for each violation or the amount of compensation which they received for the prohibited conduct, whichever amount is greater. 18 U.S.C. § 216(b).

19. Post-Employment Conflict of Interest Restrictions, 5 C.F.R. § 2641.103(a) (2020).

20. 5 C.F.R. § 2638.108(a)(1).

21. *See* 5 C.F.R. § 2641.105(a) (stating that "[t]he agency in which an individual formerly served has the primary responsibility to provide oral or written advice concerning a former employee's post-employment activities," including regarding § 207). This is consistent with our experience. Staff of the FTC's Office of General Counsel have provided us with guidance and advice regarding the application of § 207 to post-employment activities that we have inquired about.

22. 18 U.S.C. § 207; *see* OFFICE OF GOV'T ETHICS, *supra* note 17, at 11 ("None of its provisions bars any individual, regardless of rank or position, from accepting employment with any private or public employer after Government service. Section 207 only prohibits former employees from engaging in certain activities on behalf of persons or entities other than the United States, whether or not done for compensation.").

23. 18 U.S.C. § 207; *see* MASKELL, *supra* note 5, at 2–3; United States v. Nasser, 476 F.2d 1111, 1116 (7th Cir. 1973) (holding in favor of constitutionality of prohibition language).

before, the federal government as a part of their new job with the intent to influence "in connection with a particular matter . . . in which the person participated personally and substantially" as a federal employee, that behavior constitutes a violation.[24] This prohibition lasts forever.

Second, even for a matter in which the former federal employee did *not* "participate[] personally and substantially," § 207 still prohibits the person from working on it if the person "knows or reasonably should know [the matter] was actually pending under his or her official responsibility . . . within a period of 1 year before the termination" of their employment.[25] This restriction expires after two years.[26]

In determining whether a former matter and a post-employment matter are the same, OGE rules state that "all relevant factors should be considered, including the extent to which the matters involve the same basic facts, the same or related parties, related issues, the same confidential information, and the amount of time elapsed."[27]

§ 207(j) lays out a number of exceptions to these general restrictions. For example, under this subsection, former employees are exempted from certain post-employment restrictions to carry out official duties as a federal employee, state or local government official, or representative of a higher education institution. One exception that is particularly relevant to agency technologists is an exception under several provisions of § 207 for "communications [made] solely for the purpose of furnishing scientific or technological information, if such communications are made under procedures acceptable to the department or agency concerned."[28]

As noted above, § 207 is enforced by the DOJ.[29] Accordingly, an agency where a former federal employee served—such as the FTC—does not have the authority to determine definitively how § 207 applies to a former employee, but the agency is responsible for providing former employees with advice regarding the application of § 207 to post-employment activities.[30] In

24. 18 U.S.C. § 207(a)(1). This only applies when the matter also is one "in which the United States or the District of Columbia is a party or has a direct and substantial interest," and "which involved a specific party or specific parties at the time" the former employee worked on it. *Id.* Former federal employees also cannot engage in this variety of prohibited communications and/or appearances before the District of Columbia. *Id.*

25. 18 U.S.C. § 207(a)(1)–(2).

26. *Id.* For a more fulsome explanation of the provisions of § 207, including restrictions not discussed here, see MASKELL, *supra* note 5, at 3–6.

27. 5 C.F.R. § 2641.201(h)(5)(i).

28. 18 U.S.C. § 207(j)(5).

29. 5 C.F.R. § 2641.103(a).

30. 5 C.F.R. § 2641.105(a).

determining whether and how to pursue prosecution under § 207, however, the DOJ may take into account a former federal employee's reliance on advice received from the agency where they formerly served.[31]

C. POST-EMPLOYMENT CONFLICT OF INTEREST RESTRICTIONS UNDER FTC RULES

The FTC's rules also restrict what matters a former employee can work on after their employment with the FTC ends.[32] Generally speaking, the FTC's post-employment conflict rules prohibit former employees from communicating to or appearing before the FTC and from assisting or advising behind-the-scenes regarding certain "proceeding[s] or investigation[s]."[33]

Most relevant to former technologists is § 4.1(b) of the FTC's rules.[34] After leaving the agency, a former employee generally cannot work on a proceeding or investigation that is the same as one in which they "participated" on behalf of the agency.[35] A former employee also cannot later work on a proceeding or investigation if they received or saw "nonpublic documents or information" pertaining to it while working for the agency.[36] These restrictions are permanent, but the FTC's rules also establish certain time-limited restrictions for former employees.[37]

There is no bright-line rule that enables a former employee to conclude with certainty that an activity in which they would like to engage constitutes the same "proceeding or investigation" as one in which they participated while employed by the FTC. According to a note in the FTC's rules, "a new 'proceeding or investigation' may be considered the same matter as a seemingly separate 'proceeding or investigation' that was pending during the former employee's tenure."[38] In assessing this differentiation, "the Commission . . . consider[s]: the extent to which the matters involve the same or related facts, issues, confidential information and parties; the time elapsed; and the

31. 5 C.F.R. § 2641.105(c).

32. 16 C.F.R. § 4.1(b)(1) (2020).

33. *Id.*; *see Post-Employment Restrictions*, FED. TRADE COMM'N, https://www.ftc.gov/about-ftc/bureaus-offices/office-general-counsel/post-employment-restrictions (last visited Aug. 22, 2020).

34. 16 C.F.R. § 4.1(b).

35. *Id.*

36. *Id.*

37. *Id.* A former employee cannot work on a proceeding or investigation that was pending under their official responsibility within a year of when they left the agency. *Id.* This restriction lasts for two years after an employee leaves the agency. *Id.* In addition, for one year after leaving the agency, Commissioners and "senior employees" cannot work on any proceeding or investigation before the FTC. *Id.*

38. 16 C.F.R. § 4.1(b)(1) n.1.

continuing existence of an important Federal interest."[39] These criteria are nearly identical to the criteria considered by the OGE in determining whether a former matter and post-employment matter are the same under § 207.[40]

The FTC's rules also set forth a formal process to help former employees determine whether or not they are indeed restricted from working on a matter in their non-FTC employment capacity.[41] In certain circumstances, a former employee is required to file a "request for clearance" to participate in a matter that is or was before the FTC.[42] If the former employee left the agency within the previous three years, these circumstances include when the proceeding or investigation was pending before the FTC while the former employee was there, when the matter is the direct result of another proceeding or investigation that was pending before the FTC while the former employee was there, or when "nonpublic documents or information" pertaining to the matter were seen (or likely would have been seen) by the former employee as part of their work for the FTC.[43]

After a former employee files a clearance request, the FTC's Office of the General Counsel (OGC), or designee, has ten business days to respond by (1) granting the request, (2) stating that it recommends the FTC deny the request, or (3) extending its consideration of the request by up to ten additional business days.[44] If a former employee is not sure whether or not they need to file a clearance request, they can ask the General Counsel for advice.[45] The General Counsel or their designee will provide advice within three business days.[46]

Significantly, the FTC's rules grant the agency the discretion to simply decline to apply the rules to any specific set of circumstances. In addition, the rules do not apply to post-employment activities that would be covered if "otherwise specifically authorized by the Commission."[47]

While § 207 is enforced by the DOJ, the FTC's post-employment conflict of interest restrictions are applied and enforced only by the FTC itself. To help current and former employees better understand the rules, the FTC provides guidance on its website.[48] The agency also gives new employees an ethics guide.

39. *Id.*
40. *See* 5 C.F.R. § 2641.201(h)(5)(i).
41. *See* 16 C.F.R. § 4.1(b)(2).
42. *Id.*
43. *Id.*
44. 16 C.F.R. § 4.1(b)(7).
45. 16 C.F.R. § 4.1(b)(6).
46. *Id.*
47. 16 C.F.R. § 4.1(b)(1).
48. *Post-Employment Restrictions*, *supra* note 33.

The guide states: "if an FTC matter was open during your [(i.e., former employee's)] time here, you likely need to receive clearance before you work on it for a new employer. If you worked on the matter while at the FTC or had access to significant non-public FTC information about the matter, you are unlikely to get clearance."[49]

III. POST-EMPLOYMENT RESTRICTIONS IN FTC PRACTICE TODAY

As discussed above, post-government employment restrictions seek to balance the need to combat the revolving door and corruption with the need to preserve the government's ability to attract and retain top-notch expertise. In the modern era, however, there is a greater need than ever in government—and perhaps especially in the FTC—for highly-skilled, technical expertise.[50] As a result, these restrictions appear to be off-balance with the FTC interpreting and applying post-government restrictions aggressively to combat the revolving door and corruption at the cost of attracting and retaining technical expertise. This is particularly true as applied to conduct that supports the FTC's objectives and doesn't implicate the corruption concerns that § 207 was designed to address. A former FTC technologist seeking to consult on a state attorney general investigation regarding consumer protection matters is better described as entering an adjoining wing than availing herself of a revolving door. Section III.A begins by identifying how post-employment restrictions arguably are failing to facilitate hiring and retention of skilled experts, specifically technologists. Why would the FTC administer conflict rules more broadly than necessary to advance the policy goals of preventing corruption and slowing the revolving door? Sections III.B–F identify several possible explanations, including increased market consolidation, the growing role of technologists as utility players, the length and breadth of consent decrees, the agency's risk-averse culture, and possible political conflicts between the FTC and other enforcement agencies.

49. FED. TRADE COMM'N, LET'S TALK ETHICS: ETHICS ORIENTATION FOR NEW EMPLOYEES 7 (2019), https://www.ftc.gov/system/files/attachments/office-general-counsel/ieo_for_new_ftc_employees.pdf.

50. For a discussion by the former FTC Commissioner on enforcement and oversight challenges created by rapidly changing technology and the possibility that the FTC is failing to keep up, see generally Terrell McSweeny, *Psychographics, Predictive Analytics, Artificial Intelligence, & Bots: Is the FTC Keeping Pace?*, 2 GEO. L. TECH. L. REV. 514 (2018).

A. IMPACT OF POST-EMPLOYMENT RESTRICTIONS ON TECHNOLOGISTS

The FTC's application of post-employment restrictions today goes beyond the policy goal of limiting corruption and the appearance of corruption.[51] The FTC may also apply post-government employment restrictions too broadly in cases involving former employees who want to work for the companies the FTC investigates, but we focus here primarily on circumstances for which there are clear public policy reasons to support a more permissive interpretation of post-employment restrictions: requests to work for state attorneys general seeking to investigate violations of law. In these cases, prohibiting former technologists from contributing does not serve the federal conflicts provisions' goal of preventing employees from leaving the government and "switching sides." On the contrary, these other entities are best characterized as being on the *same side* as the FTC, and their law enforcement work is consonant with the consumer protection and pro-competition missions of the FTC.

As technologists and former FTC officials, two of us have encountered firsthand the FTC's broad interpretation of post-employment restrictions precluding us from contributing to valuable enforcement work by other agencies and plaintiffs. In addition, we conducted informal interviews of several other former FTC employees and technologists in order to ascertain additional information and context about how post-employment restrictions affect technologists.[52]

From these interviews, we heard consistent variations on a theme: *there was general consensus that the rules were overly broad, their application opaque, and their impact felt acutely and disproportionately by former technologists*. While not everyone we spoke to had sought clearances themselves, many were aware of the process from colleagues. Several, however, had firsthand experience contacting the FTC to seek advice and, ultimately, clearance regarding matters they would like to work on that could be construed as related to matters they had worked on while employed by the FTC.

In particular, former technologists—ourselves included—have often been denied clearance by the FTC, under its own rules, to help others investigate entities subject to FTC enforcement even after a substantial period of time has passed. The crux of the problem is that the FTC often considers a state attorney general's current investigation regarding a major company to be the same "proceeding or investigation" as one conducted by the FTC of the same company for related practices—even if the FTC's investigation culminated in

51. *See* MASKELL, *supra* note 5, at 2.

52. For a discussion of methodology, see *supra* Part I.

a complaint that has already been settled with the company in question.[53] The FTC further appears to consider technologists to have "participated personally and substantially" in its investigations of technology companies.[54]

In other words, the FTC interprets its conflict rules as prohibiting us from working on the "same side" as the FTC in investigations that run parallel to the agency's mission. On at least three occasions, we have sought clearance to provide technical guidance to state attorneys general investigating the practices of major technology companies. Two of these requests for clearance were denied and the third took weeks to process. In fact, on one occasion, FTC staff told one of us directly that, even though providing assistance to a state attorney general would be working on the "same side" as the FTC, this was "irrelevant to the analysis" under FTC rules.[55]

The conflicts rules are intended to prevent the appearance or actual existence of conflicts between current employees and companies the FTC oversees, not other enforcement entities.[56] By making it unduly difficult for former technologists to receive clearances, the agency makes it less attractive for technologists to work there and discourages those who do from working on certain cases, thus limiting the agency's own efficacy. This problem is intensifying as technological advancements increase the FTC's need for technical expertise.[57] In turn, this problem also makes other avenues in the

53. 16 C.F.R. § 4.1(b)(1)(i) (restricting post-employment activities if "[t]he former employee participated personally and substantially on behalf of the Commission in the same proceeding or investigation in which the employee now intends to participate"). As discussed below, this problem likely is compounded by the fact that FTC consent decrees typically last for twenty years. *Infra* Section III.D.

54. 16 C.F.R. § 4.1(b)(1)(i). As discussed below, this problem likely is compounded by the fact that FTC technologists are relied upon as utility players. *Infra* Section III.C.

55. Email from Alternate Designated Agency Ethics Official, Office of the General Counsel, Federal Trade Commission, to one of the authors (Mar. 01, 2019, 08:00 EST) (on file with authors).

56. *See* MASKELL, *supra* note 5, at 2 (identifying the animating goals of "revolving door" laws as "protect[ing] the government against the use of proprietary information by former employees who might use that information *on behalf of a private party* in an adversarial type of proceeding or matter against the government, to the potential detriment of the public interest," "limit[ing] the potential influence and allure that a lucrative *private* arrangement, or the prospect of such an arrangement, may have on a current federal official when dealing with prospective *private* clients or future employers while still with the government," and "prevent[ing] the corrupting influence on the governmental processes of both legislating and administering the law that may occur, and the appearances of such influences, when a federal official leaves his government post to 'cash in' on his 'inside' knowledge and personal influence with those persons remaining in the government.") (emphasis added).

57. *See generally* McSweeny, *supra* note 50.

U.S. enforcement ecosystem less effective because it limits the access of state attorneys general to qualified technology experts.

In addition to interpreting its own rules in this manner, the FTC also appears to interpret § 207 quite broadly. FTC staff have advised us that activities we sought to assist alongside state attorneys general could implicate § 207 as constituting the same matter as one in which we had participated at the FTC.[58]

The FTC's procedural approach to former employees' conflict clearance inquiries raises additional problems. Based on our experience and that of the people we interviewed, it seems the FTC's OGC routinely denies clearance requests through an informal process completed over email. The OGC sometimes advises former employees to submit a formal clearance request using a form designed for that purpose, but often does not. This approach limits the transparency of the decision, avenues for appeal, and rigor of the analysis.

B. INCREASED MARKET CONSOLIDATION

Increased market concentration and horizontal expansion in the technology sector also contribute to the agency's broad application of conflicts rules to technologists. In a diversified market, it can be easy to tell that a former FTC employee's work investigating Company A is not the same "matter" as, or is an unrelated "proceeding or investigation" to, work involving Company B. But when Company A is at the heart of both the prior investigation and the prospective work—perhaps because Company A acquired "nascent or potential competitor" Company B to eliminate a threat to Company A's market—the potential for conflict of interest may be higher.[59]

There is no question that recent years have seen massive corporate consolidation, both vertical and horizontal.[60] The technology sector, in

58. 18 U.S.C. § 207(a)(1)(A) (restricting post-employment activities related to a particular matter "in which the United States or the District of Columbia is a party or has a direct and substantial interest").

59. Press Release, Fed. Trade Comm'n, FTC to Examine Past Acquisitions by Large Technology Companies (Feb. 11, 2020), https://www.ftc.gov/news-events/press-releases/2020/02/ftc-examine-past-acquisitions-large-technology-companies (describing current FTC investigation of anti-competitive acquisitions by technology companies).

60. *America's Concentration Crisis: An Open Markets Institute Report*, OPEN MKTS. INST., https://concentrationcrisis.openmarketsinstitute.org/ (last visited Aug, 22, 2020) (illustrating the wave of consolidation across a wide range of industries over the past fifty years); Lina M. Kahn, *The Ideological Roots of America's Market Power Problem*, 127 YALE L.J.F. 960, 964 (2018), http://www.yalelawjournal.org/forum/the-ideological-roots-of-americas-market-power-problem (tracing the rise of concentration and the "cripple[ing]" of antitrust enforcement);

particular, exhibits a steady trend toward greater consolidation.[61] For example, according to a recent report from the Open Markets Institute, the three largest social networking sites controlled eighty-five percent of the market in 2018, up from seventy-five percent in 2012; the two largest search engines controlled ninety-seven percent of the market in 2017, up from eighty-two percent in 2011; and the two largest e-commerce firms controlled fifty-six percent of the market in 2018, up from forty-six percent in 2016.[62]

In addition to greater consolidation in the technology sector, the resultant diminished number of targets for enforcers to go after overall has provided all enforcement agencies—including the FTC—clear reasons to investigate the largest companies for violations of trade practice law. Precisely because of their outsized market shares, large companies that violate the law have the potential to cause substantial injury to large numbers of consumers.[63] And an enforcement agency with limited resources will get the greatest "bang for its buck" going after companies with large numbers of users, substantial economic clout, and a high public profile, rather than going after smaller companies. Thus when the FTC announced its record five-billion-dollar settlement with Facebook in 2019, the size of the company was relevant: as the agency stated in its press release, "[m]ore than 185 million people in the United States and Canada use Facebook on a daily basis."[64]

A review of recent enforcement actions reveals that the enforcement efforts of the FTC and state attorneys general are indeed converging on a handful of companies. For example, in the last two years alone, Facebook has been both a target of the FTC and the subject of public investigations by

David Leonhardt, *The Monopolization of America*, N.Y. TIMES (Nov. 25, 2018), https://www.nytimes.com/2018/11/25/opinion/monopolies-in-the-us.html (describing and opining on the Open Markets dataset).

61. Lina M. Khan, *Amazon's Antitrust Paradox*, 126 YALE L.J. 710, 710 (2017) (criticizing consumer welfare as ill-adapted to measure anti-competitive harms in the twenty-first century economy, particularly online platforms); Frank Pasquale, W*hen Antitrust Becomes Pro-Trust: The Digital Deformation of U.S. Competition Policy*, 2017 CPI ANTITRUST CHRON., May 2017, at 1, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3020163 (analyzing the consolidation of the technology sector and describing the failures of antitrust doctrine, and the interpretation and application thereof by U.S. regulators, to new trends).

62. *America's Concentration Crisis*, *supra* note 60. Although the specific search engines controlling the largest market share have changed between 2011 and 2017, the increase in the market share owned by the two largest companies at that time nevertheless reflects market consolidation.

63. When it violates the law, a company that has a billion users has the potential to do greater harm than a company that has only a few thousand users.

64. Press Release, Fed. Trade Comm'n, FTC Imposes $5 Billion Penalty and Sweeping New Privacy Restrictions on Facebook (July 24, 2019), https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.

attorneys general in California,[65] the District of Columbia,[66] Massachusetts,[67] New York,[68] and Washington,[69] as well as by a group of at least forty-seven state attorneys general investigating Facebook for potential antitrust violations.[70] Similarly, Google settled a complaint with the FTC in August 2019 but has been publicly investigated in the past two years by Arizona,[71] Connecticut and New York (in tandem),[72] and fifty attorneys general probing the company's competition practices.[73]

Because of the increase in the number of investigations targeting the same handful of companies, a former employee who wishes to assist another enforcer with a new case is increasingly likely to find that the new case concerns an old target.

---

65. Cecilia Kang & David McCabe, *California Sues Facebook for Documents in Privacy Investigation*, N.Y. TIMES (Nov. 6, 2019), https://www.nytimes.com/2019/11/06/technology/facebook-california-investigation.html.

66. Matthew P. Denn & Amanda Fitzsimmons, District of Columbia v. Facebook: *General Consumer Protection Statute Can Serve as Vehicle for State Attorney General Seeking Redress for Data Privacy Violations*, DLA PIPER (June 12, 2019), https://www.dlapiper.com/en/us/insights/publications/2019/06/district-of-columbia-v-facebook/.

67. Associated Press, *Facebook Must Provide Info Sought by Massachusetts Attorney General*, BOSTON.COM (Jan. 19, 2020), https://www.boston.com/news/local-news/2020/01/19/facebook-must-provide-info-sought-by-massachusetts-attorney-general.

68. Makena Kelly, *New York's Attorney General Is Investigating Facebook After Contact-Scraping Scandal*, THE VERGE (Apr. 25, 2019, 5:15 PM), https://www.theverge.com/2019/4/25/18516716/new-york-attorney-general-facebook-contact-scraping-letitia-james.

69. Associated Press, *Washington Attorney General Sues Facebook over Campaign Ads*, U.S. NEWS & WORLD REP. (Apr. 14, 2020, 5:47 PM), https://www.usnews.com/news/best-states/washington/articles/2020-04-14/washington-attorney-general-sues-facebook-over-campaign-ads.

70. Tony Romm, *Forty-Six Attorneys General Have Joined a New York-Led Antitrust Investigation of Facebook*, WASH. POST (Oct. 22, 2019, 1:32 PM), https://www.washingtonpost.com/technology/2019/10/22/forty-six-attorneys-general-have-joined-new-york-led-antitrust-investigation-into-facebook/.

71. Ali Breland, *Arizona Investigating Google's Location Tracking: Report*, THE HILL (Sept. 11, 2018, 3:33 PM), https://thehill.com/policy/technology/406106-arizona-investigating-googles-location-tracking-report.

72. Reuters, *At Least Two US Attorneys General Are Investigating the Google+ Glitch that Exposed Hundreds of Thousands of Users' Personal Data*, BUS. INSIDER (Oct. 9, 2018, 4:37 PM), https://www.businessinsider.com/some-us-attorneys-general-are-investigating-google-data-breach-2018-10.

73. Makena Kelly, *Google Under Antitrust Investigation by 50 Attorneys General*, THE VERGE (Sept. 9, 2019, 2:59 PM), https://www.theverge.com/2019/9/9/20857440/google-antitrust-investigation-attorneys-general-advertising-search.

C. TECHNOLOGISTS ACT AS UTILITY PLAYERS

Unlike most other roles at the FTC, every FTC technologist is forced to be a utility player. Although the FTC employs hundreds of attorneys and dozens of economists,[74] it employs fewer than ten technologists.[75] The number of technologists has ebbed and flowed and has been as low as only one. Over the past couple decades, however, the technical complexity of U.S. commerce has grown, thereby increasing agency demand for technical expertise. This has an important impact on conflicts. Attorneys and economists can specialize in narrow slices of the agency's work and focus on a small docket of investigations, but technologists tend to work on a broad set of matters. As a result, for purposes of applying the FTC's post-employment restrictions, technologists may be more likely than other FTC employees to be considered to have "participated personally and substantially" in any FTC investigation of a major company.[76]

Technology now pervades nearly every industry the FTC oversees, leading some to refer to it as the "Federal Technology Commission."[77] The biggest driver of increasing technical complexity is, of course, the growth of computers and the internet to their modern-day prevalence.[78] Personal computers and the internet are still relatively recent phenomena. In the nineteen years from 1997 to 2016, the percentage of U.S. households with desktop or laptop computers more than doubled.[79] From 2000 to 2019, the

74. *See Bureau of Economics Biographies*, Fed. Trade Comm'n, https://www.ftc.gov/about-ftc/bureaus-offices/bureau-economics/biographies (last visited May 19, 2021).

75. As of May 2019, there were only five technologists at the FTC. *See* Memorandum from the Comm. on Energy & Commerce Staff to the Subcomm. on Consumer Prot. & Commerce Members and Staff 4 (May 8, 2019), https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/FTC%20Oversight%20Memo%20050319.pdf. In May 2021, an FTC official confirmed that the number of technologists on staff is fewer than ten. Notes of conversation on file with authors.

76. 16 C.F.R. § 4.1(b)(1)(i).

77. Brian Fung, *The FTC Was Built 100 Years Ago to Fight Monopolists. Now, It's Washington's Most Powerful Technology Cop*, WASH. POST (Sept. 25, 2014, 11:30 AM), https://www.washingtonpost.com/news/the-switch/wp/2014/09/25/the-ftc-was-built-100-years-ago-to-fight-monopolists-now-its-washingtons-most-powerful-technology-cop/ (quoting Geoffrey Manne, executive director of the International Center for Law and Economics).

78. *See generally* McSweeny, *supra* note 50 (detailing FTC enforcement actions in consumer protection against the backdrop of increasing technological complexity).

79. Laptop and desktop computer ownership increased from 36.6% in 1997 to 77% in 2016. ERIC C. NEWBURGER, U.S. CENSUS BUREAU, COMPUTER USE IN THE UNITED STATES: OCTOBER 1997, at 1 (1999), https://www.census.gov/content/dam/Census/library/publications/1999/demo/p20-522.pdf; CAMILLE RYAN, U.S. CENSUS BUREAU, COMPUTER AND INTERNET USE IN THE UNITED STATES: 2016, at 2 (2018), https://www.census.gov

percentage of U.S. adults who used the internet went from fifty-two percent to ninety percent.[80] The iPhone was not even introduced until 2007,[81] with the App Store following close behind it, and yet today there are almost two million apps available for download.[82] E-commerce has simultaneously ballooned over the past two decades.[83]

Today, technically complex subject matter is often at the center of the agency's investigations and proceedings. For example, the 2019 Facebook complaint discussed Facebook's implementation of facial recognition technology;[84] the 2019 Google/YouTube complaint discussed behavioral advertising;[85] the 2019 Equifax complaint discussed critical security vulnerabilities and reasonable patch management policies and procedures;[86] and the 2018 Uber complaint discussed the company's use of real-time precise geolocation data.[87]

As the role of technology in FTC investigations and enforcement has expanded, the agency has struggled to adjust accordingly, forcing the few

/content/dam/Census/library/publications/2018/acs/ACS-39.pdf. In 2016, eighty-nine percent of households had a smartphone or computer. RYAN, *supra* note 79, at 1.

80. *Internet/Broadband Fact Sheet*, PEW RESEARCH CTR. (June 12, 2019), https://www.pewresearch.org/internet/fact-sheet/internet-broadband/.

81. Lisa Eadicicco, *This Is Why the iPhone Upended the Tech Industry*, TIME (June 29, 2017, 7:00 AM), https://time.com/4837176/iphone-10th-anniversary/.

82. Sam Costello, *How Many Apps Are in the App Store?*, LIFEWIRE, https://www.lifewire.com/how-many-apps-in-app-store-2000252 (last updated Feb. 24, 2020).

83. U.S. retail e-commerce sales were estimated at $5.3 billion in the fourth quarter of 1999, when the U.S. Census Bureau first began reporting e-commerce statistics, representing 0.64% of total retail sales. Press Release, U.S. Census Bureau, Retail E-Commerce Sales for the Fourth Quarter 1999 Reach $5.3 Billion, Census Bureau Reports (Mar. 2, 2000), https://www2.census.gov/retail/releases/historical/ecomm/99q4.pdf. By the first quarter of 2020, retail e-commerce sales had ballooned to $160.3 billion, representing 11.8% of total retail sales. Press Release, U.S. Census Bureau, Quarterly Retail E-Commerce Sales: 1st Quarter 2020 (May 19, 2020), https://www2.census.gov/retail/releases/historical/ecomm/20q1.pdf.

84. Complaint for Civil Penalties, Injunction, and Other Relief at 6, 39–42, United States v. Facebook, Inc., No. 19-cv-2184 (D.D.C. July 14, 2019), https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_complaint_filed_7-24-19.pdf.

85. Complaint for Permanent Injunction, Civil Penalties, and Other Equitable Relief at 4, 7–9, Fed. Trade Comm'n v. Google LLC, No. 1:19-cv-2642 (D.D.C. Sept. 6, 2019), https://www.ftc.gov/system/files/documents/cases/172_3083_youtube_revised_complaint.pdf.

86. Complaint for Permanent Injunction and Other Relief at 6, 8–14, Fed. Trade Comm'n v. Equifax Inc., No. 1:19-mi-99999-UNA (N.D. Ga. July 22, 2019), https://www.ftc.gov/system/files/documents/cases/172_3203_equifax_complaint_7-22-19.pdf.

87. Complaint at 2, Uber Technologies, Inc., No. C-4662 (Fed. Trade Comm'n Oct. 26, 2018), https://www.ftc.gov/system/files/documents/cases/152_3054_c-4662_uber_technologies_revised_complaint.pdf.

available technologists to consult on an outsized portion of agency matters.[88] Our personal experience bears this out. As technologists for the FTC, we were asked to consult with attorneys working on virtually every case that came before the Division of Privacy and Identity Protection, as well as a number of cases originating in other divisions. In interviews with other former FTC technologists, we heard similar accounts. This means that our potential list of conflicts is much longer than non-technologists who work for the FTC for the same length of time. Nearly every matter involving technology during our tenure crossed our desks, even if many of those interactions were fleeting and insubstantial. Still, our list of potential conflicts encompasses nearly everything involving complex information technology during our employment.

The general dearth of technical experts at the FTC reflects the agency's dearth of staff more broadly. Much of the scrutiny the agency exacts on technology companies is facilitated by staff working on privacy and data security, of which the FTC has only about forty.[89] In contrast, the United Kingdom has more than five hundred people working in its Information Commissioner's office,[90] and Ireland's Data Protection Commissioner has over 130 employees.[91] As far as technologists are concerned, while the FTC has between five and nine technologists,[92] Germany—a country with one-fourth the population of the United States—has 101 technology specialists working with its data protection authorities.[93] While such a high number is unusual, other European countries nevertheless have drastically more technologists than the United States; Spain has thirty-six, France has twenty-eight, and the United Kingdom has twenty-two.[94]

The dearth of FTC technologists is also evident in comparison to the large population of economists employed by the FTC. The FTC's website currently lists approximately 80 staff in the Bureau of Economics.[95] This list does not

88. This has been our experience, as well as the experience of several people we interviewed. Contact authors for information on interviews.

89. Harper Neidig, *FTC Says It Only Has 40 Employees Overseeing Privacy and Data Security*, THE HILL (Apr. 3, 2019, 11:01 AM), https://thehill.com/policy/technology/437133-ftc-says-it-only-has-40-employees-overseeing-privacy-and-data-security.

90. *History of the ICO*, INFO. COMM'R'S OFFICE, https://ico.org.uk/about-the-ico/our-information/history-of-the-ico/ (last visited Aug. 23, 2020).

91. Peter Hamilton, *Data Commissioner to Look for More Staff and Funding*, IRISH TIMES (Mar. 7, 2019, 1:50 PM), https://www.irishtimes.com/business/technology/data-commissioner-to-look-for-more-staff-and-funding-1.3817791.

92. *See* Breland, *supra* note 71.

93. JOHNNY RYAN, BRAVE, EUROPE'S GOVERNMENTS ARE FAILING THE GDPR 4 (2020), https://brave.com/wp-content/uploads/2020/04/Brave-2020-DPA-Report.pdf.

94. *Id.*

95. *See Bureau of Economics Biographies*, *supra* note 74.

include economists who serve in other roles, such as staff advisors for Commissioners.[96] With dozens of economists and supporting analysts on staff, it is neither necessary nor feasible to ask any individual economist to take on such a broad portfolio of matters that might serve as a future potential conflict of interest.

D. LENGTHY AND BROAD CONSENT DECREES

Another possible contributor to the FTC's broad application of conflicts rules for technologists is the agency's practice of establishing broad, twenty-year settlements with parties presumed to be in violation of § 5 of the FTC Act.[97] This would not necessarily pose a problem if the FTC understood that the "proceeding or investigation" in a conflict of interest analysis under § 4.1(b) of the agency's rules should be the specific facts that gave rise to the twenty-year settlement. But if the rules are instead read broadly—too broadly in our view—to encompass "this company and privacy" or "this company and security," the twenty-year term serves as a two-decades-long restraint on future work for former employees. In combination with the fact that companies—especially technology companies—are bigger and more horizontally diversified than they were in the past,[98] broad and lengthy consent decrees dramatically limit the ability of former FTC staff to work on issues related to technology companies for a period that may cover half a person's professional career.

The FTC has existing consent decrees that will endure many years into the future with a large number of major companies. For example, from past cases, the agency has settlement provisions that will persist with Facebook until

96. *See* FED. TRADE COMM'N, FEDERAL TRADE COMMISSION ORGANIZATION DIRECTORY 2, https://www.ftc.gov/system/files/attachments/contact-federal-trade-commission/ftc_org_directory_8-8-2019.pdf (last updated Aug. 8, 2019) (listing an "Economic Advisor" for Chairman Joseph J. Simons).

97. *See Legislative Hearing on 17 FTC Bills: Hearing Before the Subcomm. on Commerce, Mfg. & Trade of the H. Comm. on Energy & Commerce*, 114th Cong. 5 (2016) (statement of David C. Vladeck, Professor, Georgetown University Law Center), https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/05.24.16_Testimony_Vladeck-CMT-LegHrg-17-FTC-Bills-20160524.pdf ("[T]he Commission has for decades generally insisted on twenty year [*sic*] orders."); *id.* at 6 ("[M]ost [data security cases] were resolved with twenty-year consent decrees."); Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 613–14 (2014) (citing twenty years as a common duration for FTC's privacy and security audits, while also noting variation among the orders); Woodrow Hartzog & Daniel J. Solove, *The Scope and Potential of FTC Data Protection*, 83 GEO. WASH. L. REV. 2230, 2297 (2015) ("While the FTC does not enter into a twenty-year consent order with every company it files a privacy-related complaint against, this burdensome timescale is the most common duration for such agreements.").

98. *See* discussion in *supra* Section III.C.

2039,[99] with Apple until 2034,[100] with Google until 2031,[101] with Google/YouTube until 2029,[102] with Twitter until 2030,[103] and with PayPal until 2038.[104]

The consent decrees often include provisions that require special behavior, oversight, or reporting with respect to a broad range of activities. For example, consent decrees negotiated as part of privacy and data security cases commonly require parties to commit to not misrepresent their privacy or security practices,[105] obtain express consent from consumers with respect to certain data practices,[106] adopt privacy or security programs incorporating certain specific practices,[107] produce regular privacy or security reports that meet

99. Stipulated Order for Civil Penalty, Monetary Judgement, and Injunctive Relief at Attachment A at 20, United States v. Facebook, Inc., No. 19-cv-2184 (D.D.C. July 24, 2019), https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf [hereinafter "FTC Facebook Order 2019"] ("This Order will terminate 20 years from the date of its issuance, or 20 years from the most recent date that the United States of the Commission files a complaint . . . .").

100. Decision and Order at 6, Apple Inc., No. C-4444 (Fed. Trade Comm'n Mar. 25, 2014), https://www.ftc.gov/system/files/documents/cases/140327appledo.pdf [hereinafter "FTC Apple Order 2014"] ("This order will terminate on March 25, 2034, or twenty (20) years from the most recent date that the United States or the Federal Trade Commission files a complaint . . . .").

101. Agreement Containing Consent Order at 7, Google Inc., No. 102316 (Fed. Trade Comm'n 2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/03/110330googlebuzzagreeorder.pdf [hereinafter "FTC Google Order 2011"] ("This order will terminate twenty (20) years from the date of its issuance, or twenty (20) years from the most recent date that the United States or the Commission files a complaint . . . .").

102. Stipulated Order for Permanent Injunction and Civil Penalty Judgement at 16, Fed. Trade Comm'n v. Google LLC, No. 1:19-cv-02642 (D.D.C. Sept. 4, 2019), https://www.ftc.gov/system/files/documents/cases/172_3083_youtube_coppa_consent_order.pdf [hereinafter "FTC Google/YouTube Order 2019"] ("For ten (10) years after entry of this Order, each Defendant must submit a compliance notice, sworn under penalty of perjury, within fourteen (14) days of any change in . . . .").

103. Agreement Containing Consent Order at 6, Twitter, Inc., No. 0923093 (Fed. Trade Comm'n 2010), https://www.ftc.gov/sites/default/files/documents/cases/2010/06/100624twitteragree.pdf [hereinafter "FTC Twitter Order 2010"] ("This order will terminate twenty (20) years from the date of its issuance, or twenty (20) years from the most recent date that the United States or the Commission files a complaint . . . .").

104. Decision and Order at 7, Paypal, Inc., No. C-4651 (Fed. Trade Comm'n May 23, 2018), https://www.ftc.gov/system/files/documents/cases/1623102-c4651_paypal_venmo_decision_and_order_final_5-24-18.pdf [hereinafter "FTC PayPal Order 2018"] ("Respondent must create certain records for 20 years after the issuance date of the Order.").

105. *See, e.g.*, FTC Facebook Order 2019, *supra* note 99, at 5; FTC PayPal Order 2018, *supra* note 104, at 3; FTC Google Order 2011, *supra* note 101, at 3–4; FTC Twitter Order 2010, *supra* note 103, at 3.

106. *See, e.g.*, FTC Facebook Order 2019, *supra* note 99, at 5–6; FTC Google Order 2011, *supra* note 101, at 4.

107. *See, e.g.*, FTC Facebook Order 2019, *supra* note 99, at 6–12; FTC Google Order 2011, *supra* note 101, at 4–5; FTC Twitter Order 2010, *supra* note 103, at 3–4.

outlined standards,[108] and make certain documents available to the FTC upon request.[109]

Because the term of the agreements is long and the scope broad, former employees may find that if they worked on or saw documents related to an investigation of a company that later settled with the FTC, future work relating generally to the data practices of that same company is then essentially off-limits for the lengthy term of the agreement. Even investigations into products or services that *did not yet exist* at the time can then be construed as the "same proceeding or investigation" under the agency's rules restricting post-employment activities.[110]

E. RISK-AVERSE AGENCY CULTURE

When we interviewed former FTC employees, they generally agreed that another cause of the agency's broad application of post-employment conflicts rules is a cultural inclination toward risk-aversion at the agency.[111] In particular, interviewees stated that there is a widespread concern about heavy congressional criticism within the agency.[112] This is viewed as a motivating factor for a number of agency considerations. Many interviewees stated a belief that the agency's extreme caution harkens back to the 1970s when, in what is known as "KidVid," the agency attempted to ban television ads for junk food directed at children—a move perceived by a congressional majority as regulatory overreach.[113] In response, Congress limited the agency's authority

108. *See, e.g.*, FTC Facebook Order 2019, *supra* note 99, at 12–14; FTC PayPal Order 2018, *supra* note 104, at 5–6; FTC Google Order 2011, *supra* note 101, at 5–6; FTC Twitter Order 2010, *supra* note 103, at 4–5.

109. *See, e.g.*, FTC Facebook Order 2019, *supra* note 99, at 20; FTC PayPal Order 2018, *supra* note 104, at 8; FTC Google Order 2011, *supra* note 101, at 6; FTC Twitter Order 2010, *supra* note 103, at 5–6.

110. 16 C.F.R. § 4.1(b)(1)(i).

111. Interviews, *supra* note 88; *see also* Nicholas Confessore & Cecilia Kang, *Facebook Data Scandals Stoke Criticism That a Privacy Watchdog Too Rarely Bites*, N.Y. TIMES (Dec. 30, 2018), https://www.nytimes.com/2018/12/30/technology/facebook-data-privacy-ftc.html ("In more than 40 interviews, former and current F.T.C. officials, lawmakers, Capitol Hill staff members, and consumer advocates said that as evidence of abuses has piled up against tech companies, the F.T.C. has been too cautious.").

112. Interviews, *supra* note 88.

113. *See* CHRIS JAY HOOFNAGLE, FEDERAL TRADE COMMISSION PRIVACY LAW AND POLICY 60–66 (2016) (describing the KidVid controversy, the ensuing fallout, and the impact on the FTC's enforcement approach); Confessore & Kang, *supra* note 111 ("The F.T.C. is haunted, for example, by a clash with Congress in the 1980s over an attempt by the agency to ban television ads for junk food directed at children, known as 'KidVid.' . . . Fears that Congress could again cripple the F.T.C. have made some career lawyers reluctant to take on politically sensitive cases, according to current and former employees, speaking about their

and withdrew its funding.[114] Many believe that the agency continues to tread lightly today out of a lingering fear of congressional backlash, an assessment echoed by our interviewees. Applying this approach to conflicts questions, the agency may reasonably calculate that there are few or no downsides to OGC rejecting a former employee's clearance request.

In contrast, granting a former employee's clearance request—especially when it concerns a major company or highly visible matter—could provide fodder for a company under the scrutiny of the FTC to attempt to drum up criticism of the agency. This is not an unfounded concern; in response to unwanted FTC investigation, companies have attempted all manner of interference strategies throughout the agency's history. For example, in 1918 when the FTC issued a report documenting the predatory and collusive practices of meatpackers and calling for the nationalization of certain components of the industry, the agency was roundly attacked.[115] The U.S. Chamber of Commerce and the New York Times Editorial Board called for the agency to be "cured of its present bolshevist and propagandist tendencies,"[116] and were echoed by Senator James Watson when he specifically targeted the FTC's Chicago field office as a "spawning ground of sovietism."[117] In response, the agency investigated, cleared of wrongdoing, but ultimately still fired eleven of the employees who worked on the report, and Congress removed the agency's oversight of meatpackers, awarding this jurisdiction

experiences during the Trump and Obama administrations."). In one memorable example of a culture of severe sensitivity to congressional censure at the agency, an interviewee described briefing their superiors on research that websites were using JavaScript code that could surreptitiously dig through a user's browser and access the sites they had visited. (Please contact authors for information on interviews.) The most heavily trafficked site that was engaging in that practice belonged to a pornography website. *Id.* The interviewee was informed that the agency would not investigate the pornography company because the FTC did not want to run the risk of being perceived as "protecting the privacy of people who watch pornography." *Id.* While no other interviewees provided similarly colorful examples to illustrate the point, this example is representative of the risk-adverse culture described by the other former FTC employees.

114. Hoofnagle, *supra* note 113, at 65 (describing the FTC Improvement Act of 1980, which passed in response to the KidVid controversy, implemented a Congressional veto of Agency action, limited the Agency's rule-making authority, and temporarily expunged funding).

115. Luke Herrine, *The Folklore of Unfairness*, 96 N.Y.U.L. REV.431, 467 (2021). The practices described in the report also provided the basis for a subsequent criminal suit by the Attorney General.

116. Editorial, *The Trade Commission*, N.Y. TIMES, Sept. 3, 1918, at 10, *available at* https://timesmachine.nytimes.com/timesmachine/1918/09/03/97024087.pdf?pdf_redirect=true&ip=0.

117. Paul A. Pautler, *A Brief History of the FTC's Bureau of Economics: Reports, Mergers, and Information Regulation*, 46 REV. INDUS. ORG. 59, 64 n.13 (2015).

instead to the more industry-friendly Department of Agriculture.[118] Sixty years later in KidVid, when the agency considered children's advertising rules, advertisers devoted the equivalent of one-fourth of the agency's budget at the time to lobbying and public relations efforts against the rules, while advertising trade associations petitioned the FTC to compel Chair Michael Perschuk to recuse himself based on his prior statements about the regulation of children's advertising.[119] When Perschuk initially refused, the advertisers sued, won, and lost on appeal; nevertheless, Perschuk eventually recused himself voluntarily to shield the rulemaking from further corruption accusations.[120] These episodes provide support for fears of corporate retaliation: when it comes to companies attempting to avoid profit-narrowing regulation, some will not hesitate to work the referees, and many of those will be rewarded with the calls they sought.

Indeed, we know of at least two instances when the agency acted on outside claims of conflict or bias that seemed exceptionally weak on their face, and for which it is difficult to explain the agency's responses as anything other than extreme risk aversion. One former technologist we interviewed publicly criticized a large technology company prior to his employment by the agency.[121] When the company filed a complaint with the FTC regarding the employee's participation in investigations of the company, the FTC removed the employee from the investigation and precluded him from working on any investigation of that company for the rest of his employment at the FTC. In another case, a large technology company complained to the FTC when a member of an FTC technologist's Ph.D. dissertation committee filed a public request for the agency to investigate that company. The request was based entirely on publicly available information but, because the company complained that the employee was somehow conflicted, the FTC prohibited

118. *Id.* (noting that the employees were "cleared of wrongdoing" and that their firing was "presumably to placate Senator Watson"); Hoofnagle, *supra* note 113, at 24–25 (recounting the episode and characterizing the Department of Agriculture as "friendlier" to the meatpackers than the FTC).

119. Herrine, *supra* note 115, at 503 ("With General Mills and Bristol-Myers in the lead and "Washington super-lobbyist Tommy Boggs" coordinating (and rumors of the tobacco lobby contributing substantially), a "war chest" of $30 million was raised to "Stop the FTC" and KidVid in particular."); *id.* at 506–07 (detailing The Association of National Advertisers, Inc., the American Association of Advertising Agencies, the American Advertising Federation, and the Toy Manufacturers of America, Inc.'s demands that Perschuk recuse himself for conflict of interest due to his "public statements concerning regulation of children's advertising that demonstrated prejudgment of specific factual issues sufficient to preclude his ability to serve as an impartial arbiter") (citing Ass'n of Nat'l Advertisers, Inc. v. FTC, 627 F.2d 1151, 1155 (D.C. Cir. 1979)).

120. Herrine, *supra* note 115, at 503.

121. Contact authors for more information.

the employee from working on any investigations of that company. As a result, an important investigation of the company was conducted without the support of any FTC technologist for several months.

The agency's attempts to inoculate itself from charges of bias by industry are likely to fail because opportunistic companies raise such charges even when there is no reasonable basis for them. Nevertheless, a deep-seated agency culture of prudence—and a history of successful corporate interference—leads the agency to reflexively shy away from even the suggestion of possible conflict.

F. POSSIBLE POLITICAL CONFLICT BETWEEN FTC AND STATE ATTORNEYS GENERAL

It is also possible that perceived political conflict may contribute to the overly broad application of post-employment conflict restrictions to FTC technologists. To be clear, the FTC often works closely with state attorneys general, including in investigations into the practices of technology companies.[122] For example, in 2012, the FTC and dozens of state attorneys general coordinated on cases brought against Google for its privacy policy practices.[123] Even though the state enforcers pressed arguably more aggressive theories than the FTC pursued in its investigation, FTC Commissioner Julie Brill praised the settlement extracted by the states.[124]

Our interviewees downplayed the possibility of rivalry between the FTC and the states as playing a significant role in the FTC's application of post-employment restrictions. Many of our respondents thought it unlikely that perceived political conflict plays a meaningful role driving the FTC's broad application of post-employment conflict rules. Nevertheless, this is a possibility worth exploring.

Although the state attorneys general and the FTC frequently are well aligned, their respective goals and approaches sometimes diverge. A 2013

122. Paul M. Schwartz, *The Value of Privacy Federalism, in* SOCIAL DIMENSIONS OF PRIVACY: INTERDISCIPLINARY PERSPECTIVES 324 (Beate Roessler & Dorota Mokrosinska eds., 2015) ("When Congress enacts privacy law, it generally allows the states space for further action."); Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747, 791–94 (2016) ("Attorneys general have enjoyed a synergistic relationship with federal agencies working on privacy and data security issues."); Bilyana Petkova, *The Safeguards of Privacy Federalism*, 20 LEWIS & CLARK L. REV. 595, 621–22 (2016) ("[T]he state attoneys general have not only coordinated their actions horizontally but have also joined efforts with the FTC.").

123. Citron, *supra* note 122, at 793.

124. *Id.*; Letter from Twenty-three Att'ys Gen. to Larry Page, Chief Exec. Officer, Google, Inc. (Feb. 22, 2012), https://epic.org/privacy/google/20120222-Google-Privacy-Policy-Final.pdf.

investigation of Google, regarding the company bypassing privacy settings in the Safari browser, led the FTC to enter a settlement with Google that required no limits on Google's future behavior.[125] State attorneys general declined the FTC's invitation to join the consent decree and continued to press a parallel case that led, arguably, to tougher restrictions on Google's conduct.[126]

There are reasons to believe that some amount of competitiveness exists between these entities. In many ways, the FTC has become the *de facto* privacy and technology regulator in the United States, even though, outside of sectoral laws like the Children's Online Privacy Protection Act (COPPA) and the Fair Credit Reporting Act (FCRA), there is currently no comprehensive federal privacy law.[127] The FTC benefits from the appearance that it is the primary and most powerful enforcer of fair trade practices in the United States because, when a regulator has a reputation as being toothless, companies subject to their jurisdiction have no incentive to comply with the relevant rules. As a result, the FTC sometimes competes with state attorneys general when enforcing high-profile cases. When state enforcement agencies investigate and impose stronger perceived penalties on companies that the FTC has already investigated, charged, and settled, this could undermine the FTC's status as supreme enforcer.[128]

The experiences of one interviewee who worked on consumer protection investigations with a state attorney general's office speak to the occasional tensions between the FTC and state attorneys general. The interviewee hypothesized that in certain, high-profile cases, the FTC's willingness to allow the former employee to consult on the state attorney general's case was hindered by the agency's interest in public credit for tackling certain cases. The interviewee hypothesized that the agency's desire for public credit was

125. Citron, *supra* note 122, at 770 (citing 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/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented).

126. *Id.*

127. Solove & Hartzog, *supra* note 97, at 600–08.

128. *See* Justin Brookman, *State Attorneys General: Evading Privacy Settings Is Illegal*, CTR. FOR DEMOCRACY & TECH. (Nov. 20, 2013), https://cdt.org/insights/state-attorneys-general-evading-privacy-settings-is-illegal/ (pointing out that the 2013 settlement by state attorneys general with Google was "considerably more expansive than the FTC's," and arguing that "it's heartening to see states increasingly take action to protect consumer privacy"); Citron, *supra* note 122, at 756 n.42 ("In important areas, [state attorneys general (AG)] have set privacy policy in the absence of federal norms; in others, they have pressed the FTC to offer greater privacy protections to consumers than those afforded by federal agencies. In the near future, there may be more aggressive state AG privacy and data security enforcement than enforcement activity at the federal level.").

responsible for the friction in that particular case because the interviewee had not encountered similar problems when working with FTC officials on previous lower-level cases. The interviewee explained that in response to a request for clearance to work with state AGs on a high-profile matter, the FTC denied clearance for the interviewee unless the interviewee was willing to work as an unpaid FTC employee and allow the FTC to mediate their recommendations to the state agencies.[129] Indeed, there is good reason for FTC staff to seek public credit for its enforcement efforts. In recent years, the FTC has been lambasted by a range of critics for its failure to take strong, decisive action to rein in unfair and deceptive trade practices.[130] Even the agency's record-breaking five-billion-dollar settlement with Facebook drew widespread criticism that it was simply not enough.[131]

Some critics have gone so far as to argue that what they consider to be the agency's too-weak enforcement efforts provide support to further constrain

129. Email from Alternate Designated Agency Ethics Official, Office of the General Counsel, Federal Trade Commission, to one of the authors (Mar. 07, 2019, 07:54 PST) (on file with authors).

130. *See, e.g.*, *Hearing on Oversight of the Federal Trade Commission: Strengthening Protections for Americans' Privacy and Data Security Before House of Representatives Subcommittee on Consumer Protection and Commerce of the House Committee on Energy and Commerce*, 116th Cong. 1 (May 8, 2019) (opening statement of Frank Pallone, Jr., Chairman, Comm. on Energy & Commerce), https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/0508%20FP%20FTC%20Oversight%20Hrg%20Opening%20Remarks.pdf (claiming the FTC "can dodo[es] little more than give a slap on the wrist to companies the first time they violate the law"); Emily Birnbaum, *GOP Senator Scolds FTC for 'Toothless' Response to Privacy Scandals*, THE HILL (Mar. 11, 2019, 1:41 PM), https://thehill.com/policy/technology/433514-gop-senator-ftc-response-to-privacy-scandals-has-been-toothless; Peter Maass, *Your FTC Privacy Watchdogs: Low-Tech, Defensive, Toothless*, WIRED (June 28, 2012, 6:30 AM), https://www.wired.com/2012/06/ftc-fail/ (calling the FTC "low-tech, defensive, [and] toothless").

131. *See*, *e.g.*, Devin Coldewey, *9 Reasons the Facebook FTC Settlement Is a Joke*, TECHCRUNCH (July 24, 2019, 8:01 PM), https://techcrunch.com/2019/07/24/9-reasons-the-facebook-ftc-settlement-is-a-joke/; Editorial Board, Opinion, *A $5 Billion Fine for Facebook Won't Fix Privacy*, N.Y. TIMES (July 25, 2019), https://www.nytimes.com/2019/07/25/opinion/facebook-fine-5-billion.html; Nilay Patel, *Facebook's $5 Billion FTC Fine Is an Embarrassing Joke*, THE VERGE (July 12, 2019, 9:05 PM), https://www.theverge.com/2019/7/12/20692524/facebook-five-billion-ftc-fine-embarrassing-joke; Adam Schwartz, *The FTC-Facebook Settlement Does Too Little to Protect Your Privacy*, ELEC. FRONTIER FOUND. (July 24, 2019), https://www.eff.org/deeplinks/2019/07/ftc-facebook-settlement-does-too-little-protect-your-privacy; Siva Vaidhyanathan, *Billion-Dollar Fines Can't Stop Google and Facebook. That's Peanuts for Them*, GUARDIAN (July 26, 2019, 6:00 AM), https://www.theguardian.com/commentisfree/2019/jul/26/google-facebook-regulation-ftc-settlement; Press Release, H. Comm. on Energy & Commerce, Pallone Statement on the FTC's Facebook Settlement (July 24, 2019), https://energycommerce.house.gov/newsroom/press-releases/pallone-statement-on-the-ftc-s-facebook-settlement ("While $5 billion is a record fine for the FTC, monetary damages are not enough.").

the agency's authority. Indeed, a number of privacy advocates have called for Congress to create a new data protection authority to counteract the FTC's failures and hold technology companies accountable.[132] Senator Gillibrand,[133] Senator Brown,[134] and Representatives Lofgren and Eshoo[135] heeded that call by offering legislation that would establish a new data protection agency in the United States.

The FTC could be concerned that if state attorneys general were to frequently pursue additional enforcement action against companies for practices that have already been the subject of FTC settlements, companies would have less of an incentive to agree to truly burdensome conditions when they are brought to the settlement negotiation table over alleged violations. It is not unusual for the FTC to release any claims it may have against the subjects of its enforcement actions as part of the negotiated settlement.[136] If a company

132. *See, e.g.*, Caitriona Fitzgerald & Mary Stone Ross, *Now Is the Time for a US Data Protection Agency*, THE HILL (Feb. 21, 2020, 9:30 AM), https://thehill.com/blogs/congress-blog/politics/483997-now-is-the-time-for-a-us-data-protection-agency ("Congress needs to create a Data Protection Agency because the Federal Trade Commission is failing to protect privacy."); PRIVACY & DIG. RIGHTS FOR ALL COAL., THE TIME IS NOW: A FRAMEWORK FOR COMPREHENSIVE PRIVACY PROTECTION AND DIGITAL RIGHTS IN THE UNITED STATES, https://www.citizen.org/wp-content/uploads/migration/privacy-and-digital-rights-for-all-framework.pdf; *The U.S Urgently Needs a Data Protection Agency*, ELEC. PRIVACY INFO. CTR., https://epic.org/dpa/; *see also* Natasha Singer, *The Government Protects Our Food and Cars. Why Not Our Data?*, N.Y. TIMES (Nov. 2, 2019), https://www.nytimes.com/2019/11/02/sunday-review/data-protection-privacy.html (describing critiques of the FTC and proposals for a new data protection agency).

133. Press Release, Kirsten Gillibrand: U.S. Sen. for N.Y., Confronting a Data Privacy Crisis, Gillibrand Announces Landmark Legislation to Create a Data Protection Agency (Feb. 13, 2020), https://www.gillibrand.senate.gov/news/press/release/confronting-a-data-privacy-crisis-gillibrand-announces-landmark-legislation-to-create-a-data-protection-agency.

134. Press Release, Sherrod Brown: U.S. Sen. for Ohio, Brown Releases New Proposal That Would Protect Consumers' Privacy from Bad Actors (June 18, 2020), https://www.brown.senate.gov/newsroom/press/release/brown-proposal-protect-consumers-privacy.

135. Press Release, Congresswoman Anna G. Eshoo, Eshoo & Lofgren Introduce the Online Privacy Act (Nov. 5, 2019), https://eshoo.house.gov/media/press-releases/eshoo-lofgren-introduce-online-privacy-act.

136. *See, e.g.*, FTC Facebook Order 2019, *supra* note 99; [Proposed] Stipulated Revised Order for Permanent Injunction and Equitable Monetary Relief at 17, Fed. Trade Comm'n v. Cephalon, Inc., No. 2:08-cv-2141-MSG (E.D. Pa. Feb. 19, 2019), https://www.ftc.gov/system/files/documents/cases/teva_proposed_stipulated_revised_order.pdf ("The Commission and the Cephalon Parties stipulate that upon entry of the Revised Order, the Commission and the Cephalon Parties each release the other from any and all claims, causes of actions and demands . . . ."); Stipulation at 2, United States v. Okumus, No. 1:17-cv-00104 (D.D.C. Jan. 17, 2017), https://www.ftc.gov/system/files/documents/cases/170117okumus_stipulation_filed.pdf ("The entry of the Final Judgment in accordance with

caught violating the FTC Act believed it was likely to just be sued again for the same behavior by another enforcer, then the FTC's avowal to release any claims related to the violation would have little value.

IV. IMPLICATIONS FOR AGENCY EFFICACY

As this Article has noted throughout, the broad application of the conflict rules undermines their purpose and the FTC's ability to fulfill its competition and consumer protection mission. The FTC is making it less attractive for technologists to work at the agency by disproportionately limiting the work they are able to do, including when the matters former employees are being precluded from participating in create neither an actual conflict nor the appearance of it. Unwieldy and unpredictable post-employment constraints will make it even less attractive, or frankly feasible, for technologists to work for the FTC than it already is, raising exactly the concerns that Congress has repeatedly noted when revising § 207.[137]

This overbroad application of the FTC's rules also undermines the agency's broader mission of consumer protection by inhibiting other consumer protection actors, such as state attorneys general, from gaining the expertise to adequately seek remedies in areas the FTC itself was unable to obtain. For example, many organizations criticized the five-billion-dollar settlement with Facebook because the settlement includes very little in the way of injunctions to restrict the company's future practices with regards to privacy harm of third-party companies, like Cambridge Analytica.[138] In fact, the final settlement also precludes Facebook, its executives, and its board of directors from being held responsible for "any and all claims" prior to the settlement date.[139] Two FTC Commissioners criticized this point, and one implied the existence of other ongoing investigations into the company that were released

this Stipulation settles, discharges, and releases any and all claims of Plaintiff for civil penalties and equitable relief pursuant to Section 7A(g)(1) of the Clayton Act, 15 U.S.C. § 18a(g)(l) . . . in connection with Defendant's acquisitions of voting securities of Web.com Group, Inc. from 2014 through 2016."); Stipulated Order for Permanent Injunction and Monetary Judgement at 7, Fed. Trade Comm'n v. Hold Billing Services, Ltd., No. 5:98-cv-006292, (W.D. Tex. May 4, 2016), https://www.ftc.gov/system/files/documents/cases/160504holdbillingstip.pdf ("Upon entry of this Stipulated Order, the FTC releases [Defendant] from any and all Claims that it may have stemming from charges to consumers' landline telephone bills through or on behalf of any third-party seller of Enhanced Services.").

137. *Supra* notes 13, 17.

138. *See, e.g.*, *supra* note 131 and sources cited therein.

139. FTC Facebook Order 2019, *supra* note 99, at 1, United States v. Facebook, Inc., No. 19-cv-2184 (D.D.C. July. 24, 2019), https://www.ftc.gov/system/files/documents/cases/182_3109_facebook_order_filed_7-24-19.pdf.

as a part of the settlement.[140] In addition, private plaintiffs already face steep hurdles to getting their privacy violations redressed due to years of judicial hostility toward privacy rights.[141] Making it harder for private plaintiffs to find and retain technology experts will make the already minimal utility of courts to vindicate privacy rights less meaningful still.

Overbroad application even limits the efficacy of the few technologists the agency does employ. In the interviews we conducted, we heard from former employees who had recused themselves from working on certain cases for fear of being broadly precluded from ever working on a related matter once they left the agency, one citing market consolidation as the justification. As such, concerns of post-employment conflict checks are likely chilling the freedom that current FTC employees have to work on certain investigations while at the agency. This corrodes the agency's effectiveness given how few technologists it employs already. With the agency's current volume of technologists, if even one technologist declines to work on cases involving Facebook or Google, for example, the agency loses a significant fraction of its available technological expertise—expertise that it cannot afford to lose.

The FTC is taking the population of employees that it has the hardest time recruiting and making it disproportionately even less attractive for them to work there. Technologists are subject to potential conflicts far more broadly than employees in other disciplines, even though technologists are much

140. *See* OFFICE OF COMM'R ROHIT CHOPRA, FED. TRADE COMM'N, COMM'N FILE NO. 1823109, DISSENTING STATEMENT OF COMMISSIONER ROHIT CHOPRA: *IN RE* FACEBOOK, INC. 17–18, (2019), https://www.ftc.gov/system/files/documents/public_statements/1536911/chopra_dissenting_statement_on_facebook_7-24-19.pdf ("This means that the proposed release not only shields Facebook from 'known' (an undefined term) Section 5 claims, but also 'known' claims under COPPA and other statutes. Given persistent questions about Facebook's compliance with these statutes, the Commission should be transparent about which claims are being released—even if they are being released because they are seen as lacking viability."); OFFICE OF COMM'R REBECCA KELLY SLAUGHTER, FED. TRADE COMM'N, DISSENTING STATEMENT OF COMMISSIONER REBECCA KELLY SLAUGHTER: IN THE MATTER OF FTC VS. FACEBOOK 14 (2019), https://www.ftc.gov/system/files/documents/public_statements/1536918/182_3109_slaughter_statement_on_facebook_7-24-19.pdf (objecting "strenuously" to the settlement's liability exculpation for Facebook's executives and calling the scope of the liability release "unjustified by our investigation and unsupported by either precedent or sound public policy").

141. Justin Brookman, *Protecting Privacy in an Era of Weakening Regulation*, 9 HARV. L. & POL'Y REV. 355, 356–65 (2015) (describing how courts have made it more and more difficult for privacy plaintiffs to receive redress through artificially narrow definitions of Article III standing and injury, and an expansive approach to First Amendment rights and the rights of corporations); Julie E. Cohen, *Information Privacy Litigation as Bellwether for Institutional Change,* 66 DEPAUL L. REV. 535, 575–77 (2017) (describing courts' response to privacy litigants as "busily constructing classes of consumers who lack remedies before the law").

harder for the agency to locate and retain than attorneys and economists.[142] An entry-level engineer's compensation at Facebook with no post-collegiate work experience can reach $166,000 and up to $189,000 at Google in 2019, while senior staff roles at the FTC can only make up to around $170,000.[143] This difference in potential salary in conjunction with the broad and opaque application of the conflict rules render it even less appealing for technologists to work at the FTC. Not only are the conflicts rules making it harder for the agency to recruit and retain the population of employees it needs most,[144] they seem fairly ineffective at reducing the revolving door problems for non-technologist employees and senior leadership.[145]

In almost cruel irony, the lack of competition among the technology companies subject to the FTC's jurisdiction further hampers its ability to enforce antitrust laws. The technology companies that the FTC investigates, like Apple, Amazon, Facebook, and Google, are frequently repeat players.[146]

142. Different factors, such as advance planning and unchanging subject matter, influence why non-technologists are easier for the agency to find and retain. For example, the Bureau of Economics at the FTC was proactive in its creation rather than reactive; that is, it was created all at once with many staff with the objective of changing the agency's focus, as opposed to bit by bit in reaction to subject matter changing beyond the agency's control.

143. Adam Janofsky & Matt Drange, *We Counted the FTC Employees who Moved Over to Tech. Is Reform Needed?*, PROTOCOL (Mar. 9, 2020), https://www.protocol.com/ftc-tech-hawley-revolving-door/; Kif Leswing, *Here's How Big Tech Companies Like Google and Facebook Set Salaries for Software Engineers*, CNBC (June 15, 2019, 9:30 AM), https://www.cnbc.com/2019/06/14/how-much-google-facebook-other-tech-giants-pay-software-engineers.html.

144. *See generally* McSweeny, *supra* note 50.

145. *See generally id.*; *see also* Rick Claypool, *The FTC's Big Tech Revolving Door Problem*, PUB. CITIZEN (May 23, 2019), https://www.citizen.org/article/ftc-big-tech-revolving-door-problem-report.

146. *See, e.g.*, Agreement Containing Consent Order, Facebook, Inc., No. 0923184 (Fed. Trade Comm'n Nov. 29, 2011), https://www.ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookagree.pdf (2011 Facebook consent order); Press Release, Fed. Trade Comm'n, Apple Inc. Will Provide Full Consumer Refunds of At Least $32.5 Million to Settle FTC Complaint It Charged for Kids' In-App Purchases Without Parental Consent (Jan. 15, 2014), https://www.ftc.gov/news-events/press-releases/2014/01/apple-inc-will-provide-full-consumer-refunds-least-325-million (2014 Apple settlement); Press Release, Fed. Trade Comm'n, Google Agrees to Change Its Business Practices to Resolve FTC Competition Concerns in the Markets for Devices Like Smart Phones, Games and Tablets, and in Online Search (Jan. 3, 2013), https://www.ftc.gov/news-events/press-releases/2013/01/google-agrees-change-its-business-practices-resolve-ftc (2013 Google-specific antitrust settlement); Press Release, Fed. Trade Comm'n, Google and YouTube Will Pay Record $170 Million for Alleged Violations of Children's Privacy Law (Sept. 4, 2019), https://www.ftc.gov/news-events/press-releases/2019/09/google-youtube-will-pay-record-170-million-alleged-violations (2019 Google and YouTube settlement); Press Release, Fed. Trade Comm'n, Google Will Pay $22.5 Million to Settle FTC Charges It Misrepresented Privacy Assurances to

The size of these companies and the range of markets they have inserted themselves into makes overlap inevitable. When the FTC prohibits an employee from working on matters related to one technology company, that often means that the employee will be forbidden from working on a whole host of investigations across a wide gamut of sectors.[147] The lack of competition in the technology sector means that the agency's broad enforcement of the conflicts rules will significantly undercut its efforts to fulfil its consumer protection and competition missions.

Meanwhile, the collateral effects of the FTC's overreaction hamper its ability to oversee those companies effectively. The agency simply does not employ enough technologists to be able to sideline them every time a subject or potential subject of investigation files a bad-faith complaint. As of 2019, the

---

Users of Apple's Safari Internet Browser (Aug. 9, 2012), https://www.ftc.gov/news-events/press-releases/2012/08/google-will-pay-225-million-settle-ftc-charges-it-misrepresented (2012 Google settlement); *Facebook, Inc., In the Matter of*, FED. TRADE COMM'N, https://www.ftc.gov/enforcement/cases-proceedings/092-3184/facebook-inc (last updated Apr. 28, 2020) (2019 Facebook settlement); Lesley Fair, *FTC Settlement with Amazon Yields $70 Million for Consumers, Advice for Business*, FED. TRADE COMM'N: BUS. BLOG (May 30, 2017, 12:07 PM), https://www.ftc.gov/news-events/blogs/business-blog/2017/05/ftc-settlement-amazon-yields-70-million-consumers-advice (2017Amazon settlement); Cecilia Kang & David McCabe, *F.T.C. Broadens Review of Tech Giants, Homing in on Their Deals*, N.Y. TIMES (Feb. 11, 2020), https://www.nytimes.com/2020/02/11/technology/ftc-tech-giants-acquisitions.html (2020 Amazon, Apple, Facebook, Alphabet, and Microsoft investigation); *Microsoft Corp.*, FED. TRADE COMM'N, https://www.ftc.gov/enforcement/cases-proceedings/002-3331/microsoft-corporation (last updated May 18, 2001) (2001 Microsoft settlement); Spencer Soper & Ben Brody, *Amazon Probed by U.S. Antitrust Officials over Marketplace,* BLOOMBERG (July 24, 2019, 5:00 AM), https://www.bloomberg.com/news/articles/2019-09-11/amazon-antitrust-probe-ftc-investigators-interview-merchants (2019 Amazon-specific antitrust investigation); Nick Statt, *Facebook Confirms New FTC Antitrust Investigation After Posting Strong Earnings*, THE VERGE (July 24, 2019, 4:27 PM), https://www.theverge.com/2019/7/24/20726371/facebook-ftc-antitrust-earnings-q2-2019-privacy-regulation-mark-zuckerberg (2019 Facebook-specific antitrust investigation).

147. Between the enormous range of sectors Amazon is involved in through its provision of cloud services and the range of sectors that sell products through its site, and the fact that online advertising is overwhelmingly dominated by Facebook and Google, all kinds of competition and consumer protection investigations will necessarily involve these companies. *See*, *e.g.*, Khan, *supra* note 61, at 768–78 (describing how Amazon leverages its delivery infrastructure into outpricing competitors in a range of industries, such as when it eliminated its biggest competitor in diapers and other baby care goods through a carefully orchestrated predatory pricing scheme and ultimate acquisition). Amazon accounted for over a third of online retail sales in the United States last year. Jessica Young, *US Ecommerce Sales Grow 14.9% in 2019*, DIGITAL COM. 360 (Feb. 19, 2020), https://www.digitalcommerce360.com/article/us-ecommerce-sales/. The FTC is also currently undergoing a review of Amazon, Apple, Facebook, Alphabet, and Microsoft's reliance on "killer acquisitions"—i.e., the practice of buying a nascent competitor to neutralize the threat posed by the smaller company's product. Kang & McCabe, *supra* note 146.

FTC only employed five full-time technologists in total, for an agency that oversees digital consumer protection issues for a nation of 330 million people and handles a range of other issues beyond privacy, security, and digital competition.[148] The FTC's lack of sufficient technologists on staff has been a frequent point of criticism by advocates,[149] former[150] and current[151] FTC officials, and Congress,[152] and the agency has acknowledged the deleterious effects of the lack of technologists on its effectiveness.[153] The overly broad application of the conflict rules exacerbates this problem.

V. POLICY RECOMMENDATIONS

We offer policy recommendations to address this problem and help pave the way for the FTC and other federal agencies to increase their technical

148. Memorandum from the Comm. on Energy & Commerce Staff, *supra* note 75.

149. BECKY CHAO, ERIC NULL & CLAIRE PARK, OPEN TECH. INST., ENFORCING A NEW PRIVACY LAW: WHO SHOULD COMPANIES HOLD ACCOUNTABLE? (2019), https://www.newamerica.org/oti/reports/enforcing-new-privacy-law/ (noting the paucity of technologists at the agency and noting that it is "unclear whether the FTC has the technological expertise it needs to enforce privacy laws").

150. McSweeny, *supra* note 50, at 530 (recommending that the FTC "scale[] up its in-house technology and research expertise"); Jessica Rich, *Give the FTC Some Teeth to Guard Our Privacy*, N.Y. TIMES (Aug. 12, 2019), https://www.nytimes.com/2019/08/12/opinion/ftc-privacy-congress.html ("To adequately police privacy in this country, the F.T.C. needs more lawyers, more investigators, more technologists and state-of-the-art tech tools. Otherwise, it will continue to operate on a shoestring, foregoing certain investigations and understaffing others.").

151. *See, e.g.*, OFFICE OF COMM'R ROHIT CHOPRA, FED. TRADE COMM'N, COMM'N FILE NO. P065404, STATEMENT OF COMMISSIONER ROHIT CHOPRA: REGARDING THE REPORT TO CONGRESS ON THE FTC'S USE OF ITS AUTHORITIES TO PROTECT CONSUMER PRIVACY AND SECURITY 4–5 (2020), https://www.ftc.gov/system/files/documents/public_statements/1577067/p065404dpipchoprastatement.pdf.

152. *See, e.g.*, Memorandum from the Comm. on Energy & Commerce Staff, *supra* note 75; *Hearing on "Oversight of the Federal Trade Commission: Strengthening Protections for Americans' Privacy and Data Security" Before the Subcommittee on Consumer Protection and Commerce of the House Committee on Energy and Commerce*, 116th Cong. (2019) (opening statement of Rep. Jan Schakowsky, Chair), https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/2019.5.8.SCHAKOWSKY.%20FTC%20Oversight%20Hearing.CPC__0.pdf (noting a contributing factor to the agency's struggle to conduct meaningful enforcement is the mere five technologists and lack of a Chief Technologist).

153. *The Technology 202: The Government's Top Silicon Valley Watchdog Only Has Five Full-Time Technologists. Now It's Asking Congress for More*, WASH. POST (Apr. 4, 2019, 8:47 AM), https://www.washingtonpost.com/news/powerpost/paloma/the-technology-202/2019/04/04/the-technology-202-the-government-s-top-silicon-valley-watchdog-only-has-five-full-time-technologists-now-it-s-asking-congress-for-more/5ca512661b326b0f7f38f30d/ (discussing a letter from FTC Chairman Joseph Simons to the House Committee on Energy and Commerce "request[ing] funding for 10 to 15 more technologists").

capacity. The FTC has joined Congress and civil society in bemoaning its lack of technical experts, and it must mitigate the obstacles that currently make correcting this problem so difficult. We offer specific suggestions and broader objectives that will help mitigate the current obstacles the agency faces in order to attract and retain technology expertise.

To be clear, we do not mean to diminish the need for conflict of interest laws, nor do we support watering down the efficacy of those laws to prevent corruption or slow the revolving door. We see civil service as an important, if not sacred, calling, and we endorse the strong use of conflicts rules to discourage cynical or opportunistic people from trading on government service for personal gain. In fact, we think in some cases conflict of interest laws may need to be strengthened as there are still a great deal of former employees that "switch sides" and join companies the agency is tasked to oversee.[154]

However, we believe that the FTC-administered rules go far beyond these important goals, especially when applied to technologists.[155] As discussed above, in many cases, former FTC technologists seek simply to work on the same side as the agency in the furtherance of consumer protection.[156] In those situations, we think a reevaluation of priorities is warranted.

First, the FTC should address the current vagueness in determining when different projects comprise either the same "proceeding or investigation" under 16 C.F.R. § 4.1(b) or the same "particular matter" under 18 U.S.C. § 207(a). Under the current formulation of the rule, in making this determination the FTC considers "the extent to which the matters involve the same or related facts, issues, confidential information and parties; the time elapsed; and the continuing existence of an important Federal interest."[157] The FTC could interpret this broad set of factors as permitting it the latitude to determine that "same side" investigations that take place after an FTC settlement complaint has already been brought constitute new and separate "proceeding[s] or investigation[s]." At present, however, the FTC interprets the vagueness of this multi-factor test to apply post-employment restrictions

154. Janofsky & Drange, *supra* note 143.

155. *See* discussion in *supra* Section III.A.

156. *Id.*

157. 16 C.F.R. § 4.1(b)(1) n.1. In setting forth these factors, the FTC refers to an analogous section of the Office of Government Ethic's regulations setting forth the factors considered to determine whether two particular matters are the same under § 207: "the extent to which the matters involve the same basic facts, related issues, the same or related parties, time elapsed, the same confidential information, and the continuing existence of an important Federal interest." 5 C.F.R. § 2641.201(h)(5)(i).

extremely broadly, in a way that we believe ultimately runs counter to the public interest.

Second, the FTC should clarify that whether or not one particular "proceeding or investigation" is the same turns more narrowly on the specific facts of the underlying investigation. The 2012 consent decree with Facebook speaks to this.[158] The consent decree stemmed from an investigation into, among other things, changes to Facebook's privacy policies that made more information about its users visible to the public than before and misled consumers about the amount of information third-party apps could obtain about users.[159] The investigation led to a settlement and twenty-year consent decree that obligated Facebook to create a "comprehensive privacy program" and to report to the FTC for twenty years.[160]

For former FTC officials who worked on the 2012 consent decree, what is the underlying matter that might trigger conflicts review today? We contend that the matter should be closely related to the facts that existed in 2012, which was largely premised on changes to privacy policies in 2009 and 2010 as well as aspects of Facebook's architecture in 2011. In contrast, the FTC seems to take a much broader interpretation, treating the underlying "matter" as "Facebook and privacy." For example, the FTC has prevented at least one of us from working on cases related to Cambridge Analytica, the company that notoriously mined Facebook user data in the 2016 election, by claiming they were too closely related to the 2012 consent decree matter, even though Cambridge Analytica did not even exist in 2011.[161] The FTC allowed another of us to participate in a matter related to Cambridge Analytica but only after a two-week delay that prevented a more meaningful role in the case. A definition of "proceeding or investigation" as expansive as "Facebook and privacy" or

158. Decision and Order, 5–8, In the Matter of Facebook, Inc., Fed. Trade Comm'n (Aug. 10, 2012) (Docket No. C-4365), https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf

159. Press Release, Fed. Trade Comm'n, Facebook Settles FTC Charges that It Deceived Consumers by Failing to Keep Privacy Promises (Nov. 29, 2011), https://www.ftc.gov/news-events/press-releases/2011/11/facebook-settles-ftc-charges-it-deceived-consumers-failing-keep.

160. Decision and Order at 5–8, Facebook, Inc., No. C-4365 (Fed. Trade Comm'n Aug. 10, 2012), https://www.ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf; Press Release, Fed. Trade Comm'n, FTC Approves Final Settlement with Facebook (Aug. 10, 2012), https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook.

161. Cambridge Analytica was founded in 2013. *See* David Ingram, *Factbox: Who Is Cambridge Analytica and What Did It Do?*, REUTERS (Mar. 19, 2018, 10:00 PM), https://www.reuters.com/article/us-facebook-cambridge-analytica-factbox/factbox-who-is-cambridge-analytica-and-what-did-it-do-idUSKBN1GW07F.

"Amazon and predatory pricing" will disqualify the FTC's technologists from working on crucial investigations, even as these companies consistently repeat the same kind of exploitative practices and necessary technological expertise becomes harder and harder for enforcers to find, attract, and retain.

Third, to bring even more clarity to its conflicts analysis, the FTC should consider announcing a bright-line rule in the form of a time limit on conduct that will be considered the same "matter" or "proceeding or investigation." For example, the FTC might decide that, for investigations into the conduct of platforms, such as social networking services or search engines, it is not the same "matter" if it occurs more than two years after an earlier matter, nor is an investigation the same "proceeding or investigation" if it arises more than two years later. This approach finds support in the rhetoric of the FTC itself, which regularly publishes paeans to the speed and dynamism of innovation in the technology industry.[162]

To blunt the potential arbitrariness of a rigid two-year deadline, this gloss on the FTC rules can be presented as a rebuttable presumption: facts will be presumed not to involve the same matter after two years, but the FTC can

162. *See, e.g.*, Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule, 84 FED. REG. 35,842, 35,843 (July 25, 2019); FED. TRADE COMM'N, BIG DATA: A TOOL FOR INCLUSION OR EXCLUSION? i (2016) ("With a smartphone now in nearly every pocket, a computer in nearly every household, and an ever-increasing number of Internet-connected devices in the marketplace, the amount of consumer data flowing throughout the economy continues to increase rapidly."); STAFF OF THE FED. TRADE COMM'N, PROTECTING CONSUMERS IN THE NEXT TECH-ADE 2 (2008) ("Consumers' roles are changing in this new marketplace, as are the products they buy, how those products are marketed and advertised, and how they are paid for . . . [and] at a dizzying pace . . . ."); Maureen K. Ohlhausen, *The Procrustean Problem with Prescriptive Regulation*, 23 COMMLAW CONSPECTUS 1, 2 (2014) ("When the regulated industry is rapidly evolving, yesterday's comfortable regulatory bed can quickly become a torture rack for tomorrow's technologies."); Maureen K. Ohlhausen, Acting Chairman, Fed. Trade Comm'n, Antitrust Enforcement in the Digital Age, Remarks Before the Global Antitrust Enforcement Symposium 6, 11 (Sept. 12, 2017) (describing technology markets as "fast-moving"); Neil Brady, *'Velocity' of Technological Change 'Speeding Up' Says FTC Commissioner*, MEDIUM (July 11, 2017), https://medium.com/@neil.brady/speed-of-technological-change-increasing-sense-of-loss-of-control-says-ftc-commissioner-259265f4389f (accounting how the former FTC Commissioner Terrell McSweeny noted that the "velocity of technological change is speeding up"); Lesley Fair, *Future of the COPPA Rule: What's on the Agenda*, FED. TRADE COMM'N: BUS. BLOG (Oct. 1, 2019, 11:46 AM), https://ftc.gov/news-events/blogs/business-blog/2019/10/future-coppa-rule-whats-agenda ("Technology changes at the speed of light, but the touchstone of the Children's Online Privacy Protection Rule remains constant."); *Financial Technology: Protecting Consumers on the Cutting Edge of Financial Transaction*, FED. TRADE COMM'N, https://www.ftc.gov/news-events/media-resources/consumer-finance/financial-technology (last visited Aug. 23, 2020) (describing the agency's approach to the "fast-moving realm of financial technology").

rebut the presumption by marshaling specific facts demonstrating the same matter.

Fourth, the FTC should also revise its rules to make it easier for former technologists to consult on "same side" investigations, such as those conducted by state attorneys general. To do this, the FTC should revise its definition of "communicate to or appear before"—a key definition that serves to specify which types of activities by former employees are subject to restriction.[163] Under the current definition, the FTC's rules are triggered when a former employee engages in "any oral communication or written communication to, or any formal or informal appearance before, the Commission or any of its members or employees on behalf of any person (except the United States) with the intent to influence."[164] We recommend that the agency add "or the Government of one of the States" to the parenthetical exception. The purpose of the rules is to enable more effective enforcement of the law by preventing agency capture or the appearance of corruption, and the exception acknowledges that other work on behalf of the government does not present that concern. The exception easily could—and should—be extended to work on behalf of state attorneys general, which support the agency's consumer protection and competition mission.

The FTC's rules must be revised, but in the meantime, the OGC can also simply exercise its discretion to grant more clearance requests from former technologists seeking to work on investigations on behalf of state attorneys general. In laying out prohibited conduct for former employees, the text of the rules clarifies that post-employment conduct may be "otherwise specifically authorized by the Commission," though the rules do not elaborate further about what those circumstances might be.[165] In addition, § 207 includes a specific exception for former employees that provide scientific or technological information. That exception states in part that certain § 207 restrictions do not apply "with respect to the making of communications solely for the purpose of furnishing scientific or technological information, if such communications are made under procedures acceptable to the department or agency concerned."[166] In many instances, state attorneys general seek former technologists' advice on policy and strategy, not solely for scientific or technological information. However, there are circumstances in which the

163. *See* 16 C.F.R. § 4.1(b)(1) (restricting when a "former member or employee . . . of the Commission may communicate to or appear before the Commission, as attorney or counsel, or otherwise assist or advise behind-the-scenes, regarding a formal or informal proceeding or investigation").

164. 16 C.F.R. § 4.1(b)(5)(ii).

165. 16 C.F.R. § 4.1(b)(1).

166. 18 U.S.C. § 207(j)(5).

FTC could rely on this exception to quickly bless requests from former technologists to provide scientific or technological information to other parties, particularly those on the "same side." Yet FTC staff never even mentioned the existence of this exception to those of us who are former technologists when we sought advice on possible conflicts.

In addition, the FTC should create greater transparency into its substantive evaluation of clearance requests, as well as into the procedures it applies in considering those requests. At present, it is difficult for members of the public and, indeed, former technologists themselves to gain insight into this process. Under the FTC's rules, "[a]ny request for clearance filed by a former member or employee pursuant to this section, as well as any written response, are part of the public records of the Commission, except for information exempt from disclosure under § 4.10(a) of [the] chapter."[167] However, documents related to clearance requests are not available on the FTC's website or in its "FOIA Reading Room." We submitted a request to the FTC under the Freedom of Information Act for "[a]ll documents relating to clearance requests filed by former FTC employees under 16 C.F.R. § 4.1(b)(2)" from January 2017 to March 2020, but our request was denied on the basis that "the resources required to process your request would cause an unreasonably burdensome review process for the agency."[168]

The agency's clearance process should also be clarified so that ex-employees know what to expect. The FTC's rules set forth particular procedures for FTC consideration of clearance requests filed by former employees. But in our experience, the staff of OGC frequently dismiss clearance requests informally over email, without either directing former employees to file formal requests pursuant to the FTC's rules or referring the matter to the Commission for approval.[169]

We also propose that OGE revise its regulations under § 207. In particular, OGE should vest federal agencies, including the FTC, with clearer authority to determine when a particular "matter" is the same as another for purposes of applying § 207. At least where independent agencies are concerned, we propose that this interpretative authority lie with the specific agency where a former federal employee previously served. This would constitute a modest shift from OGE's current guidance that the agency where an employee previously served may advise the employee as to the application of § 207 but

167. 16 C.F.R. § 4.1(c).
168. Freedom of Information Act (FOIA) request and response on file with authors.
169. *See* 16 C.F.R. §§ 4.1(b)(6)–(7).

that any advice it provides will not be binding on the DOJ.[170] Granting clearer deference to federal agencies—including the FTC—on the question of whether or not two particular matters are the same may empower the FTC to make the determination based on whether or not it believes there is a true conflict of interest, rather than based on the agency's over-prudent estimation of the broadest way in which the DOJ could possibly construe the question itself.

Finally, parallel reforms would also help alleviate the problems we have outlined, or at least they would help ensure that even if former technologists continue to be broadly precluded from contributing to similar work with other agencies, this disincentive does not completely halt the influx of technologists interested in public service. For example, a modest raise to the pay scale for government employees would help attract technologists. It is a tall order to expect recently graduated computer scientists to turn down six-figure salaries working for technology companies in the background of financial burdens like substantial student debt or supporting families.[171] Students with fewer resources are disproportionately deterred from government service, which results in a federal service that is disproportionately wealthier than the rest of the population. Public service should not be a vocation reserved for the independently wealthy. The practices of technology companies implicate every part of society, and we need enforcers with diverse backgrounds and prior experiences. Moreover, paying public servants at rates more comparable with the private sector would help to reduce the revolving door problem. Agency employees, congressional aides, and public servants at all levels of government would not need to leave the government out of financial necessity if government service paid comparable rates to the private sector. Public service may be a calling, but a calling cannot feed children or pay a landlord.

---

170. 5 C.F.R. §§ 2641.105(a), (c). This would also be consistent with at least one federal appellate case that considered a "same particular matter" question in an instance where the agency in question had advised the former employee that two matters were not the same. CACI., Inc.-Federal v. United States, 719 F.2d 1567, 1576 (Fed. Cir. 1983) ("This ruling is entitled to weight. It would be most unusual to disqualify [former employee] Sterling from bidding on the proposal because of Stevens' participation for Sterling after the Assistant Attorney General in charge of the Antitrust Division had advised Sterling that Stevens' handling of the proposal for Sterling would not be improper.").

171. *See* Adam Janofsky & Matt Drange, *We Counted the FTC Employees who Moved Over to Tech. Is Reform Needed?*, PROTOCOL (Mar. 9, 2020), https://www.protocol.com/ftc-tech-hawley-revolving-door/ (quoting one former FTC employee who now works for Electronic Arts as saying that it can be "very difficult to live there on a government salary, especially if you have student loan debt").

VI. CONCLUSION

Few question the dire need for technological expertise at the U.S. consumer protection and competition agency. Yet, the FTC is exacerbating its existing difficulty in recruiting and retaining technologists by unduly limiting the kind of work technologists can undertake after leaving government service. The FTC's interpretation and uneven application of well-intentioned conflict rules further undermine not only its own efficacy, but also the efficacy of complementary enforcement bodies that support the agency's mission. We urge a series of modest reforms to prevent post-employment restrictions from hamstringing the FTC's enforcement efforts as well as those of other agencies. We hope these reforms will also help pave the way for skilled technologists to seek and secure meaningful careers in public service without unnecessarily hemming in their future career prospects.

THROUGH THE HANDOFF LENS: COMPETING VISIONS OF AUTONOMOUS FUTURES

Jake Goldenfein[†]*, Deirdre K. Mulligan*[††]*, Helen Nissenbaum*[†††] *& Wendy Ju*[‡]

ABSTRACT

The development of autonomous vehicles is often presented as a linear trajectory from total human control to total autonomous control, with only technical and regulatory hurdles in the way. But below the smooth surface of innovation-speak lies a battle over competing autonomous vehicle futures with ramifications well beyond driving. Car companies, technology companies, and others are pursuing alternative autonomous vehicle visions, and each involves an entire reorganization of society, politics, and values. Instead of subscribing to the story of inevitable linear development, this paper explores three archetypes of autonomous vehicles—advanced driver-assist systems, fully driverless cars, and connected cars—and the futures they foretell as the ideal endpoints for different classes of actors. We introduce and use the Handoff Model—a conceptual model for analyzing the political and ethical contours of performing a function with different configurations of human and technical actors—in order to expose the political and social reconfigurations intrinsic to those different futures. Using the Handoff Model, we analyze how each archetype both redistributes the task of "driving" across different human and technical actors and imposes political and ethical propositions both on human "users" and society at large. The Handoff Model exposes the baggage each transport model carries and serves as a guide in identifying the desirable and necessary technical, legal, and social dynamics of whichever future we choose.

DOI: https://doi.org/10.15779/Z38CR5ND0J

† Senior Lecturer at Melbourne Law School, University of Melbourne, Associate Investigator in the ARC Centre of Excellence for Automated Decision-Making and Society, and an Associate at Cornell Tech's Digital Life Initiative.

†† Professor, School of Information, University of California, Berkeley; Faculty Director, Berkeley Center for Law and Technology.

††† Professor of Information Science and Director of the Digital Life Initiative, Cornell Tech.

‡ Associate Professor of Information Science in the Jacobs Technion-Cornell Institute at Cornell Tech. Much appreciation to: organizers, participants, and particularly moderator Madeleine Claire Elish at We Robot 2019; members of the Handoff team, John Chuang, Nick Doty, Daniel Griffin, Adam Wolisz, and Richmond Y. Wong for endless workshopping of the model and feedback on this work; Michael Byrne for his assistance with graphics along with the entire Digital Life Initiative research group for rich feedback, and organizers and participants in the Simons Institute for the Theory of Computer Science Data Privacy: Foundations and Applications semester (Spring 2019) for insightful and helpful comments and discussions, and the luxury of being immersed in an inspiring research community; the participants in the Digital Life Initiative's Spring 2020 Autonomous Vehicles: What is the worst that could possibly happen? workshop; and for generous funding for this research from the MacArthur Foundation and the National Science Foundation under the U.S. NSF INSPIRE SES1537324.

TABLE OF CONTENTS

I. INTRODUCTION 836

II. THE HANDOFF MODEL 843

III. AUTONOMOUS VEHICLE FUTURES 850

A. ARCHETYPE 1: "DRIVER ASSIST" 852
1. Interfaces 854
2. Responsibility and Autonomy 859
B. ARCHETYPE 2: "DRIVERLESS CAR" 862
1. Business Models and Ownership 867
2. Data Flows and Privacy 869
3. Responsibility and Autonomy 871
C. ARCHETYPE 3: "CONNECTED CARS" 877
1. Political Coordination for Connected Cars 881
2. Machine Readable Spaces and People 884
3. Data Governance 886
4. Responsibility and Autonomy 887

IV. VALUE CHOICES IN AUTONOMOUS VEHICLE FUTURES – GUIDANCE FOR POLICY-MAKERS 891

A. DRIVER ASSIST 892
1. Agency, Responsibility, and the Changing Roles for Human and Technical Actors 892
B. DRIVERLESS CARS 899
1. Repositioning the "Moral Crumple Zone" 900
C. CONNECTED CARS 902
1. Legibility 902
2. Ownership and Centralization 903
3. Privacy 903
4. Changing the Values Aperture: Transportation Access and Environmental Impact 907
5. Coda: Redefining Safety 909

V. CONCLUSION 909

I. INTRODUCTION

In December 2018, Waymo, the self-driving vehicle subsidiary of Alphabet, launched a commercial passenger transport platform called "Waymo

One."[1] Limited to a group of participants in Waymo's closed testing program, and only in a small, geographic area in Phoenix, Arizona, the launch revealed more about the rhetoric of self-driving vehicles than it illuminated the future of transport. Although Waymo's promotional videos showed passenger vehicles without human drivers in the front seats, the reality was different.[2] Vaunted as the launch of a truly "driverless," commercial transport (i.e., ride-sourcing) system, the Waymo One service still employed specially trained "drivers," "safety supervisors," or "vehicle operators" that travelled with the vehicles. Although the drivers' presence was framed more as a customer service than a legal or safety requirement,[3] it sowed doubt as to the technical *possibility* of fully driverless vehicles[4] and destabilized the terminology behind "self-driving," "driverless," or "autonomous." It also reminded us that autonomous, ride-hailing vehicles, with nobody in the front seat controlling the car, is only one vision for the future of autonomous transport—a vision that includes technology companies pursuing ways to decrease costs of ride-sourcing services.

The entities pursuing that vision, along with the entities pushing for every other configuration of autonomous vehicles, have their own ideas for how these configurations should look and perform and what their business case might be. Just as the "safety driver" in the Waymo One car both exposed and interrupted the imagined trajectory towards fully automated transport, unpacking how respective models of autonomous transport might actually work exposes the stakeholders and political interests, as well as the impacts on human and societal values that they each embed. It is within the specificities of these different visions of autonomous transport futures that their ethical and political consequences are expressed.

---

1. Waymo Team, *Riding with Waymo One Today*, MEDIUM (Dec. 5, 2018), https://medium.com/waymo/riding-with-waymo-one-today-9ac8164c5c0e.

2. Whatever degree of fully driverless testing occurring is likely a tiny fraction of all on-road testing; in fact, companies may have halted testing fully driverless vehicles entirely. *See, e.g.*, Timothy B. Lee, *Even Self-Driving Leader Waymo Is Struggling to Reach Full Autonomy*, ARS TECHNICA (Dec. 7, 2018, 8:55 AM), https://arstechnica.com/cars/2018/12/waymos-lame-public-driverless-launch-not-driverless-and-barely-public/ (reporting on the extremely limited public launch of Waymo One and abandonment of plans to launch a fully driverless program).

3. Andrew J. Hawkins, *Riding in Waymo One, the Google Spinoff's First Self-Driving Taxi Service*, THE VERGE (Dec. 5, 2018, 8:00 AM), https://www.theverge.com/2018/12/5/18126103/waymo-one-self-driving-taxi-service-ride-safety-alphabet-cost-app.

4. *See, e.g.*, Neal E. Boudette, *Despite High Hopes, Self-Driving Cars are 'Way in the Future'*, N.Y. TIMES (July 17, 2019), https://www.nytimes.com/2019/07/17/business/self-driving-autonomous-cars.html; Alex Davies & Aarian Marshall, *Are We There Yet? A Reality Check on Self-Driving Cars*, WIRED (Apr. 22, 2019, 6:00 AM), https://www.wired.com/story/future-of-transportation-self-driving-cars-reality-check/.

Each vision includes different conceptions of and roles for "drivers," "passengers," "users," and "occupants"; different systems for communications and control; different systems of spatial organization; different commercial and political arrangements; and different consequences for societal and human values. Each imagination of autonomous automotive transport involves an entire world of reorganization for politics and values—each presenting different challenges for regulators and the public. Reckoning with the implications of these reconfigurations means seeing past terminological obfuscation[5] and beyond the emphasis on discontinuities in the transport experience,[6] instead focusing on how each autonomous transport vision, promoted by various parties, moves toward a different future with particular political and ethical implications.

To perform that analysis, this Article introduces the Handoff Model to complement and help structure existing work exploring the technical, legal, and policy implications of autonomous vehicles. The model rigorously identifies how the *function* of driving is re-configured and delegated to different *components* (human, computational, mechanical, and regulatory) in alternative autonomous driving visions, and, in so doing, the model brings to light the political and ethical propositions captured in these alternative configurations.

For our Handoff analysis of autonomous vehicles, we have found it useful to create a rough classification of three archetypes (or "scripts")[7] of autonomous vehicle deployments, each of which captures a distinctive vision

5. *See generally* Meg Leta Jones & Jason Millar, *Hacking Metaphors in the Anticipatory Governance of Emerging Technology: The Case of Regulating Robots*, *in* THE OXFORD HANDBOOK OF LAW, REGULATION & TECHNOLOGY (Roger Brownsword, Eloise Scotford & Karen Yeung eds., 2017).

6. *See, e.g.*, DEP'T FOR TRANSP., THE PATHWAY TO DRIVERLESS CARS: SUMMARY REPORT AND ACTION PLAN 16 (Feb. 2015) (U.K.), https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/401562/pathway-driverless-cars-summary.pdf (defining the difference between existing driver assistance systems and higher levels of automation); Adriano Alessandrini, Andrea Campagna, Paolo Delle Site, Franceso Filippi & Luca Persia, *Automated Vehicles and the Rethinking of Mobility and Cities*, 5 TRANSP. RES. PROCEDIA 145 (2015), https://doi.org/10.1016/j.trpro.2015.01.002; Lawrence D. Burns, *A Vision of Our Transport Future*, 497 NATURE 181 (2013), https://doi.org/10.1038/497181a; Daniel J. Fagnant & Kara Kockelman, *Preparing a Nation for Autonomous Vehicles: Opportunities, Barriers and Policy Recommendations*, 77 TRANSP. RES. PART A: POL'Y & PRAC. 167 (2015), https://doi.org/10.1016/j.tra.2015.04.003.

7. Madeleine Akrich, *The De-Scription of Technical Objects*, *in* SHAPING TECHNOLOGY/BUILDING SOCIETY: STUDIES IN SOCIOTECHNICAL CHANGE 208 (Wiebe E. Bijker & John Law eds., 1997).

of an autonomous vehicle future.[8] These archetypes, while somewhat stylized, express different visions of technical, political, commercial, and economic arrangements in autonomous vehicle deployment. Drawing on similar divisions that appear elsewhere in the literature, we call these archetypes, respectively: driver assist cars, driverless cars, and connected cars. We recognize that the boundaries of these archetypes are contingent, overlapping, and hardly settled. Nonetheless, we consider them to be analytically useful for exposing what is at stake in different autonomous transport implementations. We also note that these archetypes share political and ethical concerns, and that the focus on any one issue in a single archetype will likely have relevance for the others.

The first archetype, driver assist, involves driving tasks being shared between humans and automated systems. It envisions a gradual increase in the degree and competence of automation in privately-owned-and-operated passenger vehicles, but without removal of human drivers and without new demands on other physical infrastructure. This model assumes "existing roadway"—i.e., no major instrumentation of roads and intersections—and "existing ownership"—i.e., cars are largely privately owned by individuals. Here, automation becomes the advanced rendition of Advanced Driver Assistance Systems (ADAS), which currently include capabilities like power steering, cruise control, and automated lane-keeping. This framing is preferred by the incumbent automotive industry.[9] The driver assist model retains a human "driver" (at least some of the time), typically includes less on-board sensing and computation than fully driverless vehicles in order to control cost, and reconfigures the locus of control across onboard human and computational actors. While proponents suggest this approach is safer in the short term, others argue it may be more dangerous in the long term, as it delays the proliferation of fully driverless vehicles, which are argued to be inevitably

8. *See, e.g.*, Sven Beiker, *Deployment Scenarios for Vehicles with Higher-Order Automation*, *in* AUTONOMOUS DRIVING: TECHNICAL, LEGAL, AND SOCIAL ASPECTS 193–211 (Markus Maurer et al. eds., 2018) (describing the "evolutionary" scenario involving the continued improvement of ADAS systems; the "revolutionary" scenario involving the transformation of mobility services through driverless vehicles; and the "transformative" scenario involving the creation of integrated public transport-style urban solutions). These map relatively clearly onto our description of "driverless," "ADAS," and "connected" models. *See id.*

9. Gilles Duranton, *Transitioning to Driverless Cars*, 18 CITYSCAPE: J. POL'Y DEV. & RES. 193, 195 (2016), https://www.huduser.gov/portal/periodicals/cityscpe/vol18num3/ch12.pdf.

safer.[10] Importantly, we analyze the driver assist archetype not simply as a transitional phase, but as a different vision of transport future.

The second archetype, driverless cars, is a model of a fully "driverless" vehicle that removes the occupant's capacity to control (i.e., drive) the car. Like archetype one, the second uses existing roadways. However, it generally envisions new ownership models. The defining exemplar is the (now abandoned) Google Koala car, which featured a vehicle cabin without any human driving controls—no steering wheel and no brake or accelerator pedals.[11] While that model was abandoned,[12] the design philosophy is being replicated in newer models like the General Motors Cruise constructed Chevrolet Bolt[13] (although in June 2019, Cruise also postponed launching its driverless taxi service which used vehicles without internal controls).[14] The potential for such vehicles has long been described as transformative, as they can travel both occupied and unoccupied, meaning they can operate unceasingly in various capacities.[15] Currently, because the sensing and computation needed for such vehicles is prohibitively expensive for the consumer market, fully driverless *passenger* vehicles[16] are viewed as best suited

10. *See, e.g.*, INT'L TRANSP. FORUM CORP. P'SHIP BD., SAFER ROADS WITH AUTONOMOUS VEHICLES? CORPORATE PARTNERSHIP BOARD REPORT 19 (2018), https://www.itf-oecd.org/sites/default/files/docs/safer-roads-automated-vehicles.pdf; Pete Bigelow, *Why Level 3 Automated Technology Has Failed to Take Hold*, AUTOMOTIVE NEWS (July 21, 2019, 9:00 PM), https://www.autonews.com/shift/why-level-3-automated-technology-has-failed-take-hold; Stephen Edelstein, *Audi Gives Up on Level 3 Autonomous Driver-Assist System in A8*, MOTOR AUTHORITY (Apr. 28, 2020), https://www.motorauthority.com/news/1127984_audi-gives-up-on-level-3-autonomous-driver-assist-system-in-a8.

11. Mark Bergen, *Google's Self-Driving 'Koala' Cars Now Out in the Wild*, VOX (June 25, 2015, 12:31 PM), https://www.vox.com/2015/6/25/11563902/googles-self-driving-koala-cars-now-out-in-the-wild.

12. Mike Murphy, *The Cutest Thing Google Has Ever Made Is Dead*, QUARTZ (June 13, 2017), https://qz.com/1005083/the-cutest-thing-google-has-ever-made-is-dead-waymos-firefly-self-driving-cars-goog/.

13. Andrew J. Hawkins, *GM Will Make an Autonomous Car Without Steering Wheel or Pedals by 2019*, THE VERGE (Jan. 12, 2018, 12:01 AM), https://www.theverge.com/2018/1/12/16880978/gm-autonomous-car-2019-detroit-auto-show-2018.

14. Andrew J. Hawkins, *Cruise Postpones Plan to Launch Driverless Taxi Service in 2019*, THE VERGE (July 24, 2019, 8:51 AM), https://www.theverge.com/2019/7/24/20707242/cruise-gm-self-driving-taxi-launch-delay-2019.

15. *See generally* Kevin Spieser, Kyle Treleaven, Rick Zhang, Emilio Frazzoli, Daniel Morton & Marco Povone, *Towards a Systematic Approach to the Design and Evaluation of Automated Mobility-on-Demand Systems: A Case Study in Singapore*, *in* ROAD VEHICLE AUTOMATION 229–45 (Gereon Meyer & Sven Beiker eds., 2018), https://link.springer.com/chapter/10.1007/978-3-319-05990-7_20.

16. Fatemeh Nazari, Mohamadhossein Noruzoliaee & Abolfazl (Kouros) Mohammadian, *Shared Versus Private Mobility: Modeling Public Interest in Autonomous Vehicles*

for transportation network (or "ride-sourcing") companies (TNCs).[17] This would involve a shift away from the current TNC business model, which relies on participating drivers using personal vehicles, towards fleets of driverless vehicles owned by platforms, likely large technology companies such as Google and Uber. Pilot tests along these lines are currently underway in California where both the "driverless" nature of the vehicles and the new ownership models have precipitated a suite of new regulations.[18]

Our third archetype is connected cars. This model positions vehicles as elements of broader "smart city" transport programs. Unlike driverless vehicles that navigate solely on the basis of their on-board sensor arrays and computation, connected vehicles operate in constant communication with one another as well as with other components of a static roadway infrastructure. Connected cars thus involve the most radical re-instrumentation of public space and require complex technical and political coordination. Some variations of the connected car vision include a role for the traditional automotive industry, with privately owned and operated vehicles running through connected infrastructures,[19] while others propose a holistic package of concentrated infrastructure and vehicle ownership offered to the public as a mobility service, analogous to public transport in certain ways.[20] Connected

Accounting for Latent Attitudes, 97 TRANSP. RES. PART C: EMERGING TECH. 456 (2018); Adam Stocker & Susan Shaheen, *Shared Automated Vehicles: Review of Business Models* (Int'l Transp. Forum, Discussion Paper No. 2017-09, 2017), https://www.econstor.eu/bitstream/10419/194044/1/itf-dp-2017-09.pdf. Note that we focus on passenger vehicles here rather than logistics or other types of vehicles.

17. Transportation Network Company (TNC) is the dominant term used in state regulations. Maarit Moran & Philip Lasley, *Legislating Transportation Network Companies*, 2650 TRANSP. RES. REC.: J. TRANSP. RES. BD. 163, 165 (2017) ("Thirty states define ride-sourcing providers as TNCs."). California was the first to regulate and to define TNCs. *Id.*; *see also* CAL. PUB. UTIL. CODE § 5431(c) (West 2019) (" 'Transportation network company' means an organization, including, but not limited to, a corporation, limited liability company, partnership, sole proprietor, or any other entity, operating in California that provides prearranged transportation services for compensation using an online-enabled application or platform to connect passengers with drivers using a personal vehicle.").

18. Dasom Lee & David J. Hess, *Regulations for On-Road Testing of Connected and Automated Vehicles: Assessing the Potential for Global Safety Harmonization*, 136 TRANSP. RES. PART A: POL'Y & PRAC. 85, 90–91 (2020) (describing U.S. and California-specific rules developed for on-road testing of automated and connected cars—archetype two and three in our framework).

19. *See, e.g.*, *About Us*, 5G AUTOMOTIVE ASS'N, https://5gaa.org/about-5gaa/about-us/ (last visited Aug. 31, 2020) (listing the founding members of the 5G Automotive Association, which includes Audi AG, BMW Group, and Daimler AG, as well as Ericsson, Huawei, Intel, Nokia, and Qualcomm).

20. *See, e.g.*, Linda Poon, *Can Toyota Turn Its Utopian Ideal into a 'Real City'?*, BLOOMBERG CITY LAB (Jan. 24, 2020, 10:39 AM), https://www.bloomberg.com/news/articles/2020-01-24/why-is-toyota-building-a-smart-city-from-scratch.

vehicle proponents emphasize the capability of connected autonomous vehicle systems to choreograph complex driving maneuvers that require centralized or coordinated control, like continuous flow intersections, vehicle "platooning," and ultra-high-speed travel.[21]

These models or archetypes—driver-assist, fully-driverless, and connected-cars—may appear to follow a historical trajectory wherein driver assist eventually succumbs to full automation and all private ownership is replaced by mobility-on-demand services. But the reality is more complex, the players are more tangled and integrated, the role and the location of human drivers or operators are not yet determined,[22] and the path forward is still unclear.[23] Although we acknowledge this complexity and that the landscape is constantly shifting, it remains useful to explore these archetypes as distinctive abstractions for the purpose of explaining how each disturbs the existing politics and values of transport in different ways. For us, the archetypes are a means of exploring deep connections between different technical and architectural designs for achieving ostensibly equivalent functional purposes, on the one hand, and respective political and value propositions for users and society, on the other. We recognize the difficulty of analyzing vehicle systems at a level of abstraction that includes the necessary detail to expose consequences on the political and ethical registers of interest to us. Insufficient detail elides critical elements for understanding the ethical and political implications of each archetype. Too much detail, however, risks venturing into

21. *See, e.g.*, José Víctor Saiáns-Vázquez, Esteban Fernando Ordóñez-Morales, Martín López-Nores, Yolanda Blanco-Fernández, Jack Fernando Bravo-Torres, José Juan Pazos-Arias, Alberto Gil-Solla & Manuel Ramos-Cabrer, *Intersection Intelligence: Supporting Urban Platooning with Virtual Traffic Lights over Virtualized Intersection-Based Routing*18 SENSORS 4054 (2018); Koichi Washimi, *Traffic Management System Toward Connected and Automated Vehicles Era*, 88 SEI TECH. REV. 71 (2019); CONNECTED VEHICLE URBAN TRAFFIC MGMT., https://hub.iiconsortium.org/connected-vehicle-urban-traffic-management (last visited July 31, 2020).

22. *See, e.g.*, SAE INT'L, SURFACE VEHICLE RECOMMENDED PRACTICE: TAXONOMY AND DEFINITIONS FOR TERMS RELATED TO DRIVING AUTOMATION SYSTEMS FOR ON-ROAD MOTOR VEHICLES 16 (2018), https://www.sae.org/standards/content/j3016_201806/ (defining four distinct categories of human actors: driver, passenger, fallback-ready user, and driverless operation dispatcher); Madeleine Clare Elish, *When Your Self-Driving Car Crashes, You Could Still Be the One who Gets Sued*, QUARTZ (July 25, 2015), https://qz.com/461905/when-your-self-driving-car-crashes-you-could-still-be-the-one-who-gets-sued/; Dan Hill, *How Should Humans Really Be 'in the Loop' in Cities Under Autonomous Mobility?*, MEDIUM (Oct. 6, 2016), https://medium.com/butwhatwasthequestion/how-should-humans-really-be-in-the-loop-in-cities-under-autonomous-mobility-d13c04f70bba.

23. *See generally* Eva Fraedrich, Sven Beiker & Barbara Lenz, *Transition Pathways to Fully Automated Driving and Its Implications for the Sociotechnical System of Mobility*, 3 EUR. J. FUTURES RES. (2015), https://doi.org/10.1007/s40309-015-0067-8.

all the diverse forces of people, machines, money, and whatever else that might render such an analysis entirely mundane, if possible at all.[24]

To analyze these systems at a meaningful level of abstraction, we introduce the Handoff model as a means of revealing key differences in the configurations and dynamics of system components that alter the values propositions embedded in respective systems—here, vehicle archetypes.[25] "Handoff" exposes how changes in technological configuration shape both inter-system and inter-social relations and have ramifications for a wide range of political and ethical issues, including control over and access to transport and its infrastructures and related impacts on the environment and surroundings.

The goal of our analysis is to highlight what is at stake in terms of societal values and social relations as configured through these different implementations, and to highlight the need to assess and evaluate these changes. In our Handoff analysis of each archetype, we do not aim to be exhaustive but rather to highlight political and ethical issues that the archetype makes particularly salient. While the issues raised, including distribution of ownership, expectations about data flows, and others, are latent in all three archetypes, we have highlighted those that signal more radical or otherwise more significant breaks with current arrangements in our discussions of each of the archetypes, respectively. This approach allows us more effectively to demonstrate the contingent, political nature of different autonomous futures and reflect on how we might purposefully align them with abiding societal goals and values, instead of passively watching them be shaped by prevailing sociotechnical processes and powers.

Before proceeding with the analysis, we introduce key elements of the Handoff model to our readers.

II. THE HANDOFF MODEL

Handoff is a lens for political and ethical analysis of sociotechnical systems. In recent decades, the delegation of decision-making onto automated systems has inspired widespread attention and anxiety about machines that can label ("recognize") images, process ("understand") and produce ("speak") natural

24. Akrich, *supra* note 7, at 205.

25. For another effort to encourage attention to the social impacts of technology through analytic tools, see Shane Epting, *Automated Vehicles and Transportation Justice*, 32 PHIL. & TECH. 389 (2019) (arguing for a broader vision of the ethical issues raised by mobility infrastructures and specifically for the use of complex moral assessments to evaluate the impact of autonomous vehicles on vulnerable populations, the environment, and historical or culturally significant artifacts).

language, and even anticipate what we will say and do. Inspired by claims about computational systems able to take over tasks previously performed by humans—-especially tasks thought to require human intelligence—the concept of Handoff provides a lens through which to scrutinize them. There is a need for a more detailed critical analysis of evolving systems in which a given function shifts from one type of actor to another and people are inclined to say that the latter actor is performing the same function as the former (i.e., same function, different actor), as is often the case with autonomous vehicles.

The Handoff model draws attention to assertions that systems with new actors and control delegations are performing the same function as in their previous iterations. Such assertions include, for example, that automated call-answering systems perform the same function as human receptionists, or that RFID-based systems collecting road tolls or computational systems distinguishing benign from cancerous skin moles are performing the same function as their human or mechanical counterparts. In addition to important questions about the quality of performance, efficiency, or impact on labor markets, the critical eye of Handoff directs attention towards ethical and political issues that may be disrupted by respective versions of a system, thereby belying facile assertions of sameness before and after functional Handoff or delegation of decision-making. It decomposes the "how" of the function to understand what is different and what that difference means for values. It opens our view not only to what might be the same but also to what may have changed in the reconfiguration of function across component actors.

We define "Handoff" as the following: given progressive, or competing, versions of a system (S1, S2) in which a particular system function (F) shifts from one type of actor (A) in S1 to another actor (B) in S2, we say that *F was handed off from A to B.*

The purview of our Handoff model is complex systems comprising diverse functional components. Because such systems can be varied, incorporating physical mechanisms, computational subsystems, and even humans, Handoff's units of analysis, more precisely, are "sociotechnical systems." For purposes of this analysis, we accept the theorization of such systems as noncontroversial. Sociotechnical systems are the subjects of our analytical model, even though, for the remainder of this Article, we mostly revert to the term "system." Abstractly conceived, a system may be defined in terms of its function. This function is typically achieved by coordinated functioning of a system's component parts, and themselves may be conceived as systems, which in turn comprise subsystems, or components, and so on. Because systems of interest may comprise multifarious parts, some material and others

human, we use the term *component* as neutral between the two.[26] The model assumes that *system* and *component* (or subsystem) are relative terms whose application signals the focus of analysis rather than an ontological statement. In an analogy, someone may think of the human body as a system and the organs as component parts; but for the cardiologist, the heart is the system of interest and the chambers, valves, arteries, etc., are its components. In another example, the system of a conventional automobile performing the driving function comprises a vehicle plus a human driver; in turn, each of these components may be analyzed further—the vehicle is composed of various subsystems, such as braking, safety, ignition, and so on.

As noted, systems perform functions, and it is the redistribution of these functions that interests us, whether this involves Handoffs from a human to a machine (i.e., automation), a human acting in one role to a human in another role, or a machine of one type (e.g., mechanical) to a machine of another (e.g., electronic). What those functions are, in general terms, is answered by the question, "what does a given system do?" Components also perform functions, similarly, beginning the question, "what does it do," expecting the answer will address how the component function contributes to the overall function of the system. Finally, it is important to notice that a system's function can be described at different levels of abstraction: up a level, referring to goals, purposes, or even values; down a level, the way a designer or engineer might explain how it does what it does. The Handoff model provides a sensitive tool for illuminating the interplay between the two ways a reconfiguration of function at levels of implementation can impinge on attainment of higher-order purposes.

To perform a Handoff analysis at the implementation layers, we introduce and define key concepts of the model. To start, an analyst needs to identify and explain how the relevant components work to produce the overall system function, what drives their respective actions (or motions), and how they interact with one another. To this end, we introduce the idea of components *acting-on* or *engaging* other components. Take a traditional automobile (i.e.,

26. Terminology presented a dilemma. While the term "component" does not naturally apply to human actors, for our purposes it is important to be able to refer in like manner to human and non-human components of a system. The Actor-Network-Theory, which most certainly influenced us, came up with "actant" as a way out of the dilemma. But our preference is not to adopt theoretical jargon, which can be off-putting for general readers. *See, e.g.*, BRUNO LATOUR, REASSEMBLING THE SOCIAL: AN INTRODUCTION TO ACTOR-NETWORK-THEORY (2015). Going forward, we will mostly use the term "component" but will sometimes revert to "actor" or "subsystem." In addition to human actors and physical objects that can be or constitute system components, we allow for the possibility of groups and institutions as components.

vehicle plus driver system) driving on a road. Darkness falls and a human driver (i.e., component) pushes a button, which in turn causes the car headlights to illuminate. In this instance we say that the components act on each other to produce an outcome (i.e., fulfill the function), "turn on headlights." The driver decides and pushes a button, and the button then causes the headlights to flash on.

This trivial case requires a further concept, namely, that of the mode of acting-on or engaging. Before elaborating on modes, it is worth noting that the underlying idea is not completely novel; instead, one can find versions of it in disparate works in the field of technology and society. One case in point is Larry Lessig's concept of modalities of regulation,[27] which famously emphasized the similarities among seemingly divergent modalities. By contrast, others have argued that different modalities constitute a normative difference that should not be ignored.[28]

One familiar mode of acting-on another object is physical force, where one physically embodied actor causes an outcome in another.[29] The outcome may be achieved either by producing or preventing action. The human actor pushes a button and sets off a causal chain of actions resulting in the headlights flashing on. Physical (or "material") causation, or—one could say—"brute force," may operate in multiple, different ways. For example, a physical component (or set of objects) may act on another component by constraining its range of action (e.g., a safety overlock) without necessarily causing a particular outcome. Alternatively, there could be far more complex causal interdependencies, as when numerous components function together to produce a complex configuration of outcomes on other components, and so on.

A different mode of acting-on—perhaps more subtle—is affordance. As defined by the cognitive psychologist J.J. Gibson, affordances are relational properties of things in the environment whose meaning or significance is

27. *See, e.g.*, LAWRENCE LESSIG, CODE: VERSION 2.0 (2d ed. 2006).

28. Roger Brownsword, *Lost in Translation: Legality, Regulatory Margins, and Technological Management*, 26 BERKELEY TECH. L.J. 1321, 1328 (2011); Helen Nissenbaum, *From Preemption to Circumvention: If Technology Regulates Why Do We Need Regulation (and Vice Versa)?*, 26 BERKELEY TECH. L.J. 1367 (2011); Margaret Jane Radin, *Regulation by Contract, Regulation by Machine*, 160 J. INSTITUTIONAL & THEORETICAL ECON. 142 (2004); Harry Surden, *Structural Rights in Privacy*, 60 SMU L. REV. 1605 (2007); Karen Yeung, *The Forms and Limits of Choice Architecture as a Tool of Government*, 38 L. & POL'Y 186 (2016).

29. Remaining at the intuitive level for the moment, we must look past the fact that there is nothing simple about causation, as Aristotle well demonstrated. *See* ARISTOTLE, PHYSICS 194b (C. D. C. Reeve trans., Hackett Publishing Company, Inc. 2018) (c. 350 B.C.E.); ARISTOTLE, POSTERIOR ANALYTICS 71b (G. R. G. Mure trans., eBooks@Adelaide 2007) (c. 350 B.C.E).

derived from their service to a given agent's needs or capabilities.[30] When saying that something is nourishing, or is a tool or secure cover, these observed properties must be understood in relation to actors of particular shapes, sizes, abilities, and needs. As adapted and widely popularized by Donald Norman, designers can and should take advantage of affordances in order to create artifacts that are understood by users and elicit desired behaviors required for successful operation of the respective artifacts.[31] According to Norman, an object's affordances suggest uses to us by triggering human cognitive and perceptual capacities.[32] Good designers of material objects, such as doors and switches, are able to elicit correct usage or desired reactions by effectively exploiting human actors' tendencies to respond to cues in systematic ways. The same ideas extend to digital objects, such as websites and appliance controls. For example, a social media site that displays its users' information may enhance the possibility of repurposing it by third parties by supporting an application programming interface (API) that eases data extraction, or it may diminish that possibility through technical or legal rules (for example, a prohibition on scraping) that discourage such extraction. In such cases the language of affordance is more accurate than causation. In the case of autonomous vehicles, affordances constitute a mode of acting-on that can serve designers of vehicle interfaces seeking to convey to users (e.g., drivers and passengers) what range of actions are possible and desirable in relation to the vehicle's operation. Unlike physical force, affordances are perceived and processed by users (human users, in this case) who act in accord with them, often strategically.

Returning to our mini case of a driver switching on headlights illustrates the application between mode and affordance. We observe that the human actor physically exerts force on the button, thereby initiating a causal chain resulting in the lights flashing on. When, further, we ask what made the human push the button, there may be various answers. One such answer may cite acting-on by pointing to the interface, which has successfully exploited the affordance of "push-ability" in its design of the button in question.

Other answers illustrate additional modes of acting-on. Another plausible answer may cite purpose: the driver pushed the button because visibility was poor, night had fallen, and/or it had started raining. A different answer may cite obedience to the law, which prescribes switching on the headlights under

30. *See* JAMES J. GIBSON, THE ECOLOGICAL APPROACH TO VISUAL PERCEPTION 127–28 (1979).

31. *See* DONALD NORMAN, THE DESIGN OF EVERYDAY THINGS (Basic Books rev. ed. 2013) (1988).

32. *See id.* at 1–34.

certain conditions. Each of these cases reports on an intentional action taken by the driver, here, a decision to switch on the headlights. Although the model does not view the law, or light levels, or the miserable weather as components—they do not *act on* the driver—they surely inform the driver's action. The driver chooses to act (i.e., pushes the button) after having identified conditions or pertinent rules, interpreted them, and decided to act accordingly. The driver (user), as a free agent, is the prime mover causing the headlights to flash on by pushing a button.

Now, imagine a subsequent model of the vehicle, in which the operation of headlights is automated via a small computer embedded within the vehicle. In this case, under the appropriate external conditions, the algorithm's expression in lines of software code, implemented in an embodied computer, acts-on relevant components resulting in the lights turning on. The software code (and more abstractly, the algorithm) operates like legal rules. The model does not reify them as component actors; instead, their informational content, expressed as coded instructions, is embodied in material, electronic computers, which act-on other system components, and so on. Without delving into metaphysical questions about the nature of free agency, the Handoff model asserts a difference between automated headlight switches and human-operated switches by noting that in acting-on the coded rules, the material computer is not a prime mover but has been acted-on by those responsible for the code, prior to any particular trigger external to the system. Later in the Article, the implications of some of our choices will become clear.

In the headlights case, we could say that the function of switching on the light had been handed off from human actor to computer controller. As a matter of fact, well before the general hype over autonomous vehicles, a progressive shifting, or handing off, of certain functions from a human controller (driver) to vehicle components had been underway for some time. For example, the Electronic Stability Control System (ESC system) wrests control from the driver when it senses rear wheel activity that indicates "spinning out" (i.e., loss of directional stability) or front wheel activity that indicates "plowing out" (i.e., loss of directional control).[33] In these instances, the car seizes control from the human driver and endeavors to bring the car back under control. The car's lateral acceleration and yaw rate, captured by onboard sensors, are compared to the driver's intended direction inferred from speed and steering angle measurements. If they are inconsistent, the ESC

33. Electronic Stability Control Systems for Light Vehicles, 49 C.F.R. § 571.126 (2015) (requiring ESC systems on passenger cars, multipurpose passenger vehicles, trucks, and buses with a gross vehicle weight rating of 10,000 pounds or less).

system takes over.[34] The ability to adjust brake torque independently on each wheel allows the ESC system to use uneven brake force—rather than steering input—to reestablish a yaw appropriate to the intended direction of the driver. Similarly, protections against dangerous secondary-impact injuries—driver and passenger collisions with the inside of cars caused by a crash—moved from reliance on human actors to engage safety belts to foisting protection upon initially the driver and, over time, the front and backseat passengers, through the introduction of passive restraints, such as airbags. These Handoffs, while aimed at improving safety, have met with a range of value-based resistance, presaging the need for a model such as ours to identify and manage values during functional redistributions.[35]

Finally, considering the impetus or triggering event (what we refer to as "the Trigger") for two competing or sequential Handoff configurations, we highlight specific values that may be both motivating the reconfiguration or implicated by it. Historian Peter Norton offers an account of a shift that took place during the 1960s from a paradigm of traffic safety that emphasized *control* to one that focused on crashworthiness.[36] The control paradigm centered on preventing accidents through expert driver control. It was delivered through engineers designing safer roads, expertly educated drivers and informed pedestrians, and heavy-handed enforcement to prevent reckless driving. While the control paradigm concentrated on reducing the safety risks posed by drivers, pedestrians, and roads, the crashworthiness paradigm, spurred by rising fatalities, ushered in a focus on reducing the damage of inevitable collisions and focused on reducing the damage caused by vehicle occupants colliding with the interior of the automobile. This paradigm put the design of automobiles in service of safety.

---

34. For a description of how electronic stability control systems work, see Nat'l Safety Couns., *Electronic Stability Control*, MYCARDOESWHAT.ORG, https://mycardoeswhat.org/safety-features/electronic-stability-control/ (last visited Sept. 1, 2020).

35. Automakers resisted passive restraints based on the belief that *explicitly* removing the driver and passenger from enacting safety through putting on a belt *implicitly* suggested questions about who would be held responsible and ultimately liable for injuries and fatalities. *See* Jameson M. Wetmore, *Redefining Risks and Redistributing Responsibilities: Building Networks to Increase Automobile Safety*, 29 SCI., TECH. & HUM. VALUES 377, 390 (2004) ("[W]hile automakers were wary of accepting the responsibility of making vehicles more crashworthy in the 1960s, they were even more frightened of taking on the liability that would accompany their involvement in an air bag strategy."); *see also* Jameson M. Wetmore, *Delegating to the Automobile: Experimenting with Automotive Restraints in the 1970s*, 56 TECH. & CULTURE 440, 447 (2015) (quoting retired General Motors president: "I do feel that when you have a passive system the responsibility lies more with the manufacturer and the service station that takes care of the system.").

36. *See generally* Peter Norton, *Four Paradigms: Traffic Safety in the Twentieth-Century United States*, 56 TECH. & CULTURE 319 (2015).

The shift from "crash avoidance" through driver control to "crashworthiness" was part of an effort by safety advocates who sought to place greater responsibility for safety on the automobile industry and the automobiles they produced. The paradigm shift ushered in, or, as we would say, triggered, the move from active (e.g., seat belts) to passive (e.g., air bag) restraints. The explicit aim of safety advocates was to reallocate responsibility from the public, whose attitudes and behavior had proved quite resiliently ill-suited to prevent secondary impacts, to technology that could compensate for human failings. Passive restraints were viewed as a response to the moral failings of drivers and were intended to displace immoral human actors. While airbags would not become standard until the 1990s, this 1960s paradigm shift triggered an initial move towards their development. Shifting significant aspects of the safety function away from the human driver to a subsystem of the automobile was not merely a Handoff of functionality, but a reconfiguration of responsibility and potential liability for injuries. We now see further shifts emerging in the ethical relations of a vehicle to occupant, and the social relations of a vehicle system to the broader public.

Our Handoff analysis first examines the reconfiguration of components, from vehicle-plus-driver to the inclusion of additional infrastructural, computational, and communicating components, for each vehicle archetype to achieve functionally equivalent driving. We then explore how each set of reconfigurations produce ethical and political consequences associated with how those systems relate to, constrain, and define individual human components (often within the vehicle), as well as public spaces and their users.

III. AUTONOMOUS VEHICLE FUTURES

Applying the Handoff model to autonomous vehicles moves us beyond the idea of a gradual, linear transition of control from human to computational elements in service of producing a functionally equivalent artefact (i.e., a car) that performs a functionally equivalent task (i.e., driving). The SAE International Standards for vehicle automation, for instance, describe this trajectory from traditional human control, through partial automation such as automated lane-keeping and braking (Level 2), to vehicles capable of operating without humans under constrained conditions (Level 4), to a mythical (or military) fully automated vehicle capable of operating independently under any and all conditions (Level 5).[37] This stepwise model encourages us to think

37. *See* SAE INT'L, *supra* note 22, at 6, 33–34. Notably, the document divides the act of driving into three activities—strategic, tactical, and operational—and explains that the

about vehicles as discrete objects, whose only variable is degree of computational control. The SAE model suggests development along a linear trajectory, mapped with SAE automation levels, as technical and regulatory hurdles are gradually overcome.

But the reality is different. Our claim is that each level in the SAE standards, alongside tracking a level of automation and embodying different configurations of human and technical components, expresses an agenda serving the interests of different stakeholders with different implications for various political and ethical values.[38] In other words, while the SAE levels present the transformations along one dimension, from human driver control to computational control, they occlude the complex re-scripting of components and significant political and ethical dimensions of these transitions. Applying the Handoff analytic to autonomous vehicles is useful here because it directs us to think about these vehicles and the function they perform not only as objects and tasks, but as complex systems of human, digital, and physical infrastructure, with new and transformed components and consequences for politics and ethics. Accordingly, we address the technical formations of autonomous vehicles not in terms of stepwise progress in automation, but in terms of models or archetypes of deployment that represent different systemic visions of the future of autonomous driving.

It is not our intention, here, to expand and extend the scope of work on societal implications of human-driven and autonomous vehicles or to call it into question. Rather, the contribution of the Handoff model is a richer account of cause and effect. Frequently, too much is left out when proponents and critics assert that human-driven or driverless vehicles will result in this or that outcome, respectively, reifying it as a single progression. We give shape to the multiple dimensions of these technologies while we focus on impacts of reorganization and reconfiguration on ethical and political (i.e., societal) values, such as privacy, autonomy, responsibility, and distributions of property. The transition to autonomous vehicles generates consequences for those values

automation at issue in levels 1–5 is focused exclusively on the tactical and operational aspects of driving on the road. *See id.* Though the document acknowledges that strategic driving activities such as trip planning may be delegated to technical components, they are not reflected in the levels of driving automation.

38. Without taking a deterministic view of technology, we agree with Mumford that some material arrangements are better aligned with certain political aims then others. *See generally* Lewis Mumford, *Authoritarian and Democratic Technics*, 5 TECH. & CULTURE 1 (1964) (arguing that some material arrangements—man-centered, relatively weak, resourceful and durable, dispersed, and decentralized—were more aligned with democratic forms of governance while others—immensely powerful, inherently unstable, centralized—were more aligned with authoritarian forms).

that may not be immediately evident or are described without attention to the specific implementation of autonomous driving considered. This causes important parts of the account to disappear, which we attempt to resurface by exploring the specifics of the archetypes through the Handoff model.

A. ARCHETYPE 1: "DRIVER ASSIST"

One autonomous future retains "drivers" in drivers' seats in individually owned, increasingly automated passenger vehicles. This is often described in terms of Advanced Driver Assistance Systems (ADAS), and many vehicle manufacturers are pursuing these technologies in one form or another.[39] We call the archetype associated with this system of transport "driver assist." Driver assistance technologies typically use similar sensor arrays to fully "driverless" vehicles, often including Light Detection and Ranging (LIDAR) (although Tesla notoriously relies more on computer vision rather than LIDAR),[40] ultrasonic, radar, and video cameras for "computer vision."

The driver assist approach involves a dynamic control relationship, with a balance of autonomy, control, and responsibility distributed between a human driver and an autonomous system through an interface.[41] Central to this archetype are "control transitions" between technical and human actors, which are understood to be inevitably necessary in certain situations or contexts. The reliance on a human occupant[42] to engage, disengage, and respond to failures of the automation system means the controlling components and modes are markedly different from those found in fully driverless vehicles, discussed below.

Authors have sought to classify and build taxonomies for different types of control handovers, including: stepwise (e.g., first throttle then steering, etc.), driver monitored (e.g., driver has hands on wheel and a countdown happens), and system monitored (e.g., the vehicle decides when the human is ready to

39. *See, e.g.*, Kelsey Mays, *Which Cars Have Self-Driving Features for 2019?*, CARS.COM (May 22, 2019), https://www.cars.com/articles/which-cars-have-self-driving-features-for-2019-402645/.

40. *See* Kyle Field, *Tesla Achieved the Accuracy of Lidar with Its Advanced Computer Vision Tech*, CLEAN TECHNICA (Aug. 3, 2020), https://cleantechnica.com/2020/04/24/tesla-achieved-the-accuracy-of-lidar-with-its-advanced-computer-vision-tech/.

41. Natasha Merat & John D. Lee, *Preface to the Special Section on Human Factors and Automation in Vehicles: Designing Highly Automated Vehicles with Driver in Mind*, 64 HUM. FACTORS: J. HUM. FACTORS & ERGONOMICS SOC'Y 681, 684–85 (2012).

42. This occupant may be either a driver or a fallback-ready driver depending upon whether the car is engaged in some Dynamic Driving Task. SAE INT'L, *supra* note 22, at 7.

resume control).[43] Other categories include "structured" or "unstructured,"[44] as well as system or user-initiated.[45] Vehicles may also be able to alter how a handover is performed according to an assessment of the attention, capacities of the human driver, or activities taking place within the vehicle. Interfaces designed to enable control transitions may communicate via auditory, visual, mechanical, or haptic channels, or in combinations.[46] These modes of acting, including force and affordance, on the human occupant are intended to elicit human behavior, such as increased alertness or exercise of control. The goal is to generate a feedback loop between the vehicle and the human driver for the sake of ensuring the intentions of the user are safely executed.[47]

Models for transition and Handoff have been evolving rapidly in the automotive design and research communities. The SAE defines the transfer sequence for a handover of autonomous to manual control to have five phases: P0 Original autonomous driving mode; P1 Event condition state change; P2 Request issued; P3 Takeover response; and P4 Full handover.[48] When control transitions occur in the other direction, from manual to automated, the SAE defines four phases: P0 Original manual driving mode; P1 Automation available; P2 Automation enabled; and P3 Automation engaged.[49] However, Wintersberger, Green, and Riener[50] have proposed the following additional states for take-over requests as seen in Tables 1 and 2 below.

---

43. *See* Roderick McCall, Fintan McGee, Alexander Meschtscherjakov, Nicolas Louveton & Thomas Engel, *Towards a Taxonomy of Autonomous Vehicle Handover Situations*, PROC. 8TH INT'L CONF. ON AUTOMOTIVE USER INTERFACES & INTERACTIVE VEHICULAR APPLICATIONS 193, 196 (2016).

44. *See* Brian Mok, Mishel Johns, Key Jung Lee, David Miller, David Sirkin, Page Ive & Wendy Ju, *Emergency, Automation Off: Unstructured Transition Timing for Distracted Drivers of Automated Vehicles*, 2015 PROC. IEEE 18TH INT'L CONF. ON INTELLIGENT TRANSP. SYS. 2458, 2459, https://doi.org/10.1109/ITSC.2015.396.

45. Philipp Wintersberger, Paul Green & Andreas Reiner, *Am I Driving or Are You or Are We Both? A Taxonomy for Handover and Handback in Automated Driving*, PROC. 9TH INT'L DRIVING SYMP. ON HUM. FACTORS IN DRIVER ASSESSMENT, TRAINING & VEHICLE DESIGN 1, 3–4 (2017).

46. David Beattie, Lynne Baillie, Martin Halvey & Rod McCall, *What's Around the Corner? Enhancing Driver Awareness in Autonomous Vehicles via In-Vehicle Spatial Auditory Displays*, PROC. 8TH NORDIC CONF. ON HUM.-COMPUTER INTERACTION 189, 191 (2014), https://dl.acm.org/citation.cfm?id=2641206.

47. Evangeline Pollard, Philippe Morignot & Fawzi Nashashibi, *An Ontology-Based Model to Determine the Automation Level of an Automated Vehicle for Co-Driving*, PROC. 16TH INT'L CONF. ON INFO. FUSION 596, 596–97 (2013), https://ieeexplore.ieee.org/document/6641334.

48. *See* SAE INT'L, SURFACE VEHICLE INFORMATION REPORT: HUMAN FACTORS DEFINITIONS FOR AUTOMATED DRIVING AND RELATED RESEARCH TOPICS 18 (2016), https://www.sae.org/standards/content/j3114_201612/.

49. *See id.* at 20.

50. Wintersberger et al., *supra* note 45, at 3–4.

Table 1: Handover Taxonomy (SAE 3114 Phases on the Bottom, Additional Phases on Top)

Transfer Control Sequence AD to Manual Control		Request Issued			Take-Over Response	Full Handover
	Preparation Scheduled TOR	Perception	Suspension	Sufficient TOR		
Cognitive		Perceive Request to Intervene	Cognitive Suspension of Side Activity	Road Fixation	Control Transition Function	Situation Awareness
Physical			Physical Suspension of Side Activity	Hands on Wheel Foot on Pedal		Longitudinal / Lateral Vehicle Stability
System	Detect Request to Intervene	Prepare Request Driver State Assessment, Workload Management	Detect Request Perception	Adaption of Interfaces & Information Systems	Detection of Motor Readiness	Measure Driving Performance and Situation Awareness
P0	P1		P2		P3	P4

Table 2: Handback Taxonomy (SAE 3114 Phases on the Bottom, Additional Phases on Top)

Transfer Control Sequence Manual to AD Control	Automation available	Automation enabled	Automation engaged		Full Handback
	Initialization			Handback	Reengagement
Cognitive		Decision to Activate Automation	Control Transition Function	Cognitive Suspension of Driving Task	Cognitive Reengagement in Secondary Task
Physical		Enable Automation	Set Automation to Active State	Physical Suspension of Driving Task	Physical Reengagement in Secondary Task
System	Detect Availability of Automation	Driver State Assessment	Detect Imminent Need to Activate Automation	Secondary Task Suggestions, Explanation of Transition Reason	Adaption of Interface and In-Vehicle Information System
P0	P1	P2	P3		

The augmented transition sequences proposed in these frameworks do a better job of taking into account the different cognitive and physical steps the user needs to transition through.

1. Interfaces

As these taxonomies make clear, effective control transitions require extremely complex informational interactions between technical and human actors. Timing and clarity of communications affect human capacities to regain control and situational awareness within time to navigate the obstacle.[51] This

51. *See, e.g.*, Brian Ka-Jun Mok, Mishel Johns, Key Jung Lee, Hillary Page Ive, David Miller & Wendy Ju, *Timing of Unstructured Transitions in Automated Driving*, 2015 PROC. IEEE INTELLIGENT VEHICLES SYMP. 1167, https://doi.org/10.1109/IVS.2015.7225841; Brian Mok, Mishel Johns, David Miller & Wendy Ju, *Tunneled In: Drivers with Active Secondary Tasks Need More Time to Transition from Automation*, PROC. 2017 CHI CONF. ON HUM. FACTORS IN COMPUTING SYS. 2840, https://doi.org/10.1145/3025453.3025713 (discussing controlled

raises questions as to how much engagement between the user and vehicle is necessary during routine computer-controlled driving. To what degree is, or *should*, the user be included in the control loop? And what differences in politics and values do respective decisions embody? Authors have commented that "finding the right balance between requiring the human to be ready to intervene at a moment's notice and realizing the benefits of this technology is likely to be a challenge."[52] Indeed, the practical dimension of these transitions is a topic of continuing research, with many questions still unresolved such as:

> In switching to an automated mode, how and when does the vehicle communicate to the driver the tasks for which the system is now responsible? To what extent is the driver monitored to ensure that they are sufficiently engaged with the driving task when the vehicle has control (Eye tracking? One hand on steering wheel?)? How long does the distracted or sleeping driver need to achieve sufficient awareness of the driving situation such that they can safely re-engage with the driving task? What information and cueing mechanisms will be most effective in managing this process? How does the vehicle manage if the driver is unable or refuses to resume control? In returning control to the driver, does the vehicle always return to full manual control (no automation) or does the vehicle step down through automation levels gradually?[53]

Answers to the questions posed above not only implicate safety and enjoyment but also other values. Depending on the various possible triggers for a control transition to occur and the different modes by which the vehicle acts on or engages the human driver—by force or affordance—the human driver occupies a different role in the control loop that also conditions their autonomy, privacy, and responsibility. For example, a vehicle may be compelled to drive when the human driver cannot react fast enough or is drunk, asleep, or otherwise impaired; a human, although not necessarily the human driver occupant, may need to drive, such as with teleoperation or mobility management, in complex situations like driving through a flood or crowd;[54] or a human driver may choose to remain in control for enjoyment

human participant experiments showing that timing of transition warnings and accounting for driver distraction can improve take-over response time); Mok et al., *supra* note 44.

52. JAMES M. ANDERSON, NIDHI KALRA, KARLYN D. STANLEY, PAUL SORENSON, CONSTANTINE SAMARAS & OLUWATOBI A. OLUWATOLA, AUTONOMOUS VEHICLE TECHNOLOGY: A GUIDE FOR POLICY MAKERS 68 (2016).

53. Michael Fisher, Nick Reed & Joseph Savirimuthu, *Misplaced Trust?*, ENGINEERING & TECH. REF. (2015), https://doi.org/10.1049/etr.2014.0054.

54. David Miller, Mishel Johns, Hillary Ive, Nikhil Gowda, David Sirkin, Srinath Sibi, Brian Mok, Sudipto Aich & Wendy Ju, *Exploring Transitional Automated Driving with New and Old*

even when a car is capable of autonomous driving.[55] These each affect the roles of human occupants and their understanding of respective tasks and responsibilities within the system.

With respect to the information transmitted through the interface to the human occupant, if there is no emergency danger, how much information about the surroundings and possible future risks should the vehicle communicate to the human occupant? Does the amount of information transmitted differ when the human is driving or merely supervising? Interfaces might only show sufficient information to demonstrate that the automated system is making clear and correct decisions, making the human occupant more confident in a supervisory role rather than driving. However, does this affect the human's autonomy? Would it be better for the vehicle to communicate in richer detail all of the possible risks and dangers? That might make the task of supervising a vehicle as onerous as actively driving. However, the alternative is for a human to risk not having all the information necessary to decide whether to initiate a control transition or actively drive.

A related question is whether the vehicle ought to demand the human occupant's attention in moderately risky situations, which may lead to habituation, or whether it should hail the human occupant only in clear emergencies. Considering that human attention remains a limited resource even when freed from the driving task, these questions about shifting control authority need to be addressed in situations where in-vehicle attention is focused on other activities, including some alternatives that are provided by the vehicle itself. In the real world, addressing these questions become even more complex because any given vehicle design script and interface must contend with information and control authority flowing not only among humans, software, and hardware, but with a diverse set of stakeholders, including software, hardware, and component vendors as well as traditional vehicle manufacturers.[56]

Further, users are known to appropriate technology in unanticipated ways—for example, using car batteries and mosquito nets for fishing rather than energy or malaria prevention. The ability to envision the divergent scripts users may enact in lieu of those imagined by the manufacturer or regulator can be further complicated when technologies can be combined. For instance, if

Drivers, 2016 PROC. SAE 2016 WORLD CONGRESS & EXHIBITION 2, https://doi.org/10.4271/2016-01-1442; Mok et al., *supra* note 44, at 2458.

55. Brian Mok, Mishel Johns, Nikhil Gowda, Srinath Sibi & Wendy Ju, *Take the Wheel: Effects of Available Modalities on Driver Intervention*, 2016 PROC. 2016 IEEE INTELLIGENT VEHICLES SYMP. 1358, 1358.

56. Akrich, *supra* note 7, at 205.

the driving control software—or some component of it—is an after-market device brought-in by the user, the manufacturer may not have accounted or allowed for the ways in which it may shift performance or user expectations. We caught a glimpse into the complexity of safety in autonomous driving with the Uber fatality; the "safety driver" was castigated for using a personal device at the time of the accident,[57] revealing a confused expectation that users would routinely be performing tasks other than supervising driving yet be on the hook to assume control quickly when circumstances so demand.

As legal and regulatory rules slowly stabilize, they will influence technical configurations. Further, road rules and insurer calculations will affect what tasks a human "driver," "owner," or "user" can or must perform at any particular time and the role we will expect vehicles themselves to play in enforcing desired conduct. Addressing the challenges of safe transitions of control[58] to inform interface design as well as regulatory prescriptions will require a nuanced concept of responsibility.

Assigning responsibility is particularly challenging where vehicle configurations participate in the moral conditioning of the user. While the law controls the conduct of a vehicle operator in one way, over time, control over human conduct has increasingly been delegated to vehicle systems themselves. For instance, vehicles use affordances like irritating beeping when a seatbelt is not engaged or when speed limits are exceeded, and can compel compliance by disabling an engine with an interlock device if a driver is intoxicated.[59] The way in which a vehicle grooms user conduct in the driver assist vehicle model may be radically different, however, involving real-time surveillance and behavior analysis, and triggering different vehicle responses according to situational, environmental, or other contexts. For instance, how a driver physically appears, or other non-driving behaviors like expressions of fatigue or anger, may become modes of engaging with the control system or triggers for additional information flows. Enhanced surveillance is integral to this archetype, as it allows the vehicle—or manufacturer or other provider of the assistive driving technology—to assess the extent to which the *human actor* is

57. *See* NAT'L TRANSP. SAFETY BD., PRELIMINARY REPORT: HIGHWAY HWY18MH010 3 (2018), https://www.ntsb.gov/investigations/AccidentReports/Reports/HWY18MH010-prelim.pdf.

58. *See* Helen Nissenbaum, *Accountability in a Computerized Society*, 2 SCI. & ENGINEERING ETHICS 25 (1996).

59. Bruno Latour, *Where Are the Missing Masses? The Sociology of a Few Mundane Artifacts*, *in* SHAPING TECHNOLOGY/BUILDING SOCIETY: STUDIES IN SOCIOTECHNICAL CHANGE 151, 168 (Weibe E. Bijker & John Law eds., 1992).

performing to the script.[60] Such monitoring is viewed as particularly important in detecting and countering misuse or abuse.[61]

In the driver assist archetype, information collected about the behavior of human and technical actors, primarily to support performance and safety, may secondarily flow to law enforcement for the sake of road rules compliance or to insurers for the sake of liability apportionment.[62] If vehicle manufacturers are presumed *prima facie* responsible for accidents when cars are in autonomous mode under a products liability rather than personal liability approach,[63] they may also desire fine-grained recording of in-cabin behavior during control transitions such that they would be able to subsequently pursue human drivers for negligence. Some authors have described the ways such technical systems condition user behavior as their "moral content."[64] The privacy issues associated with driver assist style vehicles are thus less defined by the commercial norms we might see in fully driverless cars, and more associated with increased policing and road enforcement and a potentially antagonistic relationship between drivers and vehicle manufacturers, as mediated by insurers.

The degree of connectivity between vehicles and vehicle manufacturers or other actors may depend on similar considerations. While autonomous driving modes in driver assist cars may not *require* web connectivity, certain manufacturers do collect different types of data, usually telematics data, when automated modes are enabled.[65] Other manufacturers, like Tesla, are gathering data from vehicle sensors irrespective of driving mode and have provided that data to law enforcement.[66] These issues are not necessarily new. For instance, seatbelt sensors participate in the control environment in non-automated vehicles. "Black box" and telemetry data, as well as dash cam footage, have

60. SAE INT'L, *supra* note 22, at 13.

61. *Id.*

62. *See, e.g.*, Belinda Bennett, Jane Evelyn & Bridget Wier, *Driving into New Frontiers? Data and Driverless Cars*, 2019 UNSW L.J.F. 1, 12; Sarah Aue Palodichuk, *Driving into the Digital Age: How SDVs Will Change the Law and Its Enforcement*, 16 MINN. J.L. SCI. & TECH. 827, 834 (2015).

63. *See, e.g.*, Kenneth S. Abraham & Robert L. Rabin, *Automated Vehicles and Manufacturer Responsibility for Accidents: A New Legal Regime for a New Era*, 105 VA. L. REV. 127, 139 (2019); Stefan Clause, Nicholas Silk & Chris Wiltshire, Bank of Eng. Gen. Ins. Div., *Potential Impacts of Autonomous Vehicles on the UK Insurance Sector*, Q. BULL., 2017 Q1, at 40, 45, https://www.actuaries.org.uk/system/files/field/document/A3%20Supporting%20paper.pdf.

64. Akrich, *supra* note 7, at 219.

65. Julia Orlovska, Casper Wickman & Rikard Soderberg, *The Use of Vehicle Data in ADAS Development, Verification and Follow-up on the System*, 2020 PROC. DESIGN SOC'Y: DESIGN CONF. 2551, 2554.

66. Stefan Jacobs, *Berliner Polizei Greift Immer Härter Gegen Raser Durch*, DER TAGESSPIEGEL (Feb. 25, 2019, 8:18 AM), https://www.tagesspiegel.de/berlin/illegale-autorennen-berliner-polizei-greift-immer-haerter-gegen-raser-durch/24033226.html.

long been used in insurance litigation. However, these practices have the potential to evolve in scale under the driver assist model, and the norms around information flow are unclear, especially between the human user and the vehicle manufacturer or service provider.

2. Responsibility and Autonomy

Private vehicle ownership, as preferred in the driver assist archetype, also introduces new responsibilities that seem analogous to those associated with contemporary, non-automated vehicle ownership. For instance, maintenance for autonomous vehicles might require the installation of software or firmware updates.[67] On the one hand, a "user" may be responsible for ensuring that the "driver" is performing at its highest capacity (i.e., using the latest version of its software), in the same way that a person is responsible for the maintenance of a vehicle. On the other, responsibility for the safety of software updates, as well as transparency of features added or removed, may also fall on the manufacturers. Satisfying manufacturer responsibility may require executing updates, irrespective of user knowledge or desire, in turn challenging the scope of owner autonomy analogously with other "tethered" goods.[68] Compelling users to update software may affect consumer rights. With current devices, for example, the choice of whether or not to update an operating system may depend on numerous factors including an assessment of whether the device is powerful enough to run that updated software. It might be necessary however, to remove that consumer choice for the sake of ensuring greater safety for the general public. These choices about what level of engagement with the computational capacities of a vehicle are permitted, encouraged, or obliged affect user autonomy and agency.[69]

ADAS used in driver assist cars reportedly cause drivers to report a loss of control over vehicles, and therefore, potentially, a sense that autonomy has been curtailed.[70] Research also suggests that "user experience" and "user

67. *See, e.g.*, Automated and Electric Vehicles Act, 2018, c. 18, § 4 (Eng.).

68. Chris Jay Hoofnagle, Aniket Kesari & Aaron Perzanowski, *The Tethered Economy*, 87 GEO. WASH. L. REV. 783, 829 (2019).

69. For an overview of the pros and cons of over-the-air software updates in the automotive context, see Dierdre K. Mulligan & Kenneth A. Bamberger, *Public Values, Private Infrastructure and the Internet of Things: The Case of Automobiles*, 9 J.L. & ECON. REG. 7, 7 (2016). For a description of the potential for the security-necessary, over-the-air updates to compromise security, limit competition, and undermine consumer protections and privacy, as well as the need for regulations to address, see *id.* at 20–26.

70. Sven Kraus, Matthias Althoff, Bernd Heissing & Martin Buss, *Cognition and Emotion in Autonomous Cars*, 2009 PROC. 2009 IEEE INTELLIGENT VEHICLES SYMP.; Alexander Meschtscherjakov, Manfred Tscheligi, Dalila Szostak, Rabindra Ratan, Roderick McCall,

acceptance" are at their highest with limited levels of vehicle automation.[71] Measuring autonomy means asking what the interface permits or prohibits and why. The interface of a prestige car, focused on comfort or driving "feel," may be engineered to produce perceptions of control and support for driver intentions.[72] In a ride-sourcing service, by contrast, it may focus on customer experience. In a logistics vehicle such as a long-haul truck, the focus may be efficiency and worker discipline.[73] These agendas will define what inputs from the human are desirable or necessary and the ways in which their behaviors are integrated into the control system. The autonomy question for human drivers in this scenario is thus determined by the capacity and compulsion to perform control inputs, as defined by the triggers and modes of the control feedback loop, but those elements are themselves dependent on broader purposes as well as commercial, political, and regulatory considerations.

Ioannis Politis & Sven Krome, *Experiencing Autonomous Vehicles: Crossing the Boundaries Between a Drive and a Ride*, 2015 PROC. 33RD ANN. ACM CONF. EXTENDED ABSTRACTS ON HUM. FACTORS IN COMPUTING SYS. 2413, 2414, https://doi.org/10.1145/2702613.2702661.

71. *See* Christina Rödel, Susanne Stadler, Alexander Meschtscherjakov & Manfred Tscheligi, *Towards Autonomous Cars: The Effect of Autonomy Levels on Acceptance and User Experience*, 2014 PROC. 6TH INT'L CONF. ON AUTOMOTIVE USER INTERFACES & INTERACTIVE VEHICULAR APPLICATION 1, 8, https://doi.org/10.1145/2667317.2667330.

72. Fisher, *supra* note 53.

73. Karen E. C. Levy, *The Contexts of Control: Information, Power, and Truck-Driving Work*, 31 INFO. SOC'Y 160, 161 (2015).

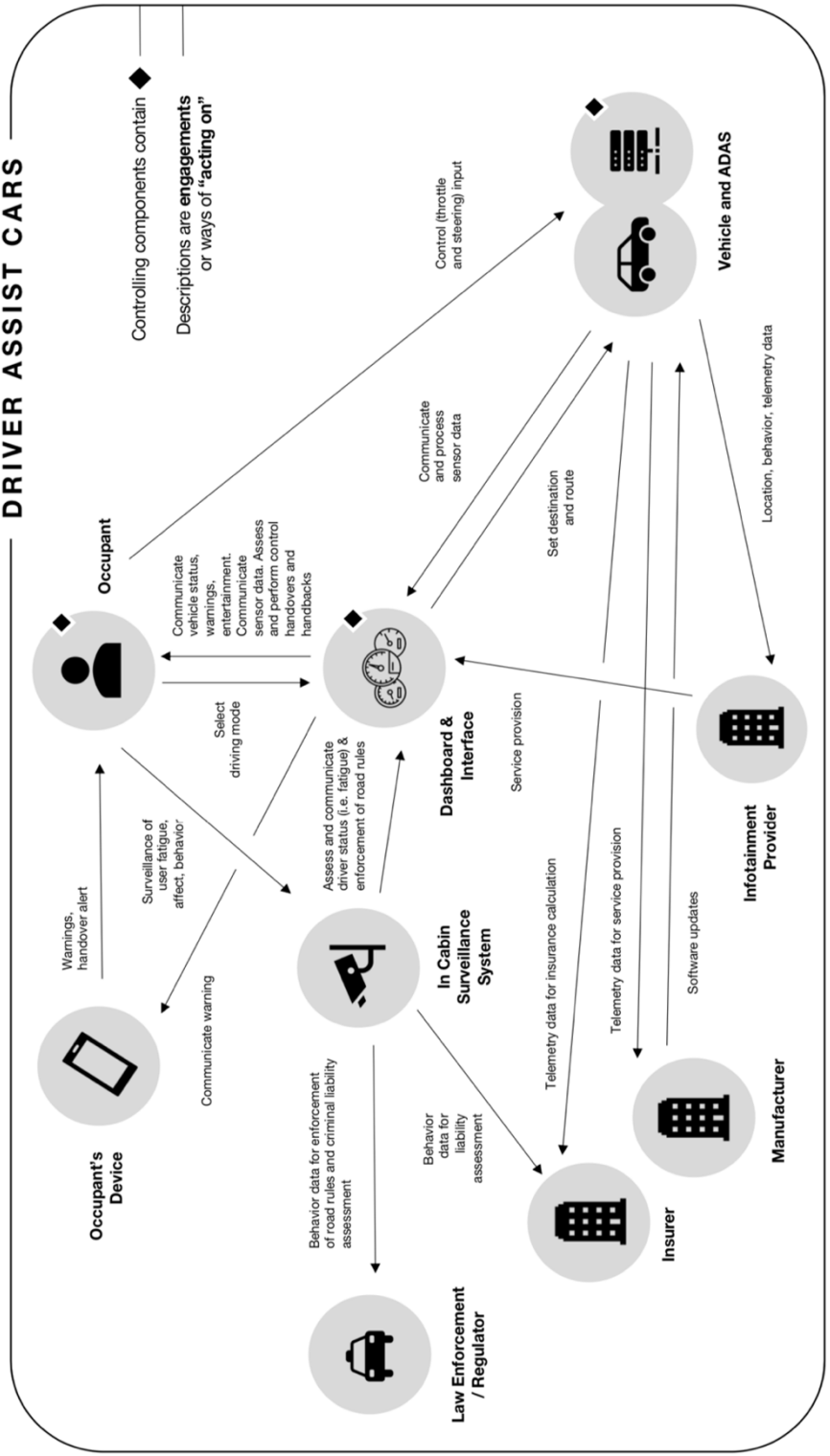


Figure 1: Distribution of Components in Driver Assist Cars

B. ARCHETYPE 2: "DRIVERLESS CAR"

For some, the fully driverless vision of autonomous transport is the best approach to capturing the economic and social benefits of autonomous vehicles.[74] Indeed in the taxonomy laid out in the SAE document, fully driverless (Level 5) is the culmination of successive developmental stages.[75] With a fully driverless car, "occupants" (i.e., "users" or "passengers," but not "drivers") would use travel time for non-driving activities with no obligation to pay attention to the road or vehicle controls. Such vehicles typically require legislative fiat, which only a few jurisdictions have provided so far.[76] Some states have created regulatory frameworks to allow such vehicles to be tested.[77] Several laws, however, are being debated (or at least proposed) that go further and enable the sale and use of vehicles without traditional vehicle controls of steering wheels and pedals.[78] This change goes beyond allowing vehicle occupants not to *have* to drive; without controls, they *cannot* drive. The critical change to the vehicle interface in this configuration is the absence of direct controls and the introduction of rich systems of information exchange between human occupants and the entities controlling the carriage of the vehicles (i.e., "operators").[79] As previously mentioned, in the near future the high cost of sensing and computational apparatus necessary for operating these vehicles will likely restrict their usage to "mobility services." Those TNCs might be privately, publicly, or communally operated, or they may be privately-owned and fleet-managed passenger vehicles.

The Waymo Chrysler Pacifica mini-van offers a useful demonstration of the driverless car control distribution designed for commercial ride-hailing.

---

74. *See, e.g.*, Hideaki Tomita, *Awaiting the Realization of Fully Autonomous Vehicles: Potential Economic Effects and the Need for a New Economic and Social Design*, VOX EU (Dec. 17, 2017), https://voxeu.org/article/potential-economic-and-social-effects-driverless-cars.

75. *See* SAE INT'L, *supra* note 22, at 23.

76. *See, e.g.*, AV START Act, S. 1885, 115th Cong. (2017); SELF DRIVE Act, H.R. 3388, 115th Cong. (2017); U.S. DEP'T OF TRANSP., THE ROAD AHEAD: NHTSA STRATEGIC PLAN 2016-2020, at 24–26 (2016).

77. *See, e.g.*, Autonomous Vehicles/Self-Driving Vehicles Enacted Legislation, NAT'L CONF. ST. LEGISLATORS, https://www.ncsl.org/research/transportation/autonomous-vehicles-self-driving-vehicles-enacted-legislation.aspx (last visited July 30, 2020).

78. *See, e.g.*, CAL. VEH. CODE § 38756 (West 2019) (repealed 2018); CAL. VEH. CODE § 38756 (West 2019) (repealed 2020).

79. The SAE term is "driverless operation dispatcher." SAE INT'L, *supra* note 22, at 17. This role is distinct from the "remote driver" who, while not seated in a position to "manually exercise in-vehicle braking, accelerating, steering, and transmission gear selection input devices (if any)," can operate the vehicle. *Id.* at 16. These roles are functional; thus, a driverless operation dispatcher may become a remote driver if they have the means to operate the vehicle remotely. *Id.*

These vehicles still retain traditional vehicle controls (and "safety drivers" for now), but nonetheless demonstrate the trajectory of this transport vision. When the in-car controls are not engaged, the driving function in these vehicles is displaced to a combination hardware and software control system that Waymo calls the "the world's most experienced driver."[80] A closer look at the interfaces and what they facilitate, however, exposes some of the other components and modes of acting embedded in this control Handoff. In the Waymo Chrysler, there is a digital screen for each back-seat passenger providing a bird's eye view (i.e., top-down view with the vehicle in the center) real-time map showing the environment as detected in relatively low resolution, coupled with pulsing higher-resolution images (of still relatively indecipherable dot representations of the physical environment generated from LIDAR sensors). There is also a mechanical interface for back seat occupants, with three buttons: "start ride," "pull over," and "help."[81]

These in-car controls are coupled with the Waymo One App for smartphones, which operates in a similar manner to other commercial ride-sourcing services. Destinations are input,[82] prices are agreed-upon, and feedback is provided following the common model of star ratings and selected responses such as "good route choice" and "clean car" (although "friendly driver" is probably no longer an option). All three interfaces—in-seat, mechanical, and the app—give a "support" option, where an occupant can contact a Waymo employee, likely situated in a control or service center, who can offer guidance on *using* (but not "driving")[83] the vehicle (e.g., instructing users on how to change destinations). This "support" component can both assist the driver to give further input into the driving system as well as direct the driving system itself by resetting the destination.

The fully driverless car archetype typically imagines a car travelling on existing roadways, capable of moving from destination to destination relying only on on-board sensing and computational apparatuses. This mode of autonomous transport developed out of the U.S. Defense Advanced Research Projects Agency (DARPA) autonomous vehicle Grand Challenge, beginning

80. WAYMO, https://waymo.com (last visited Sept. 1, 2020).

81. For information about the Waymo Chrysler Pacifica, see WAYMO PRESS, https://waymo.com/press/ (last visited Sept. 1, 2020); Hawkins, *supra* note 3.

82. This is an example of the strategic, user-determined aspects of driving that are excluded from the automation paradigms of the SAE. SAE INT'L, *supra* note 22, at 6.

83. The SAE coined the term "Dynamic Driving Task" to describe "[a]ll of the real-time operational and tactical functions required to operate a vehicle in on-road traffic . . . " and to limit which "driving" tasks are automated under the various levels of automation they define. SAE INT'L, *supra* note 22, at 6 (emphasis omitted). Again, the definition excludes "the strategic functions such as trip scheduling and selection of destinations and waypoints." *Id.*

in 2004, which expressed the goal of accelerating the "development of autonomous vehicle technologies that could be applied to military requirements."[84] That military pedigree meant autonomous vehicle technology would need to be self-reliant, operating in unknown and hostile environments, with potentially limited communications. Such self-sufficiency in a more civilian context might imply a type of independent or even libertarian politics embedded in the mode of vehicle operation, in that it gives near total decision-making power and control to the discrete vehicular unit. That account may not, however, adequately capture the more nuanced political consequences, or consequences for human values, when implementing such vehicles in the real world, or at least in an urban environment. Deploying fully autonomous vehicles in urban spaces necessitates more complex information flows and controlling components shaped by material and commercial realities.

Consider the multiple situations in which a vehicle in urban use cannot rely on autonomous control alone, such as equipment malfunction, unexpected road blockages, natural disasters, etc. It is unlikely that a vehicle could operate in an unpredictable environment without at least some human control input, one way or another. Commercial realities further suggest the use of these vehicles will be so conditioned by respective business models as to make a complete delegation of control to the vehicle itself unlikely. These contingencies might muddy the driverless car archetype; nevertheless, they are the working realities of a driverless vehicle model once its "users" (e.g., individual users and businesses operating the vehicles) are taken into account. We maintain that envisioning how a driverless vehicle actually operates in the world reveals many of its political and ethical consequences.

For a start, it is necessary to widen the lens and acknowledge other controlling actors or components, beyond the "occupant," "operator," or software control system, that are essential to the functioning driverless vehicles. Rarely acknowledged, they are necessary accomplices when the capacity to control a vehicle is removed from its occupants. This setup shares elements with the connected car archetype, discussed next, which in some versions also denies control to the vehicle occupant. The driverless archetype, however, is premised on interventions that control vehicles one-at-a-time, rather than distributing control across a variety of infrastructural systems. Further, in the driverless archetype, these are primarily supplemental control components used for error recovery, rather than structural dependencies for

84. *The Grand Challenge*, DEF. ADVANCED RES. PROJECTS AGENCY, https://www.darpa.mil/about-us/timeline/-grand-challenge-for-autonomous-vehicles (last visited Sept. 1, 2020).

networked distributed control of vehicles that are more integral to connected cars.

It is worth returning to a point made about driver-assist in the real world, namely the interdependencies between design choices and factors such as assumed purposes, material contingencies, and business drivers. We recall, therefore, that DARPA may have envisioned self-reliant vehicles because of the limited communications infrastructures and complex environments they might inhabit. By contrast, a domestic, urban environment offers infrastructures that are more reliable and, potentially, programmable. Regulators seem keen to exploit these infrastructures to define the functionality of driverless cars. For example, pilot tests of driverless vehicles with supervision by remote operators typically require a communications link that can provide information on the vehicle's location and status and supports two-way communication between the occupants and operators.[85] Thus, even driverless vehicles depend upon external infrastructure for political reasons, as well as technical.

Vehicle manufacturer Nissan's development of new controllers, interfaces, and modes of acting for their driverless vehicle control systems offers an example. Their "Seamless Autonomous Mobility" system uses a central control room with human "mobility managers"[86] who can intervene in vehicle control when facing complex obstacles.[87] This relocates an element of the driving interface to a remote location and to a remote person, who makes decisions about vehicle operation. From the promotional material available, however, the interface does not resemble a traditional vehicle interface—i.e., it is not a vehicle driving simulator—but rather it is a mapping system, where new routes can be plotted and then delivered to the vehicle for execution through its own driving software.[88] Thus the interfaces' affordances appear to support the "strategic" aspects of driving specifically cabined off from the "Dynamic Driving Tasks" assigned to vehicles in the SAE taxonomy[89] (the in-

85. *See, e.g.*, CAL. CODE REGS. tit. 13, § 227.38(b)(1) (2018).

86. *See, e.g.*, Lawrie Jones, *Driverless Cars: When and Where?*, ENGINEERING & TECH. MAG. 36 (Mar. 2017); *Seamless Autonomous Mobility*, NISSAN MOTOR CORP., https://www.nissanglobal.com/EN/TECHNOLOGY/OVERVIEW/sam.html (last visited July 30, 2020).

87. These human components fit the category of "(DDT) Fallback-Ready Users"; they are prepared to take on driving tasks if a Level 3 vehicle requests it or if there is evidence of need. When they take over the operational and tactical tasks, these human components become Remote Drivers. SAE INT'L, *supra* note 22, at 17.

88. *See, e.g.*, NISSAN MOTOR CORP., *supra* note 86.

89. SAE INT'L, *supra* note 22, at 6–7 (describing Dynamic Driving Tasks differently automated under the SAE 5-level system as "the real-time operational and tactical functions

the-moment, on-road tasks being thrown, or taken, back by the human). For instance, mobility managers draw a path on a digital map using a regular computer interface (i.e., a mouse). Thus, the human acts on the driving system by determining the route—an informational input—and the software control system on the vehicle translates that informational input and acts on other technical components of the vehicle to follow those directions. Mobility managers are typically engaged when a vehicle encounters an obstacle that it cannot negotiate, i.e., when the vehicle is stationary, rather than an emergency situation.

There are also other forms of remote controllers. Companies like Phantom Auto, for instance, are building a way for autonomous vehicles to be controlled by humans in remote locations using vehicle simulators.[90] These people are not billed as "drivers," but rather as "teleoperators." (Although the job position advertised on their website is for a Class A Driver & Remote Operator.)[91] In this situation, the system affordances allow a teleoperator to assume the controlling function of the vehicle rather than, as in the "mobility manager" example, a source of information to trigger action from the on-board computational controlling components. These two alternative interfaces invite different understandings of the human actors' relationship to the technical actors.

Differences in remote approaches highlight questions about what constitutes "driving" in these systems. They employ different ways to distribute control to new "components," different identities for those new components, different configurations of control across components, different interfaces, and different modes of acting enabled by those interfaces. Importantly, these interfaces invite human actors to visualize their roles in distinct ways. The bird's-eye view offered by the Nissan SAM system foregrounds planning and management, distancing the remote human actor from the lived experiences of the vehicles' human occupants. The Phantom Auto system in contrast foregrounds the operational and tactical aspects of driving. In doing so, it aligns the remote operator more closely with the lived experience of the vehicle's occupants. The interface designs place the remote

required to operate a vehicle in on-road traffic, excluding the strategic functions such as trip scheduling and selection of destinations and waypoints . . . .") (emphasis omitted).

90. Alex Davies, *Self-Driving Cars Have a Secret Weapon: Remote Control*, WIRED (Feb. 1, 2018, 7:00 AM), https://www.wired.com/story/phantom-teleops/.

91. *See Current Openings*, PHANTOM AUTO, https://phantom.auto/careers/?gh_jid=4073694002 (last visited June 4, 2020). This is unsurprising as regulations that allow pilot tests of such cars require remote operators/DDT fallback-ready drivers to have the proper class of license for the vehicle they operate and undergo manufacturer designed safety training. *See* CAL. CODE REGS. tit. 13 § 227.38(f) (2018).

human actors in scripts with different valences that influence the way they view their respective tasks and make ethically relevant decisions. Finally, requirements of the systems bring new players into the mix, with their own political stakes and incentives. For example, the Phantom Auto system (unlike the Nissan SAM system) requires zero-latency video transmission, which, if technically possible, could also provide a huge financial boon for telecommunications providers, over whose networks that data will flow. This technical requirement may shift the politics in unpredictable ways, including importing structural antitrust questions where mobility providers are also invested in telecommunications infrastructure.

1. Business Models and Ownership

The relationship between control, technical configuration, and business model cannot be overstated. For example, one critical difference between the two outsourced control options described above is that the Phantom Auto system requires a remote driver to operate one vehicle at a time. On the other hand, the Nissan SAM interface, while still requiring individual attention, positions a mobility manager more as a fleet manager or dispatch operator. If these become paid services, then they will likely service or facilitate different ownership models for autonomous vehicles. One appears more amenable to infrequent interventions associated with small-scale individual ownership, e.g., with personally owned cars being used on TNC platforms, whereas the other might be more suited to mobility-as-a-service arrangements, or fleet ownership and operation as a TNC. Those ownership models, and their implications for responsibility and control of vehicles, are deeply bound to system design. A fleet ownership model allows for centralized control and responsibility, sharing of and trust in collected information. Concentrated ownership of vehicles allows for greater investment per car as well as for some sensing and computation to be performed in the cloud by a central provider. Ownership and control of autonomous vehicles by a central entity also enables coordinated action such as platooning or other behaviors that take advantage of economies of scale such as calculated vehicle positioning for ride-sourcing, which is not possible, or at least more difficult (i.e., requires using "surge pricing" to incentivize), when individual sub-contractors possess and operate their own vehicles. On the other hand, non-fleet control models might prefer to distribute greater autonomy and control to each vehicle on the roadway. This may also elevate vehicle price because of the additional sensing and computation required. These systems lend themselves to different business cases, while the capital investment required still marginalizes the appeal of fully driverless cars to individual private owners.

At this stage, the leading players in driverless vehicles appear to be large technology companies interested in ride-sourcing, which demonstrates a likely business case and ownership configuration for this archetype moving forward. That said, recognizing the commercial complexity of vehicle manufacturing, these companies also seem ready to partner with vehicle Original Equipment Manufacturers (OEMs). Waymo is not, of course, the only entity exploring fully driverless cars for ride-hailing.[92] Uber has also been experimenting with these vehicles and has partnered with Toyota.[93] Lyft has a partnership with tech company Aptiv, which has a fleet of BMW cars (that include manual controls), operating on a small number of "routes."[94] Lyft also received a $500 million investment from General Motors in 2016,[95] indicating the possibility that General Motors may manufacture vehicles for autonomous ride-sourcing, or that General Motors is becoming a ride-sourcing business. General Motors has also acquired a driverless car company, Cruise, which is, for instance, building a driverless vehicle for Honda.[96] Clearly, companies are adopting new, different, complex positions in the autonomous vehicle ecosystem, which involves new roles for manufacturers, service providers, and platform operators.

Close attention to those complex manufacturing arrangements and business models highlights additional consequences for the property distributions and ownership dimensions of transport services, as well as the tendency towards de-integration of vehicle hardware and control software. Instead of building fully integrated autonomous vehicles, it is possible companies like Uber or Waymo would prefer to build autonomous driving

92. As of July 31, 2020, only three companies have permits to test cars without onboard drivers in California: Waymo LLC, Nuro Inc., and AutoX Technologies Inc. *Permit Holders (Driverless Testing)*, CAL. DEP'T MOTOR VEHICLES, https://www.dmv.ca.gov/portal/dmv/detail/vr/autonomous/driverlesstestingpermits (last visited Sept. 1, 2020).

93. *See, e.g.*, Eric Meyhofer, *Uber and Toyota Team Up on Self-Driving Cars*, UBER NEWSROOM (Aug. 27, 2018), https://www.uber.com/newsroom/uber-toyota-team-self-driving-cars/.

94. Kyle Wiggers, *Aptiv's Self-Driving Cars Have Given Lyft Passengers Over 100,000 Rides*, VENTURE BEAT (Feb. 11, 2020, 3:00 AM), https://venturebeat.com/2020/02/11/aptivs-self-driving-cars-have-given-lyft-passengers-over-100000-rides/.

95. Steve Trousdale, *GM Invests $500 Million in Lyft, Sets Out Self-Driving Car Partnership*, REUTERS (Jan. 5, 2016, 1:04 AM), https://www.reuters.com/article/us-gm-lyft-investment/gm-invests-500-million-in-lyft-sets-out-self-driving-car-partnership-idUSKBN0UI1A820160105.

96. Andrew J. Hawkins, *GM's Cruise Will Get $2.75 Billion from Honda to Build a New Self-Driving Car*, THE VERGE (Oct. 3, 2018, 8:51 AM), https://www.theverge.com/2018/10/3/17931786/gm-cruise-honda-investment-self-driving-car.

software "platforms" to be installed in driverless vehicles built by OEMs.[97] Accordingly, even if such driverless cars were individually owned, it is difficult to imagine autonomous vehicle ownership as approximating traditional vehicle ownership. As the functions of mobility managing and error correction demonstrate, such vehicles would require at the very least a degree of "tethering" to the software vendor as a service provider.[98] Tethered products represent a strategy of "maintaining an ongoing connection between a consumer good and its seller that renders that good in some way dependent on the seller for its ordinary operation."[99] We see this in the automotive world already to a certain extent with ongoing debates over schematics and servicing.[100] The need for infrastructure and legal frameworks to address "over-the-air-updates," commonly viewed as essential to maintaining performance and security in vehicle software, means tethering is essential to this archetype of autonomous vehicle futures.[101]

2. Data Flows and Privacy

The information flows between vehicles, manufacturers, insurers, platforms, regulators, and other parties in a driverless car ecosystem will increase,[102] and their implications for users, the public, and public goals are an

97. *See, e.g.*, ONDREJ BURKACKY, JOHANNES DEICHMANN, GEORG DOLL & CHRISTIAN KNOCHENHAUER, MCKINSEY & CO., RETHINKING CAR SOFTWARE AND ELECTRONICS ARCHITECTURE 3 (2018), https://www.gsaglobal.org/wp-content/uploads/2018/12/3.-Rethinking-car-software-and-electronics-architecture-Feb-2018.pdf (discussing the application of advanced driver assist systems).

98. Hoofnagle, *supra* note 68, at 785.

99. *Id.* at 785.

100. *See, e.g.*, Massachusetts Right to Repair Act, MASS. GEN. LAWS ch. 93J, § 2 (2012) (repealed 2013); AARON PERZANOWSKI & JASON SHULTZ, THE END OF OWNERSHIP: PERSONAL PROPERTY IN THE DIGITAL ECONOMY (2016).

101. *See* Mulligan & Bamberger, *supra* note 69, at 8 (discussing the need for over-the-air updates of software and the complicated set of policy questions that must be resolved to align the need with other values); *see also* Rahul Razdan, *Tesla Decepticons? Is Automotive CyberSecurity a National Defense Issue?*, FORBES (May 2, 2020, 7:33 AM), https://www.forbes.com/sites/rahulrazdan/2020/05/02/is-automotive-cybersecurity-a-national-defense-issue-/#52c6db8c1b75 (describing the lack of attention to cybersecurity implications of over-the-air updates in latest U.S. House Commerce Committee draft bill and giving perspective that this is out of step with the growing use and concerns caused by automated driving systems and with regulatory activity in other countries); H. COMM. ON ENERGY AND COMMERCE, DISCUSSION DRAFT, CYBERSECURITY RISKS TO MOTOR VEHICLE SAFETY (2020), https://assets.documentcloud.org/documents/6775841/DiscussionDraft.pdf.

102. For examples of the data being collected by automobiles in 2015, see OFFICE OF S. EDWARD J. MARKEY, TRACKING AND HACKING: SECURITY & PRIVACY GAPS PUT AMERICAN DRIVERS AT RISK (2015) (finding that information being collected by thirteen auto manufacturers included: geographic location (seven manufacturers); system settings for event

active site of political contest.[103] Dorothy Glancy, for instance, has comprehensively assessed the privacy stakes of different types of autonomous vehicle information flows, including the telemetry data traditionally collected by manufacturers.[104] She makes clear that "interactions between privacy and autonomous vehicles will depend on the design and operation of autonomous vehicles."[105] However, this analysis can be nuanced beyond the division between "self-contained" or "interdependent" vehicles as used by Glancy. Within the self-contained or driverless archetype, for instance, business cases, ownership models, and the vicissitudes of real-world operation further influence system dynamics and components, such as the form and mode of interacting with a ride-sourcing provider, the surveillance of vehicle occupants necessary to ensure safe operation or prevent vandalism, or the action of an error recovery or emergency intervention component. At a general level, moving the monitoring responsibility to a remote location requires a communication link, which in turn involves additional nodes with potential back and forth access to information flows. A real-time error correction and mobility management by remote drivers and operators further extends privacy and security considerations to vehicle sensor data.

These are subtly new types of information flows involving multiple distributed controlling components. While remote access to vehicle sensor data is not novel and relevant privacy implications have been discussed,[106] inclusion of remote human operators as shadow drivers that "tele-occupy" the same space as the vehicle "user" or "occupant" introduces novel information flows for which appropriateness must be evaluated. Again, clearly the mode of acting-on the vehicle and the triggers behind the engagements of these components, such as obstacles, emergency road conditions, or destination changes, constitute important contextual information. How those external components are represented in the system will depend on connectivity design

---

data recorder (EDR) devices, which can include data such as sudden changes in speed, steering angle, brake application, seat belt use, air bag deployment, and fault/error codes (five manufacturers); operational data, including speed, direction or heading of travel, distances and times traveled, fuel level and consumption, status of power windows, doors, and locks, tire pressure, tachometer and odometer readings, mileage since last oil change, battery health, coolant temperature, engine status, and exterior temperature and pressure (seven manufacturers)). Eight of the twelve companies reported transmitting and storing driving history data on external servers. *Id.* at 8.

103. *See* discussion *infra* Section IV.C.3.

104. *See* Dorothy J. Glancy, *Autonomous and Automated and Connected Cars – Oh My: First Generation Autonomous Cars in the Legal Ecosystem*, 16 MINN. J.L. SCI. & TECH. 619 (2015).

105. Dorothy J. Glancy, *Privacy in Autonomous Vehicles*, 52 SANTA CLARA L. REV. 1171, 1173 (2012).

106. *See, e.g.*, *id.* at 1178–81.

choices. For instance, acknowledging cyber-security threats, Waymo vehicles do not require or use constant connectivity for "driving."[107] They do, however, require certain levels of connectivity for other functions, such as following instructions that users express in the app interface. Privately-owned, non-commercial vehicles may require even less connectivity but may still retain some way to facilitate inputs from external control.

3. Responsibility and Autonomy

The responsibilities of the various component actors in these driving systems also requires rethinking. While a human occupant should perhaps not be considered a "driver" in any meaningful sense, they may have different obligations as a "passenger," "user," or "occupant," as may the other controlling components. Numerous commentators have analyzed the potential impacts of autonomous vehicles on both civil and criminal liability and likely consequences for the insurance industry.[108] Clearly, apportioning

107. Jamie Condliffe, *Why Some Autonomous Cars Are Going to Avoid the Internet*, MIT TECH. REV. (Jan. 10, 2017), https://www.technologyreview.com/2017/01/10/154642/why-some-autonomous-cars-are-going-to-avoid-the-internet/.

108. *See, e.g.*, CTR. FOR CONNECTED & AUTONOMOUS VEHICLES, PATHWAY TO DRIVERLESS CARS: CONSULTATION ON PROPOSALS TO SUPPORT ADVANCED DRIVER ASSISTANCE SYSTEMS AND AUTOMATED VEHICLES (2017) (discussing a proposal for a "single insurer" model, where a single insurer covers both driver and manufacturer); John Villasenor, Ctr. for Tech. Innovation, *Products Liability and Driverless Cars: Issues and Guiding Principles for Legislation*, *in* THE ROBOTS ARE COMING: THE PROJECT ON CIVILIAN ROBOTICS (2014); Sabine Gless, Emily Silverman & Thomas Weigend, *If Robots Cause Harm, Who Is to Blame? Self-Driving Cars and Criminal Liability*, 19 NEW CRIM. L. REV. 412 (2016); Sunghyo Kim, *Crashed Software: Assessing Product Liability for Software Defects in Automated Vehicles*, 16 DUKE L. & TECH. REV. 300 (2017–2018) (considering questions of product liability associated with increased criticality in software function compared to hardware); Alexander G. Mirnig, Rod McCall, Alexandra Meschtscherjakov & Manfred Tscheligi, *The Insurer's Paradox: About Liability, the Need for Accident Data, and Legal Hurdles for Automated Driving*, 2019 PROC. 11TH INT'L CONF. ON AUTOMOTIVE USER INTERFACES & INTERACTIVE VEHICULAR APPLICATIONS 113 (highlighting that insurers lack sufficient data about how to make decisions apportioning liability in SAE3+ applications); Fabian Pütz, Finbarr Murphy, Martin Mullins & Lisa O'Malley, *Connected Automated Vehicles and Insurance: Analysing Future Market-Structure from a Business Ecosystem Perspective*, 59 TECH. SOC'Y 101182 (2019), https://doi.org/10.1016/j.techsoc.2019.101182 (discussing the competitive disadvantage for insurers who may not be able to access the rich in-vehicle and telemetry data streams these vehicles generate and that are otherwise captured by OEMs and other service platforms, and arguing for regulatory intervention to address these information asymmetries). We also note the complication of identifying software defects in machine learning systems and increased security risks associated with higher levels of connectivity. *See, e.g.*, Abraham & Rabin, *supra* note 63 (arguing that, mirroring the movement to strict liability in workers compensation claims, we need a radically new legal regime to deal with torts questions in the context of automated vehicles; setting out a "Manufacturer Enterprise Responsibility" model for SAE level 4 and 5 vehicles that have no

liability according to whether a car is in autonomous mode or not, as attempted in the U.K. Vehicle and Technology Aviation Bill,[109] is insufficient. The different degrees of control, processes for control transitions, and user interfaces, as well as varied regulatory environments, complicate this distinction too radically. Beyond that observation, we do not intervene in these debates except to note that we agree with Glancy that "determinations such as fault or causation [become] so exceedingly complex technologically that fault and cause concepts are for all practical purposes illusory."[110] As these issues become more complex, it appears pragmatic solutions that avoid the need to apportion liability on a granular level become more likely. To that end, we address these questions with a view to a philosophical rather than legal account of responsibility.

To address the allocation of responsibility for harms within a driverless car archetype means addressing a cascade of questions. If the vehicle interface *does* include a mechanical system for directing a vehicle to "pull over," does that impose an obligation on the passenger to supervise the "driver" (i.e., vehicle) to the extent that if the vehicle is behaving absurdly, there is a responsibility to stop it? Does this depend on whether it is privately owned and operated or operated as a corporate, ride-sourcing vehicle? At what point does it become unreasonable or tortious for an occupant of an autonomous vehicle to not command the vehicle to stop? Does the passenger have an obligation to the broader public to ensure that the "driver" or controlling component is not acting dangerously or malfunctioning? When would this become the responsibility of a mobility operator, tele-operator, or control center manager? The distribution of control and control authority will proactively determine the roles of the various components in the system. These different roles will each have different levels of responsibility for system operation.

As discussed in the driver assist context, some vehicle interfaces reflect transitions of control through on-board mode lights. Others change the

fault element and does not retain existing standards for defining a defect under product liability, because the authors claim it becomes difficult to understand the concept of a defect without comparison with redundant designs; and providing an "exclusive remedy" remedy); Melinda Florina Lohmann, *Liability Issues Concerning Self-Driving Vehicles*, 7 EUR. J. RISK REG. 335 (2016) (discussing the utility of strict liability models and how they will relate to product liability models); Dorothy J. Glancy, *Sharing the Road: Smart Transportation Infrastructure*, 41 FORDHAM URB. L.J. 1617, 1644 n.140 (2013); Carrie Schroll, *Splitting the Bill: Creating a National Car Insurance Fund for Accidents in Autonomous Vehicles*, 109 NW. U.L. REV. 803 (2015) (arguing for establishment of a national scheme funded by a monthly road-users tax that operates as a no-fault compensation scheme that pays out compensation similar to Medicare and Social Security); Andrew D. Selbst, *Negligence and AI's Human Users*, B.U.L. REV. (forthcoming 2020).

109. Vehicle and Technology Aviation Bill 2016–17, HC Bill [143] (Gr. Brit.).

110. Glancy, *supra* note 104, at 670.

interface more definitively such as by color-coding the steering wheel or even changing the shape of the steering wheel.[111] But for vehicles where the person in the car is *always* a passenger, vehicle designers often try to signal the change in the person's status by removing the driver interface elements altogether. Waymo and Cruze, for example, have been petitioning the U.S. National Highway Traffic Safety Administration (NHTSA) to permit the removal of the steering wheel and driving pedals from the cabin. Another common move is to turn the front seat around to face the interior of the cabin (e.g., Magna)[112] or to reduce the size of the windows so that people inside cannot easily see out (e.g., Mercedes).[113] Many vehicle interior designs for fully autonomous vehicles harken back to planes or trains, with seats that lean back far enough to sleep. Volvo's driverless 360c concept, for example, is depicted with a person lying on a flatbed with sheets pulled up.[114] This vision makes a feature of one of the driverless cars' most troublesome features—they put people to sleep.[115] Sometimes though, it is the addition of screens throughout the interior cabin[116]—screens people could not look at if they had to attend to the road—that mark the departure between current day automobiles and driverless vehicles. Where an occupant is structurally disabled from exercising control over the vehicle, the design and efficacy of mobility management and tele-

111. Rain Noe, *Experimental Automotive Interface Design: How Should Autonomous Cars Hand Off Control to the Driver?*, CORE77 (Jan. 23, 2017), https://www.core77.com/posts/60023/Experimental-Automotive-Interface-Design-How-Should-Autonomous-Cars-Hand-Off-Control-to-the-Driver; *see also* Mishel Johns, Brian Mok, Walter Talamonti Jr., Srinath Sibi & Wendy Ju, *Looking Ahead: Anticipatory Interfaces for Driver-Automation Collaboration*, 2017 PROC. 20TH INT'L CONF. ON INTELLIGENT TRANSP. SYS. 2122; Brian Mok, Mishel Johns, Stephen Yang & Wendy Ju, *Reinventing the Wheel: Transforming Steering Wheel Systems for Autonomous Vehicles*, 2017 PROC. 30TH ANN. ACM SYMP. ON USER INTERFACE SOFTWARE & TECH. 229; CARJAM TV, *Mercedes Retractable Steering Wheel Is Art! Mercedes Driverless Cars*, YOUTUBE (Apr. 8, 2015), https://www.youtube.com/watch?v=1pOAAJZAjPU.

112. Drew Winter, *Magna Unveils Flexible Interior for Autonomous Vehicles*, WARDS AUTO (Dec. 11, 2018), https://www.wardsauto.com/autonomous-vehicles/magna-unveils-flexible-interior-autonomous-vehicles.

113. Molly Wood, *Video Feature: Inside the F 015, Mercedes's Self-Driving Car*, N.Y. TIMES (Mar. 19, 2015), https://www.nytimes.com/2015/03/20/automobiles/video-feature-inside-the-f-015-mercedess-self-driving-car.html.

114. *360c: A New Way to Travel*, VOLVO CAR CORP., https://www.volvocars.com/intl/cars/concepts/360c?redirect=true (last visited Sept. 1, 2020).

115. David Miller, Annabel Sun, Mishel Johns, Hillary Ive, David Sirkin, Sudipto Aich & Wendy Ju, *Distraction Becomes Engagement in Automated Driving*, 2015 PROC. HUM. FACTORS & ERGONOMICS SOC'Y ANN. MEETING 1676, 1679.

116. *The Mercedes-Benz F 015 Luxury in Motion*, MERCEDES-BENZ AG, https://www.mercedes-benz.com/en/innovation/autonomous/research-vehicle-f-015-luxury-in-motion/(last visited Sept. 1, 2020).

operation systems become more important because of the degree of responsibility distributed to those remote actors.

Questions of responsibility become more complex yet again if automated vehicles perform driving maneuvers too complex for humans to supervise, such as very high-speed driving or using continuous flow intersections. These possibilities raise the question: at what point on the spectrum of fully driverless vehicle activities might we abandon the idea of human responsibility altogether?

These questions of responsibility are connected to how any reconfiguration of components might impact human autonomy or agency. However, when we think of autonomy in a privately-owned, traditionally-controlled vehicle, the dramatic rearrangement of components and modes of acting in driverless vehicles inevitably challenge any meaningful connection between control, intention, and autonomy or agency.[117] That is not to say autonomous vehicles necessarily undermine autonomy. Rather, they shift what autonomy means and how it may be expressed in the automotive context. Indeed, ceding control over vehicle functionality may not necessarily eliminate any autonomy or agency for a human occupant. One example associated with the proliferation of ride-sourcing services is the shift towards use of shortest path algorithms. In combination with GPS mapping, those algorithms alter traditional taxi norms where passengers would typically have an influence, or at least say, over the route taken by the vehicle.[118] Users of ride-sourcing services, especially in the case of ridesharing or pooling, no longer express control in that way, and neither do drivers who instead follow directional commands from the automated direction system. The normalization of shortest path algorithms chosen by TNC platforms thus establishes a baseline that further automation does not necessarily disturb. Where loss of control over a route may become an issue, however, is where that route is influenced by agendas other than the passenger's intention of travelling most directly to a destination. One can imagine commercial incentives taking people past particular destinations or restaurants in the same way that entities could pay the Niantic Pokémon Go platform for Pokémon to be spawned near their

117. Sven Krome, Jussi Holopainen & Stefan Greuter, *AutoPlay: Unfolding Motivational Affordances of Autonomous Driving*, *in* AUTOMOTIVE USER INTERFACES 483 (G. Meixner & C. Muller eds., 2017).

118. *See, e.g.*, Jody Rosen, *The Knowledge, London's Legendary Taxi-Driver Test, Puts Up a Fight in the Age of GPS*, N.Y. TIMES (Nov. 10, 2014), https://www.nytimes.com/2014/11/10/t-magazine/london-taxi-test-knowledge.html.

commercial establishments to increase foot traffic.[119] Autonomous vehicles might also have their routes or destinations influenced by "public safety" agendas prohibiting travel to or through certain places or, as Elizabeth Joh has discussed, "policing" incentives that use autonomous vehicles for the sake of *de facto* arrest.[120]

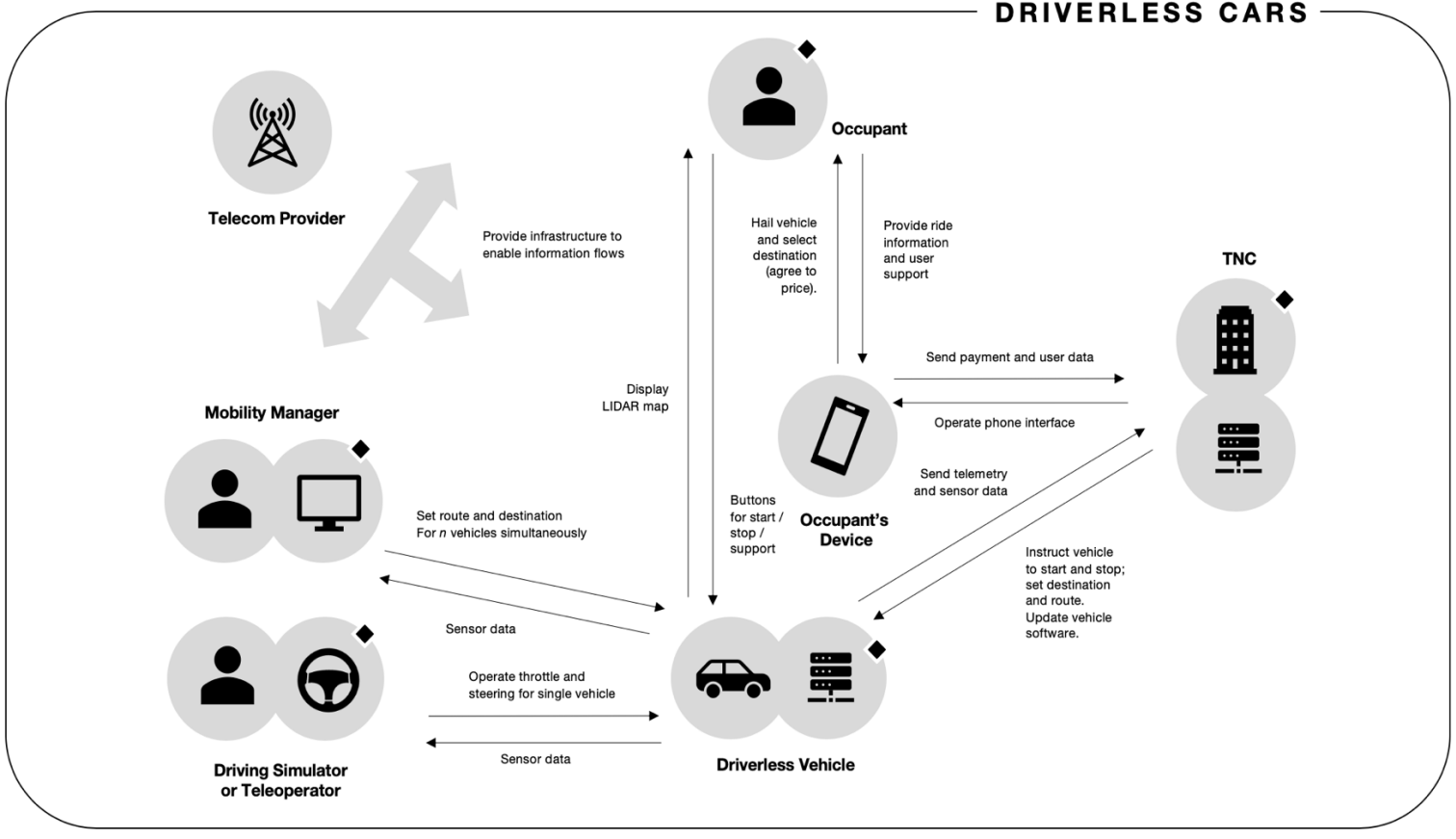
If we think of vehicles merely as another tool for transportation, the means may not matter to feelings of agency. If efficiency is the agenda, it may be that increasing transport efficiency is autonomy enhancing. Because autonomy means or requires different things for different users, designing to ensure the capacity to choose the "agenda" of the vehicle—that is to select how and for what purpose the vehicle's functions are optimized—may be more important. Some users may be satisfied with power to select a destination, or a route, while others may desire control over other operational and tactical driving decisions. It may be that occupants' interest in agency is satisfied by determining the strategic aspects of driving—where and when to go—along with the decision about what modality of transportation to use at the outset, as it is in numerous other transportation contexts. However, it may be that occupants will want the ability to tailor routes, speeds, driving styles, or the mix of values to optimize for—the scenic route rather than the fastest—or at the very least want protection against driving decisions that serve the non-safety related needs of others. Other methods may satisfy those with greater desire for the sense of freedom and autonomy associated with driving today. For instance, situational awareness and meaningful orientation, as well as connection to the environment and the driving task, may be achieved by enhancing information flows into the vehicle cabin but still without enabling control over a vehicle in a traditional way. Alternatively, it may be that those methods can be used to redirect occupants desire for agency. For instance, researchers have explored how non-driving in-vehicle activities associated with work or leisure might maintain user agency (in the sense of competence) in different ways.[121]

119. *See* Paul Tassi, '*Pokémon GO' Is Charging Sponsored PokéStops up to 50 Cents Per 'Visit,' Which Seems Like a Bad Deal*, FORBES (June 2, 2017), https://www.forbes.com/sites/insertcoin/2017/06/02/pokemon-go-is-ripping-off-its-sponsored-pokestops-charging-up-to-50-cents-per-visit/#72b826252159.

120. *See* Elizabeth E. Joh, *Automated Seizures: Police Stops of Self-Driving Cars*, 94 N.Y.U.L. REV. 113 (2019) (discussing the various ways in which autonomous vehicles could be subject to policing actions).

121. Krome, *supra* note 117.

Figure 2: Distribution of Components in Driverless Cars



C. ARCHETYPE 3: "CONNECTED CARS"

The connected cars archetype descends from the oldest vision of autonomous transport. The earliest imaginings of autonomous cars involved roadways acting as part of the communications and control system for vehicles. An exhibit at the 1939 World's Fair, sponsored by General Motors, displayed electric cars running on a roadway embedded with electric circuitry.[122] In the late 1950s, tests on short stretches of highway included detector circuits buried in the pavement that transmitted radio signals to guide the position and velocity of vehicles equipped with appropriate receivers and actuators.[123] In the 1960s, the Ohio State University pursued research in autonomous vehicles that again used electronic devices embedded in roadways; similar research was done in the U.K. with magnetic cables that successfully transported a Citroen DS at 130km/h around a test track.[124] The U.S. Bureau of Public Roads investigated the construction of electronically controlled highways in multiple jurisdictions in the 1970s and 1980s.[125] In the early 1990s, the U.S. Congress explored "intelligent vehicle highway systems."[126] At the same time, Daimler-Benz claimed to have constructed vehicles that could travel on highways for thousands of kilometers at high speed, effecting lane changes with minimum human intervention.[127]

While there is, of course, substantial overlap among driverless, driver assist, and connected cars visions, the connected cars archetype represents an alternative to "autonomous," fully driverless models where vehicles rely primarily on their own sensor arrays to navigate the physical world. In the connected cars vision, the control environment includes all vehicles continuously sharing information with one another, along with cloud computing and road infrastructures interacting, diverting, directing, and controlling vehicles by producing, receiving, and processing data. This requires

122. Gijsbert-Paul Berk, *Self-Drive Cars and You: A History Longer than You Think*, VELOCE TODAY (Aug. 5, 2014), https://velocetoday.com/self-drive-cars-and-you-a-history-longer-than-you-think/.

123. Keshav Bimbraw, *Autonomous Cars: Past, Present and Future: A Review of the Developments of the Last Century, the Present Scenario and the Expected Future of Autonomous Vehicle Technology*, 2015 PROC. 12TH INT'L CONF. ON INFORMATICS CONTROL, AUTOMATION & ROBOTICS 191, 192.

124. *Id.* at 193.

125. *Id.*

126. Intermodal Surface Transportation Efficiency Act of 1991, Pub. L. No. 102-240, § 105 Stat. 1914; *see also* Glancy, *supra* note 108, at 1624.

127. Reinhold Behringer & Nikolaus Muller, *Autonomous Road Vehicle Guidance from Autobahnen to Narrow Curves*, 14 IEEE TRANSACTIONS ON ROBOTICS & AUTOMATION 810, 813 (1998); Uwe Franke, S. Gorzig, Frank Lindner, D. Mehren & Frank Paetzold, *Steps Towards an Intelligent Vision System for Driver Assistance in Urban Traffic*, 1997 PROC. IEEE CONF. ON INTELLIGENT TRANSP. SYS. 601.

a massive proliferation of controlling components, operating through coordinated infrastructural clouds. The pure connected cars vision thus involves vehicles following trajectories controlled and decided by distributed infrastructure. At the extreme, connected cars would physically resemble driverless cars, needing just a minimal controlling interface within the vehicle. Whereas the driverless car relies on its own sensing and computational power to negotiate a virtually untouched environment, the control authority for connected cars rests with a distributed vehicular and infrastructural network orchestrated by the roadway environment itself.

Real world implementations of the connected car visions do not articulate that pure vision—at least not yet. They include different forms and scales of Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Vehicle-to-X (V2X) connectivity, with different ways of delegating control among components.[128] Unlike driverless or driver assist approaches, continuous connectivity in connected cars is absolutely necessary because of the multiple elements exercising "direct control for time-critical, flow-related interventions—for which some degree of system-level coordination is required for safe operation."[129]

V2V protocol standardization has been the focus of agencies like the NHTSA, which has been investigating the dynamics of making V2V capabilities mandatory in vehicles.[130] Standardizing transmission of basic safety messages (BSM) between vehicles to facilitate warnings to drivers has been on the regulatory agenda since at least 2014 (although the NHTSA has been researching these questions for a decade more—even acquiring dedicated vehicle communications radio spectrum from the FCC in 1997).[131] The

128. Presently, very few vehicles use robust V2V or V2I communications. Bryant Walker Smith, *A Legal Perspective on Three Misconceptions in Vehicle Automation*, *in* ROAD VEHICLE AUTOMATION 85, 89–91 (Gereon Meyer & Sven Beiker eds., 2014). V2V communications technology has been primarily tested and promoted in the context of "road train," "peloton," or "platoon" style transport configurations, designed to reduce environmental pollution by using the aerodynamic efficiencies of vehicles travelling closer together or behind a truck. *See generally* Hani S. Mahmassani, 50th Anniversary Invited Article, *Autonomous Vehicles and Connected Vehicle Systems: Flow and Operations Considerations*, 50 TRANSP. SCI. 1140 (2016). Nonetheless, engineers argue that almost every aspect of "driver" decision making would be improved by V2X connectivity. *See id.* at 1140.

129. *Id.* at 1160.

130. *See, e.g.*, OFFICE OF REGULATORY ANALYSIS & EVALUATION, NHTSA, PRELIMINARY REGULATORY IMPACT ANALYSIS: FMVSS No. 150 VEHICLE-TO-VEHICLE COMMUNICATION TECHNOLOGY FOR LIGHT VEHICLES (2016) [hereinafter "V2V COMMUNICATION"].

131. *See, e.g.*, JOHN HARDING, GREGORY POWELL, REBECCA YOON, JOSHUA FIKENTSCHER, CHARLENE DOYLE, DANA SADE, MIKE LUKUC, JIM SIMONS & JING WANG,

NHTSA proposal would require all light vehicles manufactured after 2023 to include short range radio (Wi-Fi-like) devices to transmit information that receiver vehicles then process and display for drivers.[132] Under the proposed NHTSA V2V rules published in 2017, BSM would include: time, location, elevation, speed, heading, acceleration, yaw rate, path history, exterior lights, event flags, transmission status, steering wheel angle, and vehicle size (with brake status optional).[133] It is then up to vehicle manufacturers to build safety applications into vehicles that translate this data into useful information.[134] Likely safety implementations are forward collision warnings, do not pass warnings, left turn assistance, intersection movement assistance, and blind spot lane change warnings.

The NHTSA V2V regulation, however, has little to do with vehicle control automation or autonomous transport. The connected cars archetype focuses on distribution of vehicle control throughout an infrastructural environment, whereas the above V2V applications are more about improving vehicle sensing by including information broadcast from other vehicles about their status—they do not interrupt the distribution of control or degrade the driver's control over the vehicle. This system therefore introduces new triggers for communicative action (safety warnings) operating on a driver but does not include the introduction of new control components. That said, using these communications systems does require standardizing the messaging languages and ensuring spectrum availability, which could be understood as regulatory precursors to more comprehensive V2X applications.[135]

An example of V2V communication that does complicate questions of control is truck platooning. In a truck platoon, two trucks drive one behind the other on a highway. By establishing a secure and encrypted wireless link, the lead vehicle is able to communicate acceleration and braking so that the trucks can safely drive closer together than they would if they were depending upon visual cues and driver response time alone. This allows the trucks to draft off of one another, saving approximately five percent in fuel consumption rates for the lead vehicle, and ten percent for draft vehicles.[136] In future

---

U.S. DEP'T OF TRANSP., VEHICLE-TO-VEHICLE COMMUNICATIONS: READINESS OF V2V TECHNOLOGY FOR APPLICATION (2014)*; see also* Glancy, *supra* note 108, at 1644 n.140.

132. *See* V2V COMMUNICATION, *supra* note 130.

133. Federal Motor Vehicle Safety Standards; V2V Communications, 82 Fed. Reg. 3854 (proposed Jan. 12, 2017) (to be codified at 49 C.F.R. pt. 571).

134. V2V COMMUNICATION, *supra* note 130.

135. *Id.*

136. MICHAEL LAMMERT, KENNETH KELLY & JANET YANOWITZ, NAT'L RENEWABLE ENERGY LAB., CORRELATIONS OF PLATOONING TRACK TEST AND WIND TUNNEL DATA 3–5 (2018).

systems, both longitudinal and latitudinal control for the following truck could be operated through a combination of autonomous driving technology and intervehicle communication. This would enable drivers of the trailing vehicles to supervise vehicles rather than actively drive, which can reduce driver fatigue. As the technology progresses, the intent is for truck platooning protocols to converge so that trucks from different fleets using different manufacturers' platooning hardware and software will nevertheless be able to platoon.[137] Following that, the intent is for the drivers of trailing vehicles to be able to rest or even sleep when their vehicle is in a platoon.[138] In this case, we can track a redistribution of control across the vehicles in the platoon as they become components in a system. However, moving from V2V to V2I and V2X has the potential to radically expand the number of components and the complexity of their action, which requires substantial new infrastructure.

Driverless cars are being built to work with existing infrastructures, while building in error-correction mechanisms to deal with inevitable problems. Proponents of connected cars, on the other hand, are pushing for massive re-instrumentation of urban environments. Distributed vehicular control and orchestration introduce benefits that only infrastructural coordination can bring, like advanced traffic management (vehicles no longer needing to stop and go), ultra-high-speed travel, and continuous flow intersections. While these benefits will require the implementation of new infrastructures, the result will transcend the capacity of human "driver" supervision.[139] In fact, these high-level coordinated actions are likely unachievable on roadways shared with manually controlled vehicles.[140] That need for a hundred-percent adoption, however, represents a primary limitation for this vision in existing urban environments. At the same time, it rationalizes the idea that single providers ought to be in charge of developing "smart city" infrastructures in new, ground-up developments where infrastructures can be built from scratch, like

137. *See, e.g.*, PLATOONING ENSEMBLE, https://platooningensemble.eu/ (last visited Sept. 6, 2020).

138. Sarah-Maria Castritius, Heiko Hecht, Johanna Möller, Christoph J. Dietz, Patric Schubert, Christoph Bernhard, Simone Morvilius, Christian T. Haas & Sabine Hammer, *Acceptance of Truck Platooning by Professional Drivers on German Highways: A Mixed Methods Approach*, 85 APPLIED ERGONOMICS 103042, 103042 (2020), https://doi.org/10.1016/j.apergo.2019.103042.

139. *See* Sven Krome, David Goedicke, Thomas J. Matarazzo, Zimeng Zhu, Zhenwei Zhang, J.D. Zamfirescu-Pereira & Wendy Ju, *How People Experience Autonomous Intersections: Taking a First-Person Perspective*, 2019 PROC. 11TH INT'L CONF. ON AUTOMOTIVE USER INTERFACES & INTERACTIVE VEHICULAR APPLICATIONS 275, 282–83.

140. *See, e.g.*, Kwok J. Leung, *Synergistic Traffic Intersection – A Method for Coordinating Vehicles and Facilitating the Introduction of Autonomous Vehicles*, 8 INT'L J. TRAFFIC & TRANSPORT ENGINEERING 1 (2019).

the (now abandoned) Toronto Waterfront.[141] This takes the fleet-car ownership model in the driverless car archetype and expands it to include ownership of static infrastructure in public space.

1. Political Coordination for Connected Cars

The fragmentation of control across innumerable human, vehicular, and infrastructural components raises as many questions about societal values. Alongside questions about privacy, responsibility, autonomy, and human freedom, the connected cars archetype highlights deeply political questions about the governance of public space—who is entitled to interact with it and in what ways? A careful balance between governance by commercial actors who own various components and governance by politically legitimate actors will be essential to achieving a workable and just system.

Whereas Lewis Mumford saw an authoritarian tendency in automobiles as a challenge to the human agent as "walker,"[142] these new infrastructural constellations require a new calculus of political rationality and ethical consequences. The coordinating infrastructural cloud may appear to embody what Mumford called "theological-technological mass organization,"[143] an authoritarian rather than democratic technological arrangement. But the question of whether to pursue centralized or decentralized technologies must include questions about who that central coordinating entity might be, who might control the coordinator, and toward what ends. Put another way, thinking about these transport infrastructures as democratic, libertarian, collectivist, or authoritarian does not adequately address the dynamics of private and public governance also at play. At stake here is the question of the degree to which democratic control can be exercised over the shape and function of a complex sociotechnical system that occupies public space. We must analyze the degree to which a private provider of that system becomes able to control how that system configures social relations in accordance with its own interests. That means understanding how different configurations of private and public providers—i.e., of what entity owns and controls what part of a transport system—affect ethical and political outcomes. Of particular concern is how these ownership arrangements might affect who has control

141. *See, e.g.*, Ben Spurr, *Sidewalk Labs Wants to Create a New Transportation Authority*, THE STAR (June 25, 2019), https://www.thestar.com/news/gta/2019/06/25/sidewalk-labs-wants-to-create-its-own-transportation-authority-in-quayside.html (discussing proposals for a Waterfront Transportation Management Authority to take over certain dimensions of traffic governance presently under city jurisdiction).

142. Mumford, *supra* note 38, at 8.

143. *Id.* at 2.

over deciding the conditions by which individuals are able to interact with transport systems. But again, the specifics of the system are critical.

Consider a few of the governance alternatives. One might resemble existing arrangements: the connected transport infrastructures are communally (state) owned but host mostly privately owned (or leased) vehicles.[144] In the pure connected car vision however, we would need to consider what it would mean to own a connected car when very little control can be exercised, apart from selecting a destination. Another governance arrangement might hybridize connected and driver assist models: individual control over vehicles may be necessary to manage transitions into connected car environments, such as a continuous flow intersection, and out of these environments when a human driver takes back the helm.[145] In such a case, a driver may prefer to have property rights in the vehicle, with the capacity to exclude others, rather than a license to occupy that vehicle only for the duration of a trip. In a third model (transportation totalitarianism), developers of smart city infrastructure may seek to unify ownership of the infrastructure with the vehicles that use it, rendering the transport system a form of public transport that provides mobility more as a service. The distinction between this scenario and the mobility as a service arrangement of driverless cars is that here, there is potentially control over both vehicles and infrastructures, which translates into the power to define the terms by which private actors engage with and access that infrastructure.

In any of these, democratic societies should embed sufficient oversight by legitimate governing bodies to ensure the maintenance of democratic values, such as equity and transparency with regard to resources and data management. Public transport services are typically offered to the public at large with relatively few barriers to entry and on relatively egalitarian terms.[146] Democratically governed infrastructure might privilege the goal of equality in service provision over profit.[147] The values associated with public transport are primarily connected to the utility of transport as an integral public service, *ideally* privileging holistic values like mobility, safety, equality, or environmental concerns. Private corporations may supply that utility for a fee or with the support of advertising revenues and may sometimes include unjustifiable levels

144. One must acknowledge, of course, that there is a large degree of private ownership of transport infrastructures, varying according to jurisdiction and political system.

145. Krome, *supra* note 139, at 103042.

146. *See, e.g.*, ROEL NAHUIS, THE POLITICS OF INNOVATION IN PUBLIC TRANSPORT: ISSUES, SETTINGS, DISPLACEMENTS 19 (2007).

147. *See*, *e.g.*, Ashim Kumar Debnath, M. Mazharul Haque, Hoong Chor Chin & Belinda Yuen, *Sustainable Urban Transport: Smart Technology Initiatives in Singapore*, 2243 TRANSP. RES. REC.: J. TRANSP. RES. BD. 38 (2011).

of surveillance. However, the primary function ought to remain the provision of a public service. Private mobility services, on the other hand, may deploy more market mechanisms and ways to stratify users in order to optimize for profit. For instance, there is already discussion of how market-based mechanisms (i.e., willingness to pay) might allocate rights and priorities in environments like continuous flow intersections.[148] Similarly, if infrastructural control were vested in a single private entity, they may be able to take advantage of their monopoly position to implement preferential access to roadways or TNC participation for vehicles using their driving (i.e., vehicle control) software platforms, even if individually owned.

To the degree that autonomous transport systems follow the existing political and ethical alignment of "smart cities," they may therefore replicate or amplify pathologies existing in capitalist political economy.[149] As described by Francesca Bria and Evgeny Morozov, for example, this means data extractivism and accumulation, which involves treating both individual and urban data as commodities to be bought and sold on secondary markets, using machine learning systems that treat cities and transport as optimization problems, and rejecting equality and social justice as legitimate goals of public policy.[150] Several cities in the United States are already subsidizing ride-sourcing firms rather than investing in state-owned public transport infrastructure, thus further privatizing public transport systems.[151] As private firms move into autonomous transport models in the connected car vision, their commercial logics may continue to define infrastructural arrangements, the types and volumes of information flows, and the social configurations that follow.

Private entities, even those with significant power, may still be subject to regulatory oversight in the public interest, and this oversight capacity should not be relinquished. The California Public Utilities Commission (CPUC)

148. *See, e.g.*, Muhammed O. Sayin, Chung-Wei Lin, Shinichi Shiraishi, Jiajun Shen & Tamer Başar, *Information-Driven Autonomous Intersection Control via Incentive Compatible Mechanisms*, 20 IEEE TRANSACTIONS ON INTELLIGENT TRANSP. SYSTEMS 912 (2019); Heiko Schepperle & Klemens Böhm, *Auction-Based Traffic Management: Towards Effective Concurrent Utilization of Road Intersections*, 2008 PROC. 10TH IEEE CONF. ON E-COMM. TECH. & 5TH IEEE CONF. ON ENTERPRISE COMPUTING, E-COMM. & E-SERVS. 105; Matteo Vasirani & Sascha Ossowski, *A Market-Inspired Approach for Intersection Management in Urban Road Traffic Networks*, 43 J. ARTIFICIAL INTELLIGENCE RES. 621 (2012).

149. Rob Kitchin, *The Ethics of Smart Cities and Urban Science*, 374 PHIL. TRANSACTIONS ROYAL SOC'Y A. 11–12 (2016).

150. *See generally* EVGENY MOROZOV & FRANCESCA BRIA, ROSA LUXEMBURG STIFTUNG, RETHINKING THE SMART CITY: DEMOCRATIZING URBAN TECHNOLOGY (2018).

151. *Id.* at 16.

regulates TNCs as common carriers,[152] which affords it some leverage to demand satisfaction of social goals, such as equity and environmental considerations. It has pursued ways to decrease vehicle emissions and ensure access for disabled users.[153] CPUC is even able to demand the provision of data by TNCs that can be used to develop regulatory policy. The point is that through regulating industries, elements of public interest can be advanced without full public ownership of infrastructure. Indeed, nationalization or socialization of infrastructure is not the only lever by which to manipulate the political economy of autonomous transport. That said, whatever distributions of power and control are achieved over transport systems, there is a great deal at stake in the connected car context.

2. Machine Readable Spaces and People

Systematic arrangements of control over transport infrastructures have both practical and ethical implications. In the connected car vision, control authority is delegated throughout the infrastructure and cars become individual nodes in a distributed information-processing and decision-making transport network. For example, an ordinary traffic light acts on an autonomous vehicle through light emanations that are sensed by a camera and then interpreted to indicate traffic rules. This is somewhat analogous to the traffic light indicating, by affordance, a normative or legal obligation on a driver to stop a car. A "smart" traffic light might communicate that instruction via radio signal, understood by both the vehicle and the human occupant that supervises the driving task. In the connected car archetype, however, a "smart" traffic light might stop a vehicle by directly disabling its motion. Versions of this paradigm that circumvent the need for visual signals that are meaningful to humans acutely raise Handoff questions: although we may believe human-visible signals are not necessary for functional purposes, their absence may result in systems that are inscrutable.

On one hand, this progression ameliorates the need for vehicles to directly sense physical infrastructure designed and built for human readability. That may be desirable considering the ease with which computational approximation of human sensing, like vision, can be fooled or hacked. There is evidence that computer vision processors on board autonomous vehicles might be tricked to not recognize road signs with a simple application of black

152. *See* CAL. PUB. UTIL. CODE § 5440 (West 2019).

153. *See generally* SIMI ROSE GEORGE & MARZIA ZAFAR, CAL. PUB. UTIL. COMM'N, ELECTRIFYING THE RIDE-SOURCING SECTOR IN CALIFORNIA: ASSESSING THE OPPORTUNITY (2018).

and white stickers.[154] On the other hand, infrastructures designed to computationally control vehicles may de-humanize roadways. This may mean that roadways and infrastructure privilege vehicles over other entities like pedestrians by making the experience of transport spaces less legible to non-networked humans. A road that no longer includes "stop" signs or traffic lights would be far more difficult to navigate as a pedestrian or cyclist. A more extreme example can be seen in cases like continuous flow intersections, which may have to exclude pedestrians from the space altogether. In other words, complex transport spaces may become "human exclusion zones."[155]

An alternative way of addressing these issues under the connected car vision is to ensure the machine readability of humans on roadways.[156] That is, require that humans become part of the machine-readable transport infrastructure. The development of Vehicle-to-Pedestrian (V2P) connectivity is an expression of that trajectory.[157] Designed to improve the sensing of humans (as pedestrians and cyclists) in shared spaces, V2P uses devices like smartphones as collision estimation modules.[158] In the same way that safety narratives shifted through the twentieth century from crash avoidance to vehicle crashworthiness, concentrations of infrastructure and vehicle ownership and control may produce a shift back to a technical paradigm of crash *avoidance*.[159] In other words, as infrastructure becomes a more dominant, controlling component, humans may have to become part of that controlling infrastructure to participate in public space. While visibility of humans in space has always been a trigger for a driver to engage with and control a vehicle, the point here is that concentrations of power in vehicle infrastructure enable

154. Kevin Eykholt, Ivan Evtimov, Earlence Fernandes, Bo Li, Amir Rahmati, Chaowei Xiao, Atul Prakash, Tadayoshi Kohno & Dawn Song, *Robust Physical-World Attacks on Deep Learning Visual Classification*, 2018 PROC. IEEE/CVF CONF. ON COMPUTER VISION & PATTERN RECOGNITION 1625, 1632.

155. Jesse LeCavalier, *Human Exclusion Zones: Logistics and New Machine Landscapes*, 89 ARCHITECTURAL DESIGN 48 (2019) (regarding logistical environments like warehouses).

156. The term "machine-readable humans" was first introduced in Daniel Howe & Helen Nissenbaum, *Engineering Privacy and Protest: A Case Study of AdNauseam*, 1873 CEUR WORKSHOP PROC. 57, 64 (2017).

157. *See generally* JOHN L. CRAIG, JANET FRASER & JASON CAMPOS, U.S DEP'T OF TRANSP., USDOT VEHICLE-TO-PEDESTRIAN RESEARCH: WHITE PAPER 3 (2017).

158. *See, e.g.*, Zishan Liu, Zhenyu Liu, Zhen Meng, Xinyang Yang, Lin Pu & Lin Zhang, *Implementation and Performance Measurement of a V2X Communication System for Vehicle and Pedestrian Safety*, 12 INT'L J. DISTRIBUTED SENSOR NETWORKS 1 (2016) (describing an architecture for such a system).

159. Jerry L. Mashaw & David L. Harfst, *From Command and Control to Collaboration and Deference: The Transformation of Auto Safety Regulation*, 34 YALE J. REG. 167, 257–58 (2017) (noting that autonomous vehicle technologies tend toward crash-avoidance and suggesting a return to the crash avoidance safety paradigm).

those actors to express their will over the physical world and to make it more machine-readable if that suits their agenda. This changes an individual's capacity to choose their relationship to a transport infrastructure and public space and to exist in public without technological augmentation and associated surveillance. Forcing cars to carry transmitting devices for the sake of road safety makes sense and clearly falls within the regulatory purview of governing road use. Building static infrastructure that can identify pedestrians that may wander into harm's way and communicate that to vehicles, such as computer vision systems at intersections or bus stops, goes further but has limited additional ethical impacts. Compelling pedestrians or cyclists to transmit their own location and movement, however, raises a markedly different question. This is a question that more closely hinges on the power of different entities to articulate their vision of the world.

This is very much the essence of the connected car conundrum. It is necessary to either remove elements of the roadway that are not amenable to infrastructural control (i.e., people) or to instrument and monitor them so that they become manageable for computational systems. These changes may be the product of democratic deliberation, or they may be the product of coercive, private infrastructural power.[160]

3. Data Governance

Data governance questions are similarly acute in the connected vehicle paradigm, with obvious implications on privacy. Clearly, the transmission of data is essential to the proper function of all the vehicles within a connected cars network. The data produced and distributed in a connected vehicle may include "technical data regarding the car and its components, data about the road, weather and traffic conditions, the driving behavior of the car drivers, location data, as well as data concerning the use of entertainment, navigation, and many other services by the car users."[161] Mass quantities of data streaming between vehicles and infrastructure create profound opportunities for third parties to participate in a new vehicular/infrastructural data economy, with the capacity to interact with vehicles (and the people within them) in real-time, for new purposes.

Beyond the mere functioning of vehicles, data governance will be influenced by commercial imperatives and thus provoke data protection and antitrust regulation, as well as competition over vehicle information architectures. To that end, proposed models for data architectures include

160. *See, e.g.*, Howe & Nissenbaum, *supra* note 156.

161. Wolfgang Kerber, *Data Governance in Connected Cars: The Problem of Access to In-Vehicle Data*, 9 J. INTELL. PROP. INFO. TECH. & E-COMM. L. 310, 312 (2019).

"shared servers," "in-vehicle"—i.e., consumer choice—data storage, manufacturer-controlled servers, and even "peer-to-peer" proposals, amongst others.[162] Where vehicle data is part of a continuing system of information flow between the vehicle and the vehicle manufacturer's servers, vehicle manufacturers would prefer to exclude third parties. Excluding third parties gives manufacturers more control over the vehicle interface and a commercial position in downstream markets like insurance.[163] More pro-market approaches prefer open access to vehicle data. This enables downstream actors like insurance companies to make the calculations relevant for designing their policies. Cautious consumers, on the other hand, might reject open access, preferring "in-vehicle" data storage systems that excludes third parties all together.

These various data governance approaches and architectures extend to the internal informational environment of the car. Indeed, in vehicles where humans express less control, the freed-up human attention will become the subject of market competition. In some information architectures, only the vehicle manufacturer controls the informational experience. Other approaches give multiple parties access to the infotainment system. In the United States, a group of twenty vehicle manufacturers have agreed to a voluntary regimes of privacy principles,[164] but vehicular information ecologies are already changing. Car manufacturers are already ceding control over vehicle interfaces to third parties.[165] As discussed above, it is possible this may extend to technologies actively controlling (i.e., driving) vehicles. If these types of mixed systems follow prevailing commercial logics, they could enable location and user-specific commercial messaging and otherwise radically different transport experiences.

4. Responsibility and Autonomy

This diffusion of car and driver components into a broader network of vehicles, infrastructure, manufacturers, and platforms also complicates questions of responsibility. Some have talked about how the introduction of

162. EUR. COMM'N, BIG DATA AND B2B PLATFORMS: THE NEXT BIG OPPORTUNITY FOR EUROPE (2019) (Workshop Brief, Second Workshop on "Fair and Equal Data Sharing for Cooperative, Connected and Automated Mobility"), https://www.ceps.eu/wp-content/uploads/2019/08/09172019-Brief_second_workshop_WP1_automotive-1.pdf.

163. Kerber, *supra* note 161.

164. *About Automotive Privacy*, ALL. OF AUTO. MFRS., https://autoalliance.org/connected-cars/automotive-privacy/ (last visited Sept. 6, 2020).

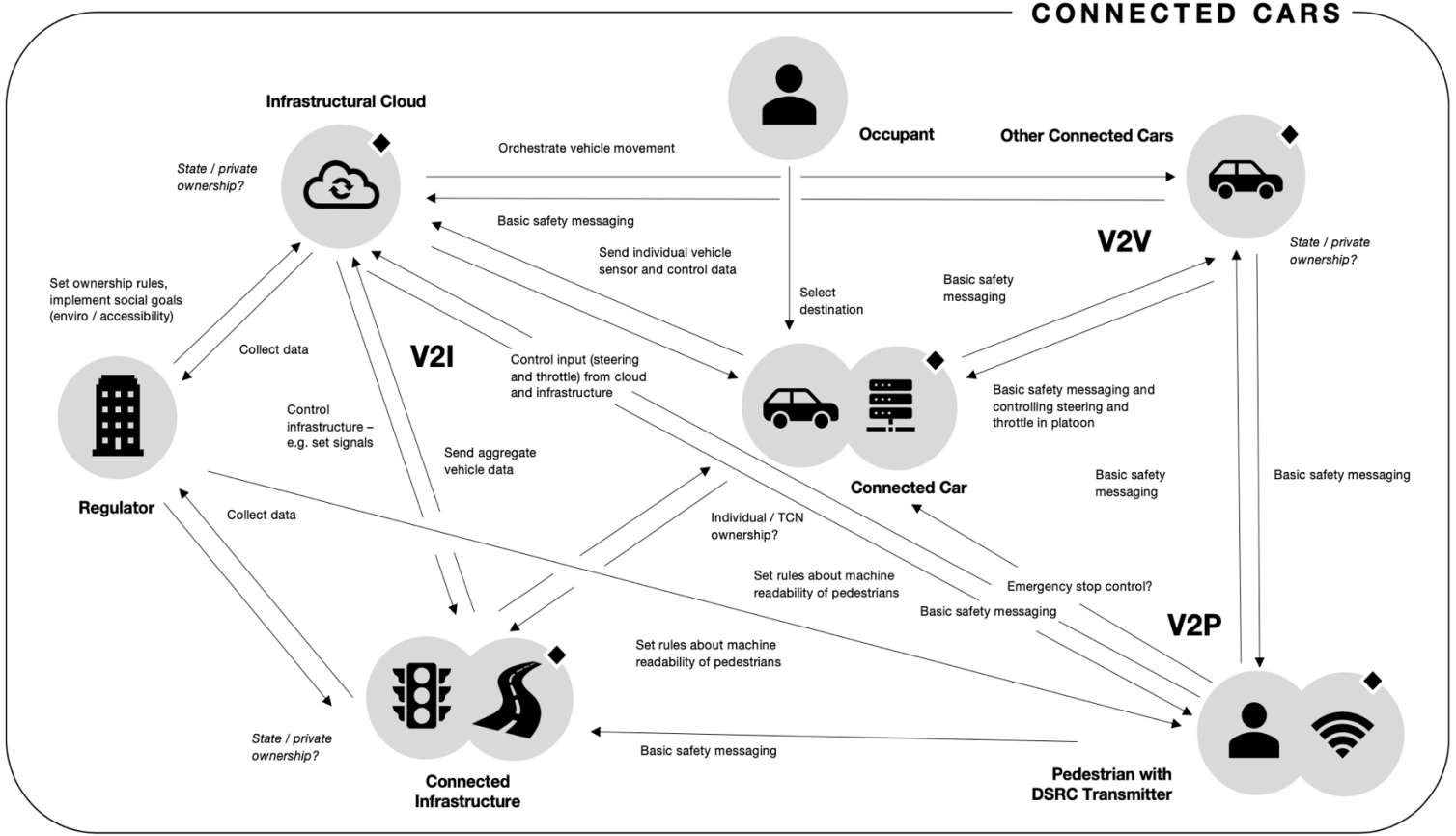
165. *See, e.g.*, Sean O'Kane, *GM Will Use Google's Embedded Android Automotive OS in Cars Starting in 2021*, THE VERGE (Sept. 5, 2019, 12:15 PM), https://www.theverge.com/2019/9/5/20851021/general-motors-android-auto-google-infotainment.

autonomous vehicles will transform the driving behavior of all road users into a single "driver"—the operating system of all vehicles operating on a certain network.[166] This represents a dramatic reconfiguration of what was once a relatively individualistic and private exercise into a broader technological network. But what would the reciprocal obligations between an individual and the network generally be? What if the sensors in one car fail because of improper maintenance, causing damage to other vehicles relying on that communications network? What if the network itself fails? In the division of fault and responsibility between vehicles and drivers, the conditions of transport infrastructure often implicate roads agencies in accident litigation. Claimants often sue over issues such as whether a road was appropriately designed, signaled, or maintained. Perhaps the camber of the road was too steep for the curve. Perhaps the speed limit was too high for the visibility. These questions will inevitably have to be reformulated in the connected roadways context. For instance, was there too much latency in the communications network? Why was a specific class of communications privileged over another class in any particular situation? Did a piece of infrastructure not transmit powerfully enough? Did the agent managing an intersection give inappropriate priority to a particular vehicle? What responsibility will the various components in the system, like state agencies or the entities operating the transport "platforms," bear for the proper operation of static infrastructure and communications networks? And, as discussed above, what responsibility will non-vehicle users of those infrastructural environments have to ensure their legibility to the ubiquitous, governing, infrastructural system?

166. *See, e.g.*, Mark A. Geistfeld, *A Roadmap for Autonomous Vehicles: State Tort Liability, Automobile Insurance, and Federal Safety Regulation*, 105 CAL. L. REV. 1611, 1621 (2017). The question of responsibility is discussed here primarily in philosophical rather than legal terms. Insurance and legal liability rules are designed to apportion risk and fault according to a specific economic or behavioral calculus. The novel questions around both civil and criminal legal responsibility have been subject to a great deal of insightful analysis. *See* sources cited *supra* note 108. While the question of human responsibility is an element of that calculus, the necessity of finding fault is also often avoided in liability systems through the introduction of no-fault or strict (product) liability systems. On the other hand, these systems often work in concert with negligence actions seeking to apportion fault to an appropriate party. The technical complexity of control hand-overs suggest the apportioning of legal liability between a vehicle manufacturer and human driver according to standards of performance (or negligence) may be difficult unless there are extreme examples of negligence or product failure. This may result in product liability approaches, single insurance schemes where a single insurer covers both the driver and the manufacturer, or even no-fault compensation schemes. Ascertaining an appropriate liability regime is not the goal of this analysis, however. Instead, we explore the question of how the information interface may result in defining the experience of responsibility for the operation of a vehicle.

The autonomy question is more complex still. Connected car approaches inevitably involve loss of individual control over cars, as well as a potential loss of control over the general informational environment. This is presented as part of the trade-off associated with using a "smart city" style platform. For instance, in order to obtain the greater public benefits of high-speed travel or continuous flow intersections, the loss of autonomy becomes the cost of obtaining access to the benefits of the "smart city." Taking our continuous flow intersection example further, one could imagine a stratification of users with respect to waiting times for cars, quality or age of vehicles, and efficiency of routes being informed by commercial imperatives. As discussed, the agreeability of that trade-off will depend on the general agenda of the "smart city." This may be highly commercialized, or it may be a primarily public arrangement. However, the consequences will inevitably include a shift away from a human driver in a vehicle and into either a public, communal, social infrastructure designed for common benefit or a corporate infrastructure designed for profit.

Figure 3: Distribution of Components in Connected Cars



IV. VALUE CHOICES IN AUTONOMOUS VEHICLE FUTURES – GUIDANCE FOR POLICY-MAKERS

The Handoff model has helped us flesh out key value propositions latent in possible autonomous vehicle futures. In contrast to the traditional tale of neat, linear building blocks towards full autonomy, suggested by the SAE taxonomy,[167] our analysis foregrounds a range of values beyond security in play across all autonomous vehicle futures. It reveals that the structural, legal, and normative constraints that stabilize the meaning and relative protection of particular values are unsettled or even upended in distinct autonomous vehicle futures.

Each autonomous future breaks more radically with certain current arrangements, unmooring particular values. Driver assist upends traditional expectations of agency and responsibility as assigned to human and technical actors. It requires cars to be more responsive to the specific lived realities of human drivers. Doing so requires new data flows, interaction patterns, and demands enhanced policy attention to human-machine-interface issues.

Driverless vehicles rearrange current understandings of what physical relationships must exist for a human to drive a vehicle. This disjuncture between physical presence and driving creates new questions about human responsibility and liability creating the need for real-time observation and communication to support remote humans when called on to drive.

If driverless cars destabilize the relationship between physical presence and driving, connected cars destabilize the boundary of the "car" itself. Bringing cars into a connected city infrastructure requires radical changes to the physical and informational environment, as well as the behaviors of the humans who occupy it. The complex coordination inherent in connected cars leans toward centralized models of vehicle ownership and data collection, opening up new questions about competition and data governance. Because the state has the potential to be an owner or to have broader regulatory authority, this archetype may open up some distinct opportunities to enhance the extent to which equitable access and environmental issues are considered to be within the frame of autonomous vehicle futures policy.

By allowing us to more clearly see and understand the political nature of each autonomous vehicle future, the Handoff analysis makes space for designers, policymakers, and the public to reflect on the values we seek to maintain and foster in autonomous vehicle futures. Rather than leaving values to fallout from processes that center the technical, the Handoff model emphasizes the "three-way intersections between design, practice, and policy

167. SAE INT'L, *supra* note 22 (setting out five levels of automation).

[that] show up with particular complexity and importance during periods of formation and emergence,"[168] and directs our gaze to the values that ought to be centered in the "policy knots"[169] of specific autonomous vehicle futures. Whether or not they are in sight, the values at stake in these futures will be addressed through design, practice, and policy. By shaking them loose, these values become not only a lens through which we choose among autonomous vehicle visions to pursue but also explicit goals to be stabilized through the technical, legal, and social practices necessary to enact desired autonomous vehicle futures. Below we discuss key policy issues raised by each archetype.

A. DRIVER ASSIST

Norms and laws expect humans to watch and audit technical actors and to read and act on technical interfaces. Yet the coordination essential for safety in the driver assist archetype and the evolving standards and regulatory frameworks require cars to be more aware of and responsive to the specific lived realities of human driving partners. The complex interactions of Handoffs (the human assessing whether the technical driver can be assigned driving tasks under existing conditions) and throwbacks (when the technical driver determines the boundary conditions that define its license to drive have been reached) demand new modes of acting-on and acting with. To enable this coordination, technical actors are required to monitor and groom human actors, and human actors are expected to monitor and heed technical actors. New data flows arise to support such interaction patterns between human and technical drivers.

1. *Agency, Responsibility, and the Changing Roles for Human and Technical Actors*

The complex coordination required as human actors shift into the role of driver, either when technical components reach their limits or because they simply wish to drive, raises important questions about how to maintain or secure necessary levels of human attention. Users performing any action in a vehicle that vehicle designers did not intend can contribute to a safety problem. If a vehicle does not actively monitor and engage the attention of the driver,

168. Steven J. Jackson, Tarleton Gillespie & Sandy Payette, *The Policy Knot: Re-Integrating Policy, Practice and Design in CSCW Studies of Social Computing*, 2014 PROC. 17TH ACM CONF. ON COMPUTER SUPPORTED COOPERATIVE WORK & SOC. COMPUTING 588, 592.

169. The "multiple gatherings and entanglements through which worlds of design, practice and policy are brought into messy but binding alignment." *Id.* at 589.

the driver is likely to perform in ways the vehicle designers did not anticipate.[170] This raises issues of a vehicle manufacturer or operator's responsibility for the driver's role in the safety system of the vehicle and how a vehicle ought to condition the conduct of its occupants. These questions of responsibility in driver assist cars are different, and perhaps more complex, than in fully driverless implementations.

The complex, coordinated action demanded in the driver assist archetype challenges the stepwise safety progress presented by the traditional autonomous vehicle narrative. While autonomous driving futures are generically and uniformly portrayed as decreasing the risk of accidents due to distracted, intoxicated, or otherwise impaired drivers by transferring responsibility to the sober and stalwart technical driver, the story in the driver assist archetype is more complicated and contingent.[171] The driver assist archetype positions the human driver—even when not driving—as the ultimately responsible and always available driver: the driver of first and last resort. While the human driver can make the first move—i.e., by calling the technical driver into being—the technical driver can always demand that the human resume driving.[172]

The ability of the technical actor to pass driving back to the human presents unique safety challenges. First, the Handoffs themselves—even with a fully awake and attentive human in the driver's seat—happen in short time frames and under challenging conditions. As the child's game of "hot potato" teaches us, even handling a simple object and managing a simple objective becomes difficult under conditions of uncertainty and pressure. In the context of driving throwbacks, the objects are large, heavy, and may behave in ways that humans find difficult to predict. At the same time, the conditions are

170. Miller et. al., *Distraction Becomes Engagement*, *supra* note 115, at 1679 (explaining the complex relationship between different media, different modes of delivery, drowsiness and re-engagement time and the design challenge this presents for the autonomous vehicle media environment).

171. *See* CASUALTY ACTUARIAL SOC'Y AUTOMATED VEHICLES TASK FORCE, RESTATING THE NATIONAL HIGHWAY TRANSPORTATION SAFETY ADMINISTRATION'S NATIONAL MOTOR VEHICLE CRASH CAUSATION SURVEY FOR AUTOMATED VEHICLES 14 (2014) (stating that the results of the National Highway Transportation Safety Administration's 2008 National Motor Vehicle Crash Causation Survey "do not conclusively determine the number of accidents automated vehicles will eliminate" because "the driver remains a vital part of the accident-reduction equation," and "[d]river behavioral issues may interfere with optimal implementation of the technology in over 30% of the accidents").

172. Our driver assist archetype captures levels 1–3 in the SAE taxonomy in which the driver is always responsible for driving, must be ready to immediately resume whatever driving tasks the car has been assigned when the car determines it is necessary, and is designated the "fall-back driver." *See* SAE INT'L, *supra* note 22.

variable and complex, and are made more so by the behaviors of other humans also driving on the road. Freeing the human occupant from the mundane task of driving and inviting them to relax and potentially even turn their attention to other tasks is a key selling point of automated vehicles. However, in a driver assist scenario, this invitation to relax or reduce focus can be in tension with the need to quickly and unexpectedly have a human become the driver. While research suggests some interesting, counterintuitive relationships between human attention to other tasks and transitions into the driving role:[173] 15.3% of all accidents are caused by distractions or inattention today.[174] In the driver assist archetype, safety demands successfully navigating these Handoffs between human and technical actors.

Second, an inebriated or intoxicated human is less able to handle the cognitive and physical demands of a call to action. While driving drunk causes accidents, being unexpectedly and jarringly called to drive may cause more. Inebriated humans are unlikely to foresee a call to drive and may get behind the wheel, lulled by the belief that they will not need to drive, rather than rely on a designated driver or call a cab. This might lead the driver assist archetype to increase the number of inebriated humans behind the wheel even if it decreases accidents caused by drunk drivers.[175] At the same time, it introduces the possibility that vehicles place less faith in their human occupants as controllers and prioritize the authority of the technical system. Problems associated with that approach are apparent with the example of two Boeing 737 MAX passenger planes crashing in 2018 and 2019.[176] In each case, it appears that the pilots fought unsuccessfully against a malfunctioning automation system that repeatedly pushed the nose of the plane downward.[177]

173. *See, e.g.*, Miller et. al., *Distraction Becomes Engagement*, *supra* note 115 (finding that, contrary to common assumption that in-car entertainment would increase accidents due to distraction, watching videos or reading tablets reduced behaviors indicative of drowsiness and did not impair reaction time: discussing other work suggesting that engaging fallback drivers in "mentally activating activities" may be safer because it reduces the chance of a drowsy individual being asked to assume the wheel).

174. CASUALTY ACTUARIAL SOC'Y AUTOMATED VEHICLES TASK FORCE, *supra* note 171, at 13.

175. *Id.* at 11.

176. *See* NAT'L TRANSP. SAFETY BD., SAFETY RECOMMENDATION REPORT: ASSUMPTIONS USED IN THE SAFETY ASSESSMENT PROCESS AND THE EFFECTS OF MULTIPLE ALERTS AND INDICATIONS ON PILOT PERFORMANCE 2–3 (2019) (describing the Lion Air Flight 610 and Ethiopian Airlines Flight 302 accidents, both of which involved Boeing 737 MAX 8 planes).

177. *Id.*

The difficulty of coordinating between human and technical drivers has led some manufacturers to pursue other autonomous vehicle futures.[178]

Existing case law and guidance interpreting the National Traffic and Motor Vehicle Safety Act (NTMVSA)[179] provides guidance on the extent to which vehicle manufacturers and others need to anticipate divergent—even deviant—behavior, including interactions between original, replacement, and after-market components. NTMVSA establishes that, for purposes of a recall under NTMVSA, a motor vehicle contains a "defect" when it fails in normal operation,[180] including failures resulting from reasonably expected or "ordinary abuse."[181] However, NTMVSA provides an affirmative defense where a manufacturer can show that "the failures were attributable to gross and unforeseeable owner abuse or unforeseeable neglect of vehicle maintenance."[182] The law therefore requires vehicle manufactures to consider "reasonably foreseeable," "reasonably contemplatable," and "ordinary abuse,"

178. *Id.*; *see also* John R. Quain, *Makers of Self-Driving Cars Ask What to Do with Human Nature*, N.Y. TIMES (July 7, 2016), https://www.nytimes.com/2016/07/08/automobiles/wheels/makers-of-self-driving-cars-ask-what-to-do-with-human-nature.html (describing Google's conclusion that "the only safe way to proceed is to take the driver out of the equation" and Volvo's pursuit of "Level 4 cars . . . that don't require any driver input aside from setting a destination" to reduce the safety risks posed by human driving error).

179. National Traffic and Motor Vehicle Safety Act of 1966, 15 U.S.C. §§ 1381, 1399, 1411 (1966) (repealed 1994) (requiring manufacturers that obtain knowledge of a safety-related defect to notify the Secretary of Transportation and remedy the defect, as well as authorizing the Secretary to order a manufacturer to remedy a safety-related defect).

180. *United States v. Gen. Motors Corp.*, 518 F.2d 420, 427 (D.C. Cir. 1975). A defect under the NTMVSA is distinct from a defect under products liability law because the showing of defect required for purposes of regulatory-inspired notification is less than that required to prove a defect for product liability purposes. *See id.* However, recall letters and evidence are generally admissible for the limited purpose of showing that the defect existed or arose in a product while in the hands of the manufacturer. 5 Products Liability § 57.05 (2020); *see also* James T. O'Reilly, *Dialogue with the Designers: Comparative Influences on Product Design Norms Imposed by Regulators and by the Third Restatement of Products Liability*, 26 N. KY. L. REV. 655, 666 (1999) (explaining that, while the Third Restatement recognizes violation of a product safety requirement as a basis for liability, this alone is not enough to prevail, as "the court would examine the law or rule; determine whether it applies (taking into consideration the exclusions and qualifiers that the law or rule provides); explore the historical record of the statutory findings, statutory purpose clause, or rulemaking preamble explaining the purposes of the regulation; and compare the law's or rule's purposes of preventing risk, with the scenario of actual harm [the] plaintiff has suffered").

181. *Gen. Motors Corp.*, 518 F.2d at 434, 438 ("The protection afforded by the [Safety] Act was not limited to careful drivers who fastidiously observed speed limits and conscientiously complied with manufacturer's instructions on vehicle maintenance and operation. . . . [The statute provides] an added area of safety to an owner who is lackadaisical, who neglects regular maintenance . . . .").

182. *Id.* at 438.

thus taking into account the expected range of actual operations, past experiences with comparable vehicles, and information provided to owners about the capabilities of a vehicle. The regulatory framework's focus on defects that arise from reasonably foreseeable misuse is particularly significant in that, if the government can establish the existence of more than a *de minimis* number of failures in a safety related component, it neither needs to show what caused the failure nor rule out misuse by the user if it was "reasonably foreseeable."

NHTSA's most recent guidance document on autonomous vehicle policy gives an indication of the potential importance of its recall authority,[183] including the associated record-keeping and reporting requirements in the autonomous vehicles landscape.[184] It requests that manufacturers provide it with a "safety assessment letter" that details how they are attending to fifteen broadly defined areas that might affect safety.[185] The NHTSA issued an "Enforcement Guidance Bulletin" affirming the performance orientation of defect analysis in its recall authority,[186] stating

> Unreasonable risks due to predictable abuse or impractical recalibration requirements may constitute safety-related defects. Manufacturers have a continuing obligation to proactively identify and mitigate such safety risks. This includes safety risks discovered after the vehicle and/or equipment has been in safe operation.[187]

This Bulletin, while only a guidance document, offers insight into how NHTSA views its existing regulatory authority ought shape the autonomous vehicle landscape. The Bulletin emphasized the breadth of the NHTSA's authority over original, replaced, and after-market vehicle components, including software.[188] It also noted that NHTSA' s authority covers devices "manufactured, sold, delivered, or offered to be sold for use on public streets, roads, and highways with the apparent purpose of safeguarding users of motor vehicles against risk of accident, injury, or death," which could cover software

183. *See* NHTSA, U.S. DEP'T OF TRANSP., FEDERAL AUTOMATED VEHICLES POLICY: ACCELERATING THE NEXT REVOLUTION IN ROADWAY SAFETY 11, 50 (2016) [hereinafter "HAV POLICY"].

184. *See id.* at 50.

185. *Id.* at 15–16.

186. *See* NHTSA Enforcement Guidance Bulletin 2016-02: Safety-Related Defects and Automated Safety Technologies, 81 Fed. Reg. 65705, 65708 (Sept. 23, 2016) (explaining that the agency can rely on an engineering defect or technical cause of a safety defect, but "merely a 'non-de minimis' quantity" of failures could be sufficient to support a defect finding).

187. *Id.* at 65705–06 (citations omitted).

188. *See id.* at 65707 ("software (including, but not necessarily limited to, the programs, instructions, code, and data used to operate computers and related devices), and after-market software updates" are motor vehicle equipment within the meaning of the Act).

"that enables devices not located in or on the motor vehicle to connect to the motor vehicle or its systems."[189] For these reasons, it reminded suppliers of equipment that they too were bound by the notification duties for safety-related defects set out in the Act.[190] Importantly for this "driver assist" archetype, the Bulletin focused on the issue of human-machine coordination, emphasizing "[a] system design or configuration that fails to take into account and safeguard against the consequences of reasonably foreseeable driver distraction or error may present an unreasonable risk to safety."[191] Tort liability further shores up NHTSA's position that manufacturers cannot merely warn drivers to stay alert but must design for the foreseeable risks of distraction and inattention. Manufacturers and others must adopt fault-tolerant designs for driver assist whenever doing so would be a cost-effective method for reducing the risk of driver error.[192]

Beyond clarifying that known and foreseeable human failings must be accounted for in autonomous design, NHTSA has provided limited guidance. NHTSA's autonomous vehicle policy directs manufacturers and other entities to document processes for assessing, testing, and validating the human-machine interface issues so important in the driver assist archetype.[193] However, beyond directing that autonomous vehicles should include indicators that inform humans that the system is properly functioning, engaged, unavailable, malfunctioning, or requesting the human resume driving, it points manufacturers and others elsewhere for concrete guidance.[194]

189. *Id.* (citations omitted).

190. *See id.*

191. *Id.* at 65709 (offering three examples that touch on the safety implications of shifting interfaces and affordances including: a gearshift lacking standard tactile cues offered without a safety or method of effective warning to prevent a driver from exiting a vehicle that is not in park; a driver assist archetype that does not account for "reasonably foreseeable situations where a distracted or inattentive driver-occupant must retake control"; and a software system that is expected to last the life of the vehicle but does not receive secure updates which results in a safety risk).

192. Geistfeld, *supra* note 166, at 1627–28 (explaining that product liability requires "fault-tolerant product designs" ("[W]hen a safer design can reasonably be implemented and risks can reasonably be designed out of a product, adoption of the safer design is required over a warning that leaves a significant residuum of such risks.") and that the standard requires application of the risk-utility test, "which requires the product design to incorporate any safety feature costing less than the associated safety benefit").

193. *See* HAV POLICY, *supra* note 183, at 22. In addition to the human driver, manufacturers and others are directed to consider the human factor and communication needs of passengers, other vehicles, and pedestrians. *See id.*

194. *See id.* (directing entities to the SAE International, ISO, NHTSA, American National Standards Institute, and the International Commission on Illumination).

The core technical standard defining levels of automation provides very little direction on human-machine interactions. It describes actions essential to the coordination (such as monitoring),[195] roles (such as the "fallback-ready user"),[196] and aspects of humans ("receptivity"),[197] but provides little guidance about the intricacies of the delicate, interactive dance required of the human and technical actors. In levels 1 through 3, existing guidance emphasizes human authority (requiring technical actors to "disengage[] immediately upon driver request") and human responsibility (stating that human drivers must "supervise . . . and intervene to maintain safe operation" at levels 1 and 2 and must "verif[y] . . . readiness" and "determine[] . . . appropriate[ness]" of engaging the autonomous vehicle, remain "receptive to a request to intervene," and "determine[] whether and how to achieve minimal risk condition," at level 3).[198] At levels 4 and 5, the guidance emphasizes the greater authority of technical actors, allowing them to "permit[] engagement" of the driving automation system and "delay user-requested disengagement."[199] A 2016 NHTSA report found that, despite the importance of human-machine interaction issues to safety in increasingly autonomous vehicles, existing standards provided very limited guidance on human factors for safety.[200]

The importance of the complicated, coordinated actions between humans and technical actors for human life demands greater attention and activity by the NHTSA. More can be done to enable sound human-machine interaction research and design processes. As the autonomous policy requires, the NHTSA should hold public workshops and solicit external peer review to gather information to support the development of additional human-machine interaction guidance. Workshops and expert reviews should seek to import guidance from aviation safety, where recent events have starkly revealed the risks of misunderstandings between human and technical actors who share operational tasks. However, experts caution against use of the "aviation precedent" as "take-over procedures that might work effectively in aviation

195. SAE INT'L, *supra* note 22, at 12–13.

196. *Id.*

197. *Id.* at 14 (defining receptivity as "an aspect of consciousness characterized by a person's ability to reliably and appropriately focus his/her attention in response to stimulus").

198. *Id.* at 21–22.

199. *Id.* at 22–23.

200. *See* QI D. VAN EIKEMA HOMMES, NHTSA, ASSESSMENT OF SAFETY STANDARDS FOR AUTOMOTIVE ELECTRONIC CONTROL SYSTEMS 22 (2016) (reviewing ISO 26262: Road Vehicles–Functional Safety, MIL-STD-882E: Department of Defense Standard Practice–System Safety, DO-178C: Software Considerations in Airborne Systems and Equipment Certification, FMVSS: Federal Motor Vehicle Safety Standard, AUTOSAR: Automotive Open System Architecture, and MISRA C: Guidelines for the Use of the C Language in Critical Systems).

simply do not transfer to the ground vehicle case, regardless as to how much designers might like to think so or try to make it so."[201]

Addressing what's been historically called the "hours of boredom and moments of terror" problem[202]—but now manifests as the "months of monotony to milliseconds of mayhem" problem[203]—requires experts to distill insights. This problem also requires the NHTSA and others to produce guidance from the slim but growing set of autonomous vehicle crashes and the disengagement reports required by states such as California. These real-world autonomous vehicle case studies allow designers and policymakers to better understand the human-machine interaction challenges arising from the operational conditions in which different manufacturers are testing autonomous vehicles. Pursuing the driver assist archetype creates an urgent need to put human-machine interface issues "at the forefront of conceptualizing our future through technology, as opposed to 'sweeping up after the parade has gone by.' "[204] To date, policy makers in the United States have neglected the urgency and importance of this task.

B. DRIVERLESS CARS

Driverless autonomous vehicles sever the physical relationship between human drivers and vehicles. Human occupants cannot drive; instead, humans at physically distant locations can and at times must. Human occupants are freed of responsibility and liability. The car's occupants remain in the physical crumple zone, but the distant human fallback driver is now in the "moral crumple zone."[205] The real-time observation and communication needs of this physically distant human "fallback driver" destabilizes the role the car as a "place" plays in protecting privacy.[206]

201. Peter A. Hancock, *Some Pitfalls in the Promises of Automated and Autonomous Vehicles*, 62 ERGONOMICS 479, 484–85 (2019).

202. PETER A. HANCOCK & GERALD P. KRUEGER, NAT'L DEFENSE UNIV., CTR. FOR TECH. & NAT'L SEC. POL'Y, HOURS OF BOREDOM, MOMENTS OF TERROR: TEMPORAL DESYNCHRONY IN MILITARY AND SECURITY FORCE OPERATIONS (2010).

203. *Id.* at 3.

204. D. D. Woods, Presidential address of the Human Factors and Ergonomics Society: Watching People Watch People at Work (1999).

205. *See generally* Madeleine Clare Elish, *Moral Crumple Zones: Cautionary Tales in Human-Robot Interaction*, 5 ENGAGING SCI. TECH. & SOC'Y 40 (2019).

206. *See* Dorothy J. Glancy, *Privacy in Autonomous Vehicles*, 52 SANTA CLARA L. REV. 1171, 1219–25 (2012) (discussing protection for privacy rights associated with vehicles on public roads).

1. Repositioning the "Moral Crumple Zone"

While the scholarly consensus is "that elimination of a human driver will shift responsibility onto manufacturers as a matter of products liability law, with most tort litigation involving claims for design or warning defects,"[207] our attention here is one step down. It seems unlikely that even the driverless archetype will completely delegate control to the technical actors.[208] Within the car manufacturer, the human operator *qua* "fallback driver"—who must exist in the current testing environment, and, as we posit above, will inevitably persist in the driverless archetype due to material obstacles, equipment malfunctions, and unexpected events including hostile attacks—seems positioned in what Madeleine Clare Elish named the "moral crumple zone."[209] The displacement of the human in the car, coupled with their role as "fallback," or shall we say "failsafe," for a system presented as "driverless," brings attention to a particular set of political and ethical consequences.

Who are the remote "fallback drivers" in the driverless car future? Are these the content moderators and crowd workers of the future? Like the crowd workers performing a vast range of "microwork" behind the scenes and screens of today's AI driven platforms, as documented by Mary L. Gray and Siddharth Suri, these humans will be called into action to exercise human judgment where computation fails.[210] This work is likely to be a catastrophic mix of boring and high stakes. Like the "safety driver" implicated in the Uber fatality described above, will these humans, bored by the monotony of supervising machines designed to perform largely without supervision, find themselves asleep at the wheel, mired in guilt, and blamed for being unready or unable to quickly assume control for driving when the car demands?

As described above, the interfaces and affordances may do a better or worse job positioning or priming these "fallback drivers" for the quick action required. Will interfaces for remote human "fallback drivers" be designed like cockpits and aligned with the bespoke one-on-one driving experience elicited by the driverless car archetype, perhaps keeping them on edge and aware of the lived experience of passengers hurtling down a winding mountain road or

207. Geistfeld, *supra* note 166, at 1619–20.

208. *See id.* at 1630 (explaining that the NHTSA's ruling that Google's self-driving car is the equivalent of a human driver for federal regulatory purposes, and that this logic resolves the associated tort questions necessary to establish manufacturer liability despite the absence of case law "recognizing that a manufacturer incurs a tort duty for defective software").

209. Elish, *supra* note 205, at 41 (arguing that the "moral crumple zone" represents the misattribution of a failure in a complex socio-technical system to a human actor who had limited control over the behavior).

210. *See generally* MARY L. GRAY & SIDDHARTH SURI, GHOST WORK: HOW TO STOP SILICON VALLEY FROM BUILDING A NEW GLOBAL UNDERCLASS (2019).

inching through streams of rubbernecking traffic? Or will they mimic the bird's-eye view, inviting a more disinterested and less embodied experience of "fallback" driving? Given the presumption of minimal intervention captured in the term "fallback driver," one can imagine a single human safety operator managing numerous cars. Yet the stakes can be extraordinarily high if any single car requires human intervention, let alone several at once in the event of a disengagement due to a system malfunction or cybersecurity exploit that affects numerous vehicles.

The mindset and role evoked by the job description and requirements, employee training, and interface design will shape this new, online-crowd-workers perception of the fallback drivers' work. While rules in states like California currently set guidelines about job requirements—requiring drivers to obtain appropriate licenses and show competency with the skills relevant to particular driverless vehicles and requiring companies to submit training materials—it is unclear whether and how such requirements will persist when autonomous vehicle manufactures claim their driverless cars satisfy NHTSA safety standards.

The "last mile" of AI functionality in the driverless car archetype seems as likely to rely on human judgment as content management, facial recognition, and furniture identification. The question is whether these human drivers, though removed from the car, will nonetheless remain in the hot seat.

While many legal scholars have opined on the shift of liability to manufacturers for driver assist and driverless cars,[211] none have considered which specific humans within the manufacturer will bear the blame. The "moral crumple zone" "call[s] attention to the ways in which automated and autonomous systems deflect responsibility in unique and structural ways, protecting the integrity of the technological system at the expense of the nearest human operator."[212] As both the Volkswagen emissions scandal and the Arizona Uber crash that Elish reviews in her discussion[213] reveal, manufacturer liability for technical wrongdoing can be placed on different internal actors. There is a high likelihood that "fallback drivers" will be very low on the food chain, even more so than the Uber "safety-driver"—perhaps, at best, akin to the Uber and Lyft drivers of today and, at worst, akin to the

211. *See* Geistfeld, *supra* note 166, at 1619 n.25 (noting scholarly consensus that elimination of a human driver will shift responsibility onto manufacturers with respect to products liability law but divergence about exactly how liability claims will be sorted out and how to apportion responsibility among the manufacturer and other entities within the supply chain).

212. Elish, *supra* note 205, at 51–52.

213. *See id.* at 52–53 (describing how video footage of the safety-driver glancing down into her lap led both police and reporters to blame her for the accident).

low wage offshore workers of today's *Ghost Work* force. Battles over the legal status and rights of today's AI-backstopping workforce may seem more central when lives hang more fully off their work and the consequences of holding them accountable for failures—placing them in the crumple zone—seems less commensurate with their pay and more personally and legally disastrous.

C. CONNECTED CARS

If driverless cars destabilize the relationship between physical presence and driving, connected cars destabilize the boundary of the "car" itself. Connected cars are more appropriately viewed as one element of a connected city or environment. The physical, informational, and legal dependencies needed to stabilize a connected vehicles future present the most radical break from current arrangements. It requires material and human elements to actively support vehicle mobility. From embedding streets and signs with computation and communication to rerouting pedestrian and bike traffic, the connected cars archetype demands legibility and predictability of other human and material actors. This archetype places intelligence and action largely outside of the vehicles themselves. The complex coordination inherent in the connected cars archetype depends upon a bird's-eye view and complex algorithms. This in turn leans heavily toward centralized models of vehicle ownership and data collection, which creates questions about competition and data governance. Because the state has the potential to be either an owner or a regulator of private owners, this centralization opens up some distinct opportunities to enhance the extent to which equitable access and environmental issues are considered within the frame of autonomous vehicle futures policy.

1. Legibility

The complexity of coordination required for streaming traffic flows and other imagined goods of the connected car archetype rely heavily on algorithms. These algorithms demand consistent, predictable, and machine-readable environments. The heightened levels of dependence on the accuracy and reliability of data coming into the connected car environment places a larger burden on the built environment and human and other occupants to be legible. In this archetype, cars, roads, and street signs may all be viewed as critical infrastructure.

This portends either a massive re-instrumentation of urban environments or a tight alignment between connected cars and new urban environments such as the now defunct Sidewalk Labs Toronto Waterfront project that can be architected from the ground up and the network down. Retrofitting existing environments is cumbersome and expensive, and coexistence with non-connected cars is difficult and dangerous.

It is easy to imagine that small acts of rebellion—tagging stop signs—previously viewed as low level crimes could be viewed and prosecuted more seriously due to the potential implications for human safety. While a human can readily comprehend the meaning of a stop sign despite many forms of graffiti, machine learning algorithms are less resilient. As on the internet, where tagging websites has at times been considered and prosecuted as a federal crime, the meaning and effect of graffiti may change as safety depends more and more on legibility. As in the airport where we perform for security screening machines by taking off shoes, removing certain items of clothing, and items from pockets and bags to make ourselves and our belongings more legible, the connected cars environment might require us to enact our humanness in prescribed ways.

Perhaps norms will evolve as parents urge their children to carry smart phones set to signal human presence to the connected car network. Perhaps such signaling will be legally required in some contexts or efforts at obfuscation subject to criminal charges. If human safety hangs in the balance, all sorts of soft and hard demands for cooperation could arise.

2. Ownership and Centralization

Each archetype is currently more aligned with particular ownership models—of vehicles or of infrastructure and information flows. While driver assist models support private individual ownership and driverless models lend themselves to TNC fleet management, connected cars models extend beyond the vehicle to also include static infrastructure. Ownership and business models influence the ability of regulators to foster public goods, such as equitable access to transportation, or reduce the production of negative externalities, such as pollution.

The connected car archetype offers perhaps the starkest example of this. The communication, control, and data processing platforms that control vehicles, as well as the vehicles themselves in this archetype, may be offered by technology companies or alternatively by—or in cooperation with—cities, states, roads organizations, or other governing bodies. Either way, this archetype seems certain to discourage today's dominant personal ownership model and position data about mobility as a collective resource.

3. Privacy

As in the smart city and smart grid context, issues of data governance will demand renewed attention. The privacy issues arising from massive collections of individuals' data demand close scrutiny, but so do questions about the extent to which analysis and use of these new data troves could serve public purposes.

The robust, real-time monitoring and data collection from the user and continuous access to the software ecosystem of cars presented in each archetype create new privacy and security challenges, as well as issues for competition and consumer protection.[214] Even where connectivity will not be essential for active control, it will likely continue to be an intrinsic part of the vehicle "service" due to the need to update software to address emerging security and safety risks, which raises further ethical and political questions. Some have argued that if Android driving platforms—or some equivalent—became the norm for private vehicles, we might see "platform economy" surveillance dynamics at work even in those privately owned and operated vehicles.[215] Current battles around consumers' and non-manufacturers' rights to repair machinery with embedded code will no doubt escalate.[216]

There is little question that data produced through interaction with the applications and platforms of TNCs, as well as communications between human occupants and remote operators/drivers, will be collected and used by companies to optimize performance and improve safety. Whether they can or must be transmitted to other entities for the sake of informing or enforcing public policies, supporting ancillary commercial activities such as behavioral advertising, or increasing competition is less settled. Questions about the identifiability, retention, and permitted uses of data transmitted among automobiles and between automobiles and infrastructure are an active site of policy making and remain unsettled.[217]

For instance, driverless cars will likely record video footage from inside the cabin. Today's in-cabin recording systems and dash-cams typically only retain footage for a short time before overwriting older data.[218] Retention of video footage is triggered by events like heavy braking or driver intervention. Without a driver to ensure important footage is maintained, for instance, after

214. *See generally* Mulligan & Bamberger, *supra* note 69 (describing potential for the security-necessary, over-the-air updates to compromise security, limit competition, and undermine consumer protections and privacy, and the need for regulations to address such potential risks).

215. *See, e.g.*, Luis F. Alvarez León, *Eyes on the Road: Surveillance Logics in the Autonomous Vehicle Economy*, 17 SURVEILLANCE & SOC'Y 198 (2019).

216. *See generally* Mulligan & Bamberger, *supra* note 69.

217. *See* HARDING, *supra* note 131, at 144–57 (2014) (discussing privacy issues, draft privacy impact assessment, conflicts between privacy and other goals such as recalls, and the range of potential technical and policy controls).

218. *See, e.g.*, *Garmin Offers Dash Cam*, FLEETOWNER (Mar. 19, 2014), https://www.fleetowner.com/technology/article/21687441/garmin-offers-dash-cam (describing Garmin dash cam recording practices as: "When an incident—like hard braking or a collision—is detected by the built-in G-Sensor, Dash Cam knows to save the current, last and next recordings, preserving a complete record of the event").

an accident, commercial autonomous vehicle in-cabin surveillance will likely require computational pattern recognition or computer vision systems that continuously evaluate or profile the behavior of all occupants without necessarily transmitting or continuously recording all content. But if in-cabin video footage is streamed and potentially captured to support remote operation, it may be an attractive method for evaluating the experience of users and deterring property damage or other forms of undesirable behavior.[219]

Various state and federal actions have been taken to address some of the privacy issues arising from increased data collection in increasingly automated and connected cars. Existing federal law governing access and use of data collected by "event data recorders" (EDRs) set important privacy precedents.[220] California law requires either notice to users of the personal information collected by the autonomous technology that is not necessary for the safe operation of the vehicle and how it will be used or the anonymization of any such data.[221] This recent action builds on California's strong history of protecting privacy in the automotive sector. For example, California enacted the first law requiring automobile manufacturers that install EDRs in vehicles to disclose that fact in the owner's manual and limit the access and use of EDR data to either vehicle service and repair or for public safety purposes after the removal of identifiers.[222] California has also enacted legislation that limits abusive use of GPS data in the rental car market.[223]

Unfortunately, existing federal protections do not address the privacy issues raised by autonomous vehicles, and the NHTSA continues to shirk responsibility for addressing them. The privacy protections afforded by federal law address data that is captured by EDRs, which are defined as being *within*

219. *See* Meredith Broussard, *The Dirty Truth Coming for Self-Driving Cars*, SLATE (May 16, 2018, 9:00 AM), https://slate.com/technology/2018/05/who-will-clean-self-driving-cars.html.

220. *See* 49 U.S.C. § 30101 note (2015) (Driver Privacy Act of 2015) (establishing that data retained by an EDR is the property of the owner or lessee of the car and generally requires a court order for others to access it).

221. *See* CAL. CODE REGS. tit. 13, § 227.38(b)(1) (2018).

222. CAL. VEH. CODE § 9951 (West 2019).

223. CAL. CIV. CODE § 1939.23 (West 2019). The law was preceded by an action by the California Attorney General's Office under the state Business and Professions Code against a rental car franchise for failing to adequately notify renters of the presence of a GPS device in their rental vehicles. *See* Press Release, Office of the Att'y Gen., Attorney General Lockyer Announces $700,000-Plus Consumer Protection Settlement with State's Largest Independent Car Rental Firm (Nov. 9, 2006), https://oag.ca.gov/news/press-releases/attorney-general-lockyer-announces-700000-plus-consumer-protection-settlement.

the car.[224] In addition, the protections explicitly exclude audio and video data.[225] As described above, autonomous vehicles transmit data outside the car and rely on a range of data, including audio and video data, to support safety and other functionalities.[226] The privacy implications of this detailed data about the drivers and occupants of cars being streamed and stored outside vehicles require new regulations.[227]

The NHTSA's most recent guidance document on autonomous vehicle policy not only omits privacy guidance[228] but also eschews responsibility for it, stating that "privacy is not directly relevant to motor vehicle safety."[229] Furthermore, while the guidance document contains "best practices for states," it does not mention the privacy issues nor recommends approaches to address them.[230] In stark contrast, the NHTSA has provided detailed consideration of the privacy issues raised by proposed regulations for V2V and V2I communications.[231]

On the other hand, the Federal Trade Commission (FTC), the lead federal consumer protection agency, has indicated that privacy and security issues related to cars are fully within their sights and authority.[232] The transparency

224. *See* 49 C.F.R. § 563.5(b) (2011) ("Event data recorder (EDR) means a device or function in a vehicle that records the vehicle's dynamic time-series data during the time period just prior to a crash event . . . or during a crash event . . . , intended for retrieval after the crash event . . . [where] the event data do not include audio and video data.").

225. *See id.* ("[T]he event data do not include audio and video data.").

229. *See* discussion *supra* Section III.C.

227. Shane Prevost & Kettani Houssain, *On Data Privacy in Modern Personal Vehicles*, 2019 PROC. 4TH INT'L CONF. ON BIG DATA & INTERNET OF THINGS 1, 2–3 (describing the wealth of telematic and other data that a Tesla vehicle generates and transmits and the limitations of current federal privacy laws).

228. NHTSA, U.S. DEP'T OF TRANSP., AUTOMATED DRIVING SYSTEMS 2.0: A VISION FOR SAFETY (2017) [hereinafter "VISION FOR SAFETY"]. This is an about-face from the 2016 policy guidance which addressed privacy issues, reflecting the Obama Administration's commitment to privacy as stated in the *White House Consumer Privacy Bill of Rights*, as well as ethical implications of AV algorithms. *See* HAV POLICY, *supra* note 183, at 19. The 2016 guidance requested companies provide information about privacy and ethical implications in Safety Assessment Letters filed with NHTSA's general counsel's office for each autonomous vehicle. *See id.* at 15.

229. *Automated Driving Systems: FAQ*, NHTSA, https://www.nhtsa.gov/vehicle-manufacturers/automated-driving-systems#automated-driving-systems-faq (last visited Sept. 1, 2020) (noting the important role the Federal Trade Commission plays in protecting consumer privacy in the connected car space).

230. VISION FOR SAFETY, *supra* note 228, at 19–24.

231. *See* Federal Motor Vehicle Safety Standards; V2V Communications, 82 Fed. Reg. 3854 (proposed Jan. 12, 2017) (to be codified at 49 C.F.R. pt. 571).

232. *See, e.g.*, Ashkan Soltani, *Booting Up a New Research Office at the FTC*, FED. TRADE COMM'N (Mar. 23, 2015, 11:00 AM), https://www.ftc.gov/news-events/blogs

recommendation in the 2016 NHTSA autonomous vehicle policy, which called on manufacturers and other relevant entities to "provide consumers with accessible, clear, meaningful data privacy and security notices/agreements which should incorporate the baseline protections outlined in the White House Consumer Privacy Bill of Rights and explain how [they] collect, use, share, secure, audit, and destroy data generated by, or retrieved from, their vehicles,"[233] provided an important hook for the FTC's enforcement authority.[234] While companies may nonetheless provide some information about their privacy practices, the omission of privacy from NHTSA's current guidance sidelines privacy protection. In the absence of federal standards, states will fill the gap, creating an increasingly complex privacy regulatory framework for manufacturers, other vendors, and consumers.

4. *Changing the Values Aperture: Transportation Access and Environmental Impact*

At stake in these different formations is control over system functionality, residing in the hands of either highly efficient actors animated by profit or bureaucratized public entities responsive to a potentially distinct set of public goals, while subject to different forms of regulation and oversight or some hybrid of both. At first glance, one might view this as hinging fully on private versus public ownership of cars, infrastructure, and data, but such a view would miss an important site of action.

The different business models that might arise under the three archetypes invite in different potential regulators with different abilities to push for public

/techftc/2015/03/booting-new-research-office-ftc (describing the Office of Technology Research and Investigation's research on the Internet of Things, including connected cars); Donald S. Clark, Director, FTC, Comment Letter on the Advance Notice of Proposed Rulemaking Regarding Federal Motor Vehicle Safety Standards: Vehicle-to-Vehicle (V2V) Communications Pursuant to Chapter 301 of the Department of Transportation, Motor Vehicles and Driver Programs (Oct. 20, 2014), https://www.ftc.gov/system/files/documents/advocacy_documents/federal-trade-commission-comment-national-highway-traffic-safety-administration-regarding-nhtsa/141020nhtsa-2014-0022.pdf (raising privacy and cybersecurity issues); STEPHANIE GILLEY, FED. TRADE COMM'N, INTERNET OF THINGS WORKSHOP 235–91 (2013), http://www.ftc.gov/sites/default/files/documents/public_events/internet-things-privacy-security-connected-world/final_transcript.pdf.

233. HAV POLICY, *supra* note 183, at 19.

234. *See* Jessica L. Rich, FED. TRADE COMM'N, Comment Letter on "Federal Automated Vehicles Policy," at 3 (Nov. 21, 2016), https://www.ftc.gov/system/files/documents/advocacy_documents/comment-jessica-l-rich-director-bureau-consumer-protection-ftc-national-highway-traffic-safety/ntsb_letter_comment112116.pdf (explaining that the "transparency principle, which requires OEMs to have public-facing privacy policies, is an important one because it would permit the FTC to take action against companies that misstate their information collection and use practices").

priorities—private or public ownership is only the start of the conversation. The connected cars archetype invites in distinct regulators, with unique ambits, tools, dispositions, and relationships with stakeholders. For example, in California, the connected cars archetype will bring the CPUC into the mix. The CPUC's authority includes environmental, equity, and other public concerns intertwined with mobility, not just safety. Unlike the driver assist archetype and driverless car archetype, the connected cars archetype may allow public entities to prioritize agendas beyond safety—including equitable access and urgency—in vehicle routing. The CPUC has also broken new ground dealing with privacy and security issues in the context of demand response energy systems (the "smart grid"), giving them a sound basis for considering privacy and security issues in the "smart grid" of cars. Where NHTSA has deferred privacy at the federal level to the FTC, the CPUC could step in to establish farther reaching data governance policies, as it has in other areas. This could include policies that address access to data for public purposes—such as evaluating impact, research, or oversight—and privacy rules that address issues of data identifiability, purpose limitations, portability, and limitations on government use for non-transportation law enforcement activities, like policing or immigration. The NHTSA and the California Department of Motor Vehicles (DMV), like other state motor vehicle departments, lack the same breadth of authority.

For example, while the California DMV regulates many relevant aspects of autonomous vehicles, the CPUC has extraordinarily broad regulatory authority over TNCs and Charter-Party Carriers—both likely actors in this archetype—and can create new regulations where they believe necessary.[235] Today, CPUC regulations tackle important political and ethical issues. For example, the CPUC requires TNCs to submit annual reports with detailed information on aspects of their operations necessary to address public safety and to advance equitable access across racial and ethnic demographics.[236] CPUC regulations also require TNCs offering fare-splitting services to report on the environmental impact of fee-splitting operations as part of their annual reports.[237] Some suggest that reducing car ownership could lower the

235. The Charter-Party Carriers' Act states in part that "the commission may supervise and regulate every charter-party carrier of passengers in the State and may do all things . . . which are necessary and convenient in the exercise of such power and jurisdiction." CAL. PUB. UTIL. CODE § 5381 (West 2019).

236. *See* Decision Adopting Rules and Regulations to Protect Public Safety While Allowing New Entrants to the Transportation Industry, Rulemaking 12-12-011, CPUC Decision 13-09-045, at 29–33 (Sept. 19, 2013).

237. *See* Decision on Phase II Issues and Reserving Additional Issues for Resolution in Phase III, Rulemaking 12-12-011, CPUC Decision 16-04-041, at 59 (April 21, 2016).

environmental impacts of transportation in comparison to current individual ownership models, but research suggests a more complicated environmental calculus.[238] The CPUC's authority over TNCs gives it the ability to obtain data to make independent assessments about the environmental impacts of current models. Consistent with its broad mandate, the CPUC also has the authority to potentially adopt additional regulations to advance public values, despite the business model which may well concentrate ownership of vehicles, data, and infrastructure in private hands. Regardless, these dynamics are complex and clearly constitute a spectrum with different ownership and operating configurations that have different implications for public goods, are subject to different regulators with different powers, and are likely to be found in different applications instituted in different geographies and jurisdictions.

5. Coda: Redefining Safety

We previously introduced historian Peter Norton's argument that the meaning of safety is fluid and contingent.[239] Regardless of which autonomous vehicle future society pursues, we are poised once again for a paradigmatic shift in the meaning of safety from crashworthiness back to crash avoidance. While the shift—from crash avoidance to crashworthiness—that Norton documented was triggered by safety advocates who sought to place greater responsibility for safety on the automobile industry and the automobiles they produced, today's shift is triggered by technology. Each archetype reallocates some responsibility from the driver to the manufacturer. The driverless car archetype and connected cars archetype shift responsibility and liability quite heavily toward manufacturers. We have come full cycle from crash avoidance to crashworthiness back to crash avoidance again.

V. CONCLUSION

In this Article, we introduced the Handoff model and attempted to demonstrate its utility through an analysis of autonomous vehicles. The goal has been to demonstrate how the Handoff model affords unique and critical insights into the operation of these systems—in terms of new components and modes of acting—that have dramatic consequences for both human and

238. *See* REGINA R. CLEWLOW & GOURI SHANKAR MISHRA, DISRUPTIVE TRANSPORTATION: THE ADOPTION, UTILIZATION, AND IMPACTS OF RIDE-HAILING IN THE UNITED STATES (2017) (associating TNC use with a net six-percent reduction in overall public transit use in seven major metropolitan areas (Boston, Chicago, Los Angeles, New York, the San Francisco Bay Area, Seattle, and Washington, D.C.) and concluding that forty-nine to sixty-one percent of trips taken by TNC would not have been made at all, or would have been made by walking, biking, or public transit).

239. *See supra* 115 and note 36.

societal values. In our view, this is a critical ameliorant to the focus on the ongoing transition of control into computational components, instead showing the structural, political and ethical stakes of those changes. In the autonomous vehicles context, it takes us beyond the abstract political claims associated with different transport models and their different ideas of utopia and, in breaking down how those different systems actually work, reveals the more nuanced political and ethical implications. Today the *lingua franca* of autonomous vehicle policy centers technology, framing increased automation as the goal and the good. But values should lead and the choice of which autonomous vehicle future to pursue is first a political and ethical one. Leading with values tools like the Handoff model helps us see past the technological to the political and ethical stakes. The entangled and contingent nature of values and specific regulatory institutions in the United States makes the landscape particularly fraught. Choosing one autonomous vehicle future need not be better or worse for privacy, for example, but some will surely require the adoption of more new policies. While some political goals may be better served by particular autonomous futures, it is more likely that, by carefully reasoning about Handoffs and coupling technical innovation with an equal share of policy innovation, we can co-create visions of autonomous vehicles that suit our ethics and politics.