33:2 BERKELEY TECHNOLOGY LAW JOURNAL

2018

Pages

365

to

606

Berkeley Technology Law Journal

Volume 33, Number 2

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 Boalt Hall
Berkeley, California 94720-7200
btlj@law.berkeley.edu
http://www.btlj.org

BERKELEY TECHNOLOGY LAW JOURNAL

VOLUME 33 NUMBER 2 2018

TABLE OF CONTENTS

ARTICLES

SUBSCRIBER INFORMATION

The *Berkeley Technology Law Journal* (ISSN1086-3818), a continuation of the *High Technology Law Journal* effective Volume 11, is edited by the students of the University of California, Berkeley, School of Law and is published in print three times each year (March, September, December), with a fourth issue published online only (July), by the Regents of the University of California, Berkeley. Periodicals Postage Rate Paid at Berkeley, CA 94704-9998, and at additional mailing offices. POSTMASTER: Send address changes to Journal Publications, 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 33 BERKELEY TECH. L.J. ___ (2018).

BTLJ ONLINE

The full text and abstracts of many previously published *Berkeley Technology Law Journal* articles can be found at http://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 the Express*O* and 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 Express*O* submission website can be found at http://law.bepress.com/expresso and the Scholastica submission website can be found at https://scholasticahq.com/law-reviews.

Citations. All citations should conform to THE BLUEBOOK: A UNIFORM SYSTEM OF CITATION (Columbia Law Review Ass'n et al. eds., 20th ed. 2015).

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

COOLEY LLP

HOGAN LOVELLS

FENWICK & WEST LLP

ORRICK, HERRINGTON & SUTCLIFFE LLP

WHITE & CASE LLP

Benefactors

COVINGTON & BURLING LLP

MORRISON & FOERSTER LLP

FISH & RICHARDSON P.C.

SIDLEY AUSTIN LLP

JONES DAY

WEIL, GOTSHAL & MANGES LLP

KIRKLAND & ELLIS LLP

WILMER CUTLER PICKERING HALE AND DORR LLP

LATHAM & WATKINS LLP

WILSON SONSINI GOODRICH & ROSATI

MCDERMOTT WILL & EMERY

WINSTON & STRAWN LLP

Corporate Benefactors

BLOOMBERG LAW

COMPUTER & COMMUNICATIONS INDUSTRY ASSOCIATION

CORNERSTONE RESEARCH

FUTURE OF PRIVACY FORUM

GOOGLE, INC.

HEWLETT FOUNDATION, THROUGH THE CENTER FOR LONG-TERM CYBERSECURITY

INTEL

INVENTIONSHARE

LITINOMICS

MICROSOFT CORPORATION

MOZILLA

NERA ECONOMIC CONSULTING

NOKIA

PALANTIR

RLM TRIALGRAPHIX

THE WALT DISNEY COMPANY

Members

Baker Botts LLP	Kilburn & Strode
Baker & McKenzie LLP	Kilpatrick Townsend & Stockton LLP
Crowell & Moring	Knobbe Martens LLP
Desmarais LLP	Morgan, Lewis & Bockius LLP
Durie Tangri LLP	Paul Hastings LLP
Finnegan, Henderson, Farabow, Garrett & Dunner, LLP	Ropes & Gray LLP
GTC Law Group LLP & Affiliates	Simpson Thacher & Bartlett LLP
Haynes and Boone, LLP	Troutman Sanders LLP
Hickman Palermo Becker Bingham	Turner Boyd LLP
Irell & Manella LLP	Van Pelt, Yi & James LLP
Keker Van Nest & Peters LLP	Weaver Austin Villeneuve & Sampson LLP

BOARD OF EDITORS 2017–2018

Executive Board

Editor-in-Chief
CHRISTIAN CHESSMAN

Managing Editor
DUSTIN VANDENBERG

Senior Articles Editors
ALICE CHI
JON MADDERN
ROBERT OLSEN

Senior Executive Editor
TAMARA WIESEBRON

Senior Production Editor
KRISTOFER HATCH

Senior Scholarship Editor
JOE CRAIG

Senior Annual Review Editors
VANESSA ING
JOYCE LI

Senior Online Content Editor
CHANTE WESTMORELAND

Editorial Board

Submissions Editors
CHRISTOPHER BROWN
AMIT ELAZARI

Production Editors
LOUISE DECOPPET
SAFFA KHAN
MEGAN MCKNELLY
CHELSEA MORI

Technical Editors
NADIA KALE
DANIEL LUECKE
AYN WOODWARD

Annual Review Editors
MARIA BELTRAN
NIR MAOZ

Notes & Comments Editors
BRITTANY JOHNSON ANDREW NGUYEN

Symposium Editors
DARIUS DEHGHAN
JESSICA HOLLIS

Web & Technology Editors
JOHN HAZELWOOD
TED KANG

Online Content Editor
KATIE BURKHART

Podcast Editor
ANTHONY BEDEL

LLM Member Relations Editors
JONATHAN DEBBI
MARTYNA SKRODZKA

Member Relations Editor
BARCLAY OUDERSLUYS

Alumni Relations Editor
ERICA SUN
KEVIN CHIU

External Relations Editor
BLAKE MEREDITH

Articles Editors

TIANA BAHERI
ALEX BARATA
BRANDON CHAVEZ
CHRIS CHUANG
ERIC CHUANG
KATHARINE CUMMINGS
MARK JAYCOX
YARDEN KAKON
LAURA KELLEY
AARON LEE
DINA LJEKPERIC
ANGELA LYONS-JUSTUS
CHARLES MILLER
BIHTER OZEDIRNE
AAMIR VIRANI
ELLE XUEMENG WANG

MEMBERSHIP

Vol. 33 No. 2

Associate Editors

LORRAINE ABDULAHAD
NIYATI AHUJA
ROBERTA AMORIM
BLAKE ANDERSON
CHELSEA ANDRE
NICHOLAS CALCATERRA
SAVANNAH CARNES
STELLA CHANG
DANIEL CHASE
INAYAT CHAUDHRY
GILBERT CHOI
RIYANKA ROY CHOUDHURY
NOMI CONWAY
HUGO CUGNET
TRENTON DAVIS
JOHN DETERDING
GRACE FERNANDEZ
YESENIA FLORES
SREYA GANGULY
KATIE GONZALEZ
ELIZA GREEN
ANUSHREE GUPTA
KAREN GRAEFIN VOM HAGEN
MICHAEL HOMER
JONATHAN HUANG
VICTORIA HUANG
CAROLINA JUVIN
ALEXANDER KROIS
HYUN KYU LEE
YUAN LI
JULIA LIPIZ
DENISE LOUZANO
SAM MILLER
ARUNDHATI NAYUDU
KATHERINE NOLAN
DEBBIE OH
LARA OLAFSDOTTIR
PAYMANEH PARHAMI
SANJANA PARIKH
ANJELI PATEL
AYESHA RASHEED
COLIN RAVELLE
COURTNEY REED
NOELLE REYES
ALYSE RITVO
AYELET ROSENTAL
ELIZABETH FREEMAN ROSENZWEIG
MIRANDA RUTHERFORD
ARPITA SENGUPTA
KELLY SERANKO
AISLINN SMALLING
WESLEY TIU
MEI XUAN
FAN YANG
LI ZHANG
EVAN ZIMMERMAN

Members

DIANE AGUIRRE-DOMINGUEZ
ANANDITA ARORA
LUKE BLACKETT
NICHOLAS BOLDUC
LAUREN CARROLL
CAROLINE YEN-RON CHEN
SIYING CHEN
CONCORD CHEUNG
CHANTE ELIASZADEH
JORDAN FRABONI
CHRIS GAO
YESOL HAN
SPENCER HAZAN
MEHTAB KHAN
SINDHU KOMMI
RYAN KWOCK
PING LIU
SABRINA MCGRAW
FEI MO
CRISTINA MORA
SAISHRUTI MUTNEJA
SADAF NAKHAEI
SILVIA SEGADE
EMRE YUZAK
TIANYUAN ZHUANG

BTLJ ADVISORY BOARD

BERKELEY CENTER FOR LAW & TECHNOLOGY 2017–2018

OPEN DATA, GREY DATA, AND STEWARDSHIP: UNIVERSITIES AT THE PRIVACY FRONTIER

Christine L. Borgman†

ABSTRACT

As universities recognize the inherent value in the data they collect and hold, they encounter unforeseen challenges in stewarding those data in ways that balance accountability, transparency, and protection of privacy, academic freedom, and intellectual property. Two parallel developments in academic data collection are converging: (1) open access requirements, whereby researchers must provide access to their data as a condition of

---

DOI: https://doi.org/10.15779/Z38B56D489

† Distinguished Professor and Presidential Chair in Information Studies, University of California, Los Angeles. This Article is based on the Tenth Annual Berkeley Law Privacy Lecture, hosted by the Berkeley Center for Law and Technology on November 16, 2017. http://christineborgman.info

Full disclosure: The author is actively engaged in the University of California activities mentioned herein. She was a founding member of the UCLA Privacy and Data Protection Board, a member of the PISI Steering Committee, Co-Chair of the UCLA Data Governance Task Force, and currently is Chair of the University of California Academic Computing and Communications Committee (UCACC) (2017–2018 academic year; Vice Chair 2015–2017). In her role as a UCACC officer, she is a member of the UC Office of the President Cyber Risk Governance Committee (2015–2018). She has been a member of the Advisory Board to the Electronic Privacy Information Center (EPIC) since its founding in 1994 and served on the EPIC Board of Directors from 2010 to 2017. The opinions in this Article are her own.

Acknowledgements are due to the many colleagues in the University of California who have aided, abetted, and supported these privacy initiatives: Amy Blum, Jim Chalfant, Dana Cuff, Jim Davis, Jerry Kang, David Kay, Leah Lievrouw, Gene Lucas, Maryann Martone, Joanne Miller, Jan Reiff, Sheryl Vacca, Kent Wada, Scott Waugh, Shane White, and other members of the PISI and DGTF committees. My research group at the UCLA Center for Knowledge Infrastructures provided essential critique and commentary on the Article and talk: Bernadette Boscoe, Peter Darch, Milena Golshan, Irene Pasquetto, and Michael Scroggins. Morgan Wofford provided extensive bibliographic research. James Dempsey of the Berkeley Center for Law and Technology provided detailed comments on the draft paper. Outside UC, credit is due to Marc Rotenberg and the staff at the Electronic Privacy Information Center as well as Anne Washington of George Mason University. Special thanks are due to Chris Jay Hoofnagle, Paul Schwarz, and others at the Berkeley Center for Law and Technology, whose invitation to give the Tenth Annual BCLT Privacy Lecture provided the incentive to write this Article, and to Erwin Chemerinsky (Berkeley) and Katie Shilton (University of Maryland) who provided extensive and insightful commentary as respondents to the public lecture on November 16, 2017.

obtaining grant funding or publishing results in journals; and (2) the vast accumulation of "grey data" about individuals in their daily activities of research, teaching, learning, services, and administration. The boundaries between research and grey data are blurring, making it more difficult to assess the risks and responsibilities associated with any data collection. Many sets of data, both research and grey, fall outside privacy regulations such as HIPAA, FERPA, and PII. Universities are exploiting these data for research, learning analytics, faculty evaluation, strategic decisions, and other sensitive matters. Commercial entities are besieging universities with requests for access to data or for partnerships to mine them. The privacy frontier facing research universities spans open access practices, uses and misuses of data, public records requests, cyber risk, and curating data for privacy protection. This Article explores the competing values inherent in data stewardship and makes recommendations for practice by drawing on the pioneering work of the University of California in privacy and information security, data governance, and cyber risk.

TABLE OF CONTENTS

> The world's most valuable resource is no longer oil, but data.[1]
>
> If you can't protect it, don't collect it.[2]

I. FRAMING THE PROBLEM

Universities are stewards of vast amounts of data. These data provide many new opportunities for research, teaching, administration, partnerships, and strategic planning. Data take many forms, have many origins, and have many uses. Data ownership is rarely clear, especially for research data, and the costs and mechanisms for stewardship are poorly understood. Although data are difficult to manage and govern in any institution, universities face a particularly complex set of responsibilities and risks.

Stewardship of data and of public trust are sometimes asymmetrical. The university community, which includes students, faculty, staff, and many other stakeholders, expects a reasonable degree of confidentiality in their dealings with an institution of research and learning. They also expect the university to respect their privacy and to keep their data secure. Furthermore, faculty and students expect their universities to respect their academic and intellectual freedom while managing and governing data. The public, which extends beyond the university community, expects universities to be fair, transparent, and accountable for resources. Good stewardship means releasing some kinds of data and preventing the release of other kinds of data. The same data may fall into either category, depending on the time, purpose, or entity requesting access. Few universities, or other institutions, have adequate governance mechanisms to address these stewardship challenges effectively.

This broad set of concerns was framed succinctly by the University of California Privacy and Information Security Initiative (PISI) which was charged in 2010 by then-President Mark Yudof to make recommendations for an overarching privacy framework to address the university's statutory and regulatory obligations; governance, implementation, and accountability structures; and policy vehicles for university policy and practice in privacy and

1. *The World's Most Valuable Resource Is No Longer Oil, but Data*, ECONOMIST (May 6, 2017), www.economist.com/leaders/2017/05/06/the-worlds-most-valuable-resource-is-no-longer-oil-but-data [https://perma.cc/L2HD-J7NL].

2. This is an increasingly common privacy and security aphorism. *See* Richard Bejtlich, *New Cybersecurity Mantra: "If You Can't Protect It, Don't Collect It"*, BROOKINGS INSTITUTION: TECHTANK (Sept. 3, 2015), https://www.brookings.edu/blog/techtank/2015/09/03/new-cybersecurity-mantra-if-you-cant-protect-it-dont-collect-it/ [https://perma.cc/8DDT-64RA].

information security.[3] As evidence of the importance placed on this effort, the President's office selected members of the PISI Steering Committee from the upper echelons of the University, including the Provost, General Counsel, Chief Compliance and Audit Officer, Chief Information Officer, and representatives from the campuses and the Academic Senate.

In considering its charge, "the Steering Committee was guided by the following principles"[4]:

- We must maximally enable the mission of the University by supporting the values of academic and intellectual freedom.
- We must be good stewards of the information entrusted to the University.
- We must ensure that the University has access to information resources for legitimate business purposes.
- We must have a University community with clear expectations of privacy—both privileges and obligations of individuals and of the institution.
- We must make decisions within an institutional context.
- We must acknowledge the distributed nature of information stewardship at UC, where responsibility for privacy and information security resides at every level.

These principles have proved to be robust in the several years since the final report was submitted to the President and the Regents. Most of the recommendations have been adopted and implemented, including appointing Chief Privacy Officers and establishing joint Academic Senate-Administration boards on privacy and information security on each of the ten campuses. At the UC-wide level, the Academic Senate monitors PISI implementation via the UC Academic Computing and Communications Committee (UCACC). Individual campuses have extended the PISI principles in various ways. UCLA, which established a joint Senate-Administration Privacy and Data Protection Board in 2005, extended the PISI principles and recommendations in the Data Governance Task Force Report.[5]

3. UC PRIVACY & INFO. SEC. INITIATIVE STEERING COMM., PRIVACY AND INFORMATION SECURITY INITIATIVE STEERING COMMITTEE REPORT TO THE PRESIDENT 1, 27–28 (2013), http://ucop.edu/privacy-initiative/uc-privacy-and-information-security-steering-committee-final-report.pdf [https://perma.cc/6ANW-HCCK].

4. *Id.* at 1–2.

5. UCLA DATA GOVERNANCE TASK FORCE, UCLA DATA GOVERNANCE TASK FORCE FINAL REPORT AND RECOMMENDATIONS 1, 8 (2016), http://evc.ucla.edu/reports/DGTF-report.pdf [https://perma.cc/97TQ-3AGM].

Identifying problems and principles is an essential starting point to address the challenges of the day. Applying these principles to solve these problems is much harder. Over the last several years, the complexity of these challenges has become ever more apparent. This Article explores the current landscape of opportunities, responsibilities, risks, and frontiers facing universities in a data-rich world. It draws on the pioneering work of the University of California, one of the world's premier public research universities, at the forefront of both data governance and data exploitation. It also draws on a large body of work on policy and practice for governing access to research data.

The epigraphs at the top of the Article frame the arguments herein. Data have become the "new oil" as one of the modern world's most valued commodities. Market leaders, whether in commerce or in higher education, may be those most adept at exploiting data in their realms. As non-consumptive goods, arguably more valuable than the finite supply of oil, data can be mined, combined, and reused for multiple applications over long periods of time.[6] The aphorism, "if you can't protect it, don't collect it," has circulated in the privacy, security, and hacker communities for a decade or more. Leaking data can be at least as dangerous as leaking oil. For universities to sustain the public trust, and to live by the principles that guided the UC Privacy and Security Initiative, they must address the converse of that aphorism: "if you collect it, you must protect it."

II. THE DATA-RICH WORLD OF RESEARCH UNIVERSITIES

Universities are stewards of many kinds of data, some of which they collect, others that they acquire, and yet others that are byproducts of regular activities. The value of these data, the possibilities for exploitation, the responsibilities for stewardship, and the types of associated risks vary immensely.

Intentional data collection is the more obvious sort, such as materials gathered by investigators as part of research projects and information about current and prospective students gathered by the registrar. These data tend to be governed by established mechanisms such as grant contracts, Institutional Review Boards, HIPAA, and FERPA.[7] At the other extreme is incidental data

6. *See* CHRISTINE L. BORGMAN, BIG DATA, LITTLE DATA, NO DATA: SCHOLARSHIP IN THE NETWORKED WORLD 7 (2015); *see also generally* CHARLOTTE HESS & ELINOR OSTROM, UNDERSTANDING KNOWLEDGE AS A COMMONS: FROM THEORY TO PRACTICE (2007).

7. *See, e.g.*, Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936; Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232g (2012); Protection of Human Subjects, 45 C.F.R § 46 (2009).

collection that is difficult to identify or govern, such as that gathered by students, by staff in administrative roles, and by technology such as security cameras controlled within offices or departments. A growing source of incidental data collection is software packages that individuals install on university networks for otherwise legitimate purposes in teaching and research. In between is a vast array of data collection that may be more or less intentional, more or less governed, and whose applications may be more or less foreseeable at the time of collection. These include learning management systems, personnel systems that include faculty dossiers for academic evaluation and promotion, identity cards that encode various privileges (library usage, food service, building access, debit charges, etc.), and much more.

In all of these arenas, data volumes and variety are growing at rates far greater than most administrators or faculty realize. Those individuals who recognize the value and opportunities in these data are not necessarily obligated to seek permission to exploit them. Third parties outside the university may be the first to recognize data opportunities, and approach individuals at any level of the university for partnerships. Governance mechanisms to assure protection of privacy, academic freedom, intellectual property, information security, and compliance with regulations in the uses of such data are nascent, at best.

Of this immense landscape of data issues in universities, this Article focuses on two exemplars. The first is research data, spanning all academic domains from the sciences, technology, and medicine to the social sciences, humanities, and the arts. Although the data management issues in these areas are critical and far from solved, at least two decades of practice and policy inform current discussions. The second is data collected by universities about members of its community, including students, faculty, staff, visitors, patients, and other stakeholders. Data collection about individual persons, both intentional and incidental, is accelerating rapidly with the implementation of systems that can exploit "data exhaust" from the activities of individuals.[8] Despite several decades of research on principles and practice for "privacy by design," developers too often default to collecting as much data as possible.[9]

8. VIKTOR MAYER-SCHÖNBERGER & KENNETH CUKIER, BIG DATA: A REVOLUTION THAT WILL TRANSFORM HOW WE LIVE, WORK, AND THINK 113 (2013) ("Data exhaust . . . refers to data that is shed as a byproduct of people's actions and movements in the world . . . Many companies design their systems so that they can harvest data exhaust and recycle it, to improve an existing service or to develop new ones.").

9. *See generally* Victoria Bellotti & Abigail Sellen, *Design for Privacy in Ubiquitous Computing Environments*, *in* PROCEEDINGS OF THE THIRD EUROPEAN CONFERENCE ON COMPUTER-SUPPORTED COOPERATIVE WORK 77 (Giorgio de Michelis, Carla Simone, & Kjeld Schmidt eds., 1993); Herbert Burkert, *Privacy-Enhancing Technologies: Typology, Critique, Vision*, *in*

Data that universities collect about their communities is also a large and diverse category. The primary exemplar discussed herein is teaching and student learning, itself an area of data explosion. Fully online courses can capture data on every keystroke of every participant, if they choose to do so, creating rich profiles on individual students and interactions between them. Less obvious is the amount of data produced in hybrid courses, where learning management systems complement interactions in campus classrooms. Students acquire their readings and assignments online, participate in online discussions and other activities, and submit their assignments through these systems, all of which is discretely time-stamped. When universities aggregate this learning data with other kinds of data they hold on their students, extensive profiles result. These datasets can be deployed for learning analytics, institutional reports to government and accreditation agencies, academic research, or for surveillance of activities and behavior.

A. RESEARCH DATA

Scholars collected research data long before the advent of the scholarly journal, which is barely 350 years old.[10] Data are reported in publications, usually in selected and synthesized forms. Some data are kept for reuse by investigators; other data may be bartered in exchange for still further data or as invitations to collaborate.[11] Until recently, data were considered part of the research process, rather than products to be disseminated. Data release has become a condition of obtaining grants and publishing papers in many domains, especially in the biosciences and medicine.[12] Survey research in the

---

TECHNOLOGY AND PRIVACY: THE NEW LANDSCAPE 125 (Philip E. Agre & Marc Rotenberg eds., 1997); Ian Goldberg, David Wagner & Eric Brewer, *Privacy-Enhancing Technologies for the Internet*, *in* PROCEEDINGS OF THE IEEE COMPCON '97 at 103 (1997); Katie Shilton, *Participatory Personal Data: An Emerging Research Challenge for the Information Sciences*, 63 J. AM. SOC'Y FOR INFO. SCI. TECH. 1905 (2012); Katie Shilton, *Values Levers: Building Ethics into Design*, 38 SCI. TECH. & HUMAN VALUES 374 (2012).

10. *350 Years of Scientific Publishing*, ROYAL SOC'Y, https://royalsociety.org/journals/publishing-activities/publishing350/ [https://perma.cc/7RZ9-BLRG] (last visited June 15, 2018).

11. Stephen Hilgartner & Sherry I. Brandt-Rauf, *Data Access, Ownership, and Control: Toward Empirical Studies of Access Practices*, 15 KNOWLEDGE: CREATION DIFFUSION UTILIZATION 355, 357, 363–66 (1994).

12. *See, e.g.*, Joseph S. Ross & Harlan M. Krumholz, *Ushering in a New Era of Open Science Through Data Sharing: The Wall Must Come Down*, 309 JAMA 1355, 1356 (2013); Joseph S. Ross, *Clinical Research Data Sharing: What an Open Science World Means for Researchers Involved in Evidence Synthesis*, 5 SYSTEMATIC REVS. 159 at 1 (2016); Geoffrey Boulton et al., *Science as a Public Enterprise: The Case for Open Data*, 377 LANCET 1633, 1634 (2011).

social sciences has a long history of data sharing. For example, in the humanities, archaeology is a growth area for data sharing and archiving.[13]

When datasets were small and locally controlled, issues of data stewardship and governance rarely arose. As datasets grew larger and distributed collaborations became more common, tools to mine and combine data became more sophisticated. These opportunities vary immensely between domains, universities, countries, and cultures, as do applicable policies.[14] As the volume of publicly available research data expands, concerns for stewardship of these data become more urgent.[15]

1. Scope and Definitions

One part of the challenge in managing research data is the difficulty of defining "research" or "data" succinctly. Information, documents, and materials exist in many forms and in many states, only a portion of which might be considered research data for the purposes of governance. The Oxford English Dictionary is a good starting place to define concepts such as research:

> The act of searching carefully for or pursuing a specified thing or person; an instance of this. Systematic investigation or inquiry aimed at contributing to knowledge of a theory, topic, etc., by careful consideration, observation, or study of a subject. In later use also: original critical or scientific investigation carried out under the auspices of an academic or other institution. Investigation undertaken in order to obtain material for a book, article, thesis, etc.; an instance of this.

Locating a singular definition of research used within the University of California proved similarly elusive. At UCLA, for example, the Office of Research Administration lists responsibilities and resources on its website but does not define research in its glossary of terms. Research, like beauty, is often

13. *See generally* Eric Kansa, *Openness and Archaeology's Information Ecosystem*, 44 WORLD ARCHAEOLOGY 498 (2012); Eric C. Kansa, Sarah Whitcher Kansa & Benjamin Arbuckle, *Publishing and Pushing: Mixing Models for Communicating Research Data in Archaeology*, 9 INT'L J. DIG. CURATION 57 (2014).

14. BORGMAN, *supra* note 6, at 55–58.

15. *See, e.g.*, Francine Berman & Vint Cerf, *Who Will Pay for Public Access to Research Data?*, 341 SCIENCE 616 (2013); Tony Hey & Anne E. Trefethen, *Cyberinfrastructure for e-Science*, 308 SCIENCE 817 (2005); Jeremy York, Myron Gutmann & Francine Berman, What Do We Know About the Stewardship Gap? 1 (July 17, 2016) (unpublished manuscript), https://deepblue.lib.umich.edu/bitstream/handle/2027.42/122726/StewardshipGap_Final.pdf [https://perma.cc/26V3-VQXT].

in the eye of the beholder, who may be a grant-funding program manager or an academic personnel officer.[16]

One area in which firm definitions are needed are studies involving human subjects. In the United States, such studies fall under the regulation of the federal Department of Health and Human Services. DHHS regulations define research as "a systematic investigation, including research development, testing and evaluation, designed to develop or contribute to generalizable knowledge."[17] If a study meets these requirements and is deemed to involve human subjects, then the protocol must be submitted to the Institutional Review Board (IRB) of the university. Whether a study is considered research or involves human subjects is not always obvious. A systematic study that involves a survey of students for the purposes of university strategic planning is usually not considered research because it is not intended for publication, and thus not for generalizable knowledge. Relatedly, systematic investigations of human activity that are intended for publication, but that do not require direct contact with individual living persons, may or may not be deemed research for the purpose of IRB review. Further, problems arise when data collected for administrative purposes later are deemed worthy of publication, which is not an uncommon occurrence.

"Research data" is similarly problematic to define and is often left undefined in guidelines for releasing or depositing data from a research project. At best, data may be defined by example, such as observations, facts, samples, or records. A definition developed elsewhere is the basis for this Article's discussion: "data refers to entities used as evidence of phenomena for the purposes of research or scholarship."[18] This phenomenological definition covers data in any academic discipline, recognizing that one scholar's signal is another's noise.

2. Open Access to Research Data

Practices and policies for open access to research data are intertwined with those for open access to scholarly publications such as journal articles. Since the early days of "electronic publishing" in the 1990s, activists have called for open access to scholarly publications as a means to democratize access to information.[19] Open access has taken many forms, such as disseminating

16. *See* DONALD E. STOKES, PASTEUR'S QUADRANT: BASIC SCIENCE AND TECHNOLOGICAL INNOVATION 16 (1997).

17. 45 C.F.R. § 46.102(d) (2017).

18. BORGMAN, *supra* note 6, at 29.

19. *See* Stevan Harnad, *The PostGutenberg Galaxy: How to Get There from Here*, 11 INFO. SOC'Y 285, 288 (1995) ("[T]he general public, which is likewise gaining greater access to the Net, also stands to benefit from the free availability of scholarly literature . . . ."); Stevan

preprints prior to publication, disseminating post-prints after publication, or publishing in journals that are free to read online.[20] Scholars are also publishing a growing number of books in open access formats, often with print-on-demand options. Open access increases the dissemination of research, which tends to enhance the visibility of authors and their institutions, so the payoffs are several. Economic models for open access dissemination vary widely, as do stewardship models; and responsibility for access and for sustainability often fall to different parties.[21]

Providing access to research data is often a condition for publishing an article, whether or not the article itself is published in an open access form.[22] Thus, data release usually occurs at the time of submitting a paper for publication. Datasets can be contributed to archives or repositories, which assign them a unique identification number, and that ID is linked to the paper. Ideally, it becomes possible to search for data and identify associated publications, or to search for publications and identify associated datasets.[23] Publishing articles in open access venues and disseminating preprints are more established practices than is providing open access to data. Data release varies widely by domain, with the greatest acceptance in the biosciences and medicine, and by type of data, research method, funding source, and other factors.[24]

Harnad, *Post-Gutenberg Galaxy: The Fourth Revolution in the Means of Production of Knowledge*, 2 PUBLIC-ACCESS COMPUTER SYS. REV. 39, 47 (1991) ("A decade and half later my own rewarding experience with electronic skywriting has convinced me that this newest medium's unique potential to support and sustain open peer commentary must now be made generally available too . . . .").

20. *See* PETER SUBER, OPEN ACCESS 97–98 (2012).

21. *See, e.g.*, Isabel Bernal, *Open Access and the Changing Landscape of Research Impact Indicators: New Roles for Repositories*, 1 PUBLICATIONS 56, 58–60 (2013); CHRISTINE L. BORGMAN, SCHOLARSHIP IN THE DIGITAL AGE: INFORMATION, INFRASTRUCTURE, AND THE INTERNET 255, 259–60 (2007); *Open Access Policies*, HARVARD UNIV., https://osc.hul.harvard.edu/policies [https://perma.cc/S5G9-SHUY]; Jennifer Howard, *Open Access Gains Major Support in U. of California's Systemwide Move*, CHRON. HIGHER EDUC. (Aug. 2, 2013), www.chronicle.com/article/Open-Access-Gains-Major/140851 [https://perma.cc/3KB7-RW42]; *UC Open Access Policies*, OFFICE OF SCHOLARLY COMMUNICATION, http://osc.universityofcalifornia.edu/open-access-policy/ [https://perma.cc/T9KD-QAEX]; Richard Van Noorden, *Europe Joins UK Open-Access Bid*, 487 NATURE 285, 285 (2012). *See also generally* JOHN WILLINSKY, THE ACCESS PRINCIPLE: THE CASE FOR OPEN ACCESS TO RESEARCH AND SCHOLARSHIP (2006); Randall Munroe, *The Rise of Open Access*, 342 SCIENCE 58 (2013).

22. *See* BORGMAN, *supra* note 6, at 48; GEOFFREY BOULTON ET AL., SCIENCE AS AN OPEN ENTERPRISE 27 (2012) https://royalsociety.org/~/media/policy/projects/sape/2012-06-20-saoe.pdf [https://perma.cc/2APE-E2BW].

23. BORGMAN, *supra* note 21, at 116–18; *see* Philip E. Bourne, *Will a Biological Database Be Different from a Biological Journal?*, 1 PLOS COMPUTATIONAL BIOLOGY 179, 180–81 (2005).

24. *See generally* BORGMAN, *supra* note 21; *see also* BORGMAN, *supra* note 6, at 260–64.

A legacy of open access publishing that contributes to stewardship challenges is that the notion of "publication" has become more diffuse. Whether something can be considered a formal publication matters for evaluating scholarship, and thus for hiring, tenure, grant proposals, library collections, and much more. In the print world, publications were more readily distinguishable from "grey literature." The latter category consists of documents such as working papers, reports, pamphlets, and preprints that have scholarly value, but that have not been vetted by peer review or disseminated through a formal publication process. In the online world, versions of scholarly documents proliferate. The same or similar content, often with the same or similar titles and authors, may appear as preprints, post-prints, working papers, slide decks, and as the formal "official" version of a publication. Initial versions of documents may or may not become formal publications at a later time. Others may diverge into multiple publications. Choosing which version to cite is a judgment call by the citing author.

The publication versioning problem intersects with the data stewardship problem in at least two ways. One is determining the relationship between a dataset and a publication or other document that describes the dataset. Research projects can generate many versions of publications and many versions of datasets, resulting in a complex array of many-to-many relationships between datasets and publications explaining the context in which they were created.

The second problem is the differing degrees of validation and of permanence of publications and datasets. The popular term "data publishing" suggests that data and publications are released to the scholarly communication system with comparable status.[25] Similarly, data citation is promoted as a means to encourage data release by giving comparable scholarly credit.[26] This equivalence is also embedded in technology by assigning Digital Object Identifiers (DOI) to each article and dataset.[27] DOIs are a formal system of persistent and unique identifiers that is managed by scholarly

25. *See* Mark A. Parsons & Peter A. Fox, *Is Data Publication the Right Metaphor?*, 12 DATA SCI. J. WDS32, WDS40 (2013); BORGMAN, *supra* note 6, at 225–27.

26. *See generally* NAT'L RESEARCH COUNCIL, FOR ATTRIBUTION—DEVELOPING DATA ATTRIBUTION AND CITATION PRACTICES AND STANDARDS: SUMMARY OF AN INTERNATIONAL WORKSHOP 210 (Paul F. Uhlir ed., 2012); CODATA-ICSTI Task Grp. on Data Citation Standards & Practices, *Out of Cite, Out of Mind: The Current State of Practice, Policy, and Technology for the Citation of Data*, 12 DATA SCI. J. CIDCR1, CIDCR14–CIDCR15 [hereinafter CODATA-ICSTI Task Group].

27. *See* CODATA-ICSTI Task Group, *supra* note 26, at CIDCR32; NAT'L RESEARCH COUNCIL, *supra* note 26, at 52.

publishers, libraries, and other stakeholders.[28] However, journal articles are subject to far more scrutiny, and to greater investments in stewardship, than are datasets.[29] In scholarly communication, publishing implies a process of peer review, validation, dissemination, and access.[30] Publishers and libraries provide stewardship and access.

In contrast, datasets are published only in the dictionary sense of "making public."[31] Rarely are datasets peer-reviewed. Although data repositories may assess datasets for technical standards, such as adequate metadata and documentation, responsibility for scholarly or scientific quality is left to the contributors.[32] Long-term accessibility of datasets is a significant concern. Datasets may remain available only for fixed time periods at the end of a grant project and funding for repositories is often unstable. When datasets are

28. *See, e.g.*, *Discussion Board for the Persistent Identifiers Working Group RDA*, RESEARCH DATA ALLIANCE, https://www.rd-alliance.org/groups/pid-interest-group.html [https://perma.cc/YKX9-82VS] (last visited Feb. 20, 2018) ("The purpose of the Persistent Identifier Interest Group is to synchronize identifier-related efforts, address important and emerging PID-related topics and coordinate activities, including appropriate RDA Working Groups, to practically solve PID-related issues from the engaged communities."); Jan Brase, Michael Lautenschlager & Irina Sens, *The Tenth Anniversary of Assigning DOI Names to Scientific Data and a Five Year History of DataCite*, 21 D-LIB MAGAZINE (2015); *Metadata Enables Connections*, CROSSREF (Aug. 4, 2018), https://www.crossref.org/services/ [https://perma.cc/UC4A-VMQ8] (describing use of metadata to persistently catalogue and track scholarly publications); Micah Altman & Mercè Crosas, *The Evolution of Data Citation: From Principles to Implementation*, 37 IASSIST Q. 62, 65 (2013) ("Global persistent identifiers, such as DOIs and Handles, offer a mechanism to provide a permanent link that can be configured to always resolve to a web page from which the data can be accessed, independent of whether the location of that page changes over time."); *see also* Matthew S. Mayernik & Keith E. Maull, *Assessing the Uptake of Persistent Identifiers by Research Infrastructure Users*, 12 PLOS ONE 1, 1 (2017) (evaluating whether research infrastructures are being increasingly identified and referenced in the research literature to via persistent citable identifiers); Tobias Weigel et al., *A Framework for Extended Persistent Identification of Scientific Assets*, 12 DATA SCI. J. 10, 13 (2013) (presenting a framework for persistent identification that fundamentally supports context information).

29. *See* Christine L. Borgman, *Data Citation as a Bibliometric Oxymoron*, *in* THEORIES OF INFORMETRICS AND SCHOLARLY COMMUNICATION 93, 94 (Cassidy R. Sugimoto ed., 2015) ("Scholarly publication normally requires peer review and dissemination in a venue with recognized status for credit and attribution. Journals and books usually meet this standard of publication. . . . Data are far more complex objects—if they are objects at all—than the entities to which bibliometrics applies.") (internal citation omitted).

30. *See* BORGMAN, *supra* note 21, at 58–60, 65–68.

31. *See* BORGMAN, *supra* note 6, at 47–49.

32. *See generally* LOUISE CORTI ET AL., MANAGING AND SHARING RESEARCH DATA: A GUIDE TO GOOD PRACTICE (1st ed. 2014) (outlining a comprehensive set of best practices for data management and sharing); *see also* Veerle Van den Eynden & Louise Corti, *Advancing Research Data Publishing Practices for the Social Sciences: From Archive Activity to Empowering Researchers*, 18 INT'L J. DIGITAL LIBR. 113, 119–20 (2017).

released by posting on local websites, links degrade quickly.[33] Authors may assume, all too readily, that assigning a DOI to an object, whether a journal article, conference paper, dataset, presentation slide deck, glass slide, or other entity, makes that item a publication and assures long-term accessibility. Unfortunately, assigning a persistent identifier only ensures that the item has a unique ID. It does not guarantee that the ID will retrieve any content.[34]

3. Opportunities in Research Data

Democratizing access to knowledge is among the drivers of open access to publications and to research data. The opportunities in these categories differ in important ways, however. Open access to publications expands readership to audiences far beyond the privileged communities that enjoy access to expensive journals and books through their university libraries. Whether read in the form of preprint, post-print, or published journal article, open access dissemination of scholarly work has created a vast international audience of interested students, researchers, enthusiasts, patients, parents, and other parties. Having the domain knowledge and linguistic ability to exploit these materials is another matter, but providing access is a good start on equity issues.

Similarly, open access to research data expands scholarly data resources far beyond the investigators who collected and analyzed them. Others can exploit these data, as intact datasets or in combination with other resources, for many purposes. The barriers of requisite domain knowledge and linguistic skills still apply, but the opportunities to exploit data are potentially boundless. Among the policy drivers commonly cited for open access are transparency, to allow others to inspect and evaluate findings; reproducibility, to verify findings by repeating a study; and reuse, whether as an independent dataset or aggregated

33. *See* Borgman, *supra* note 29, at 100; Alberto Pepe et al., *How Do Astronomers Share Data? Reliability and Persistence of Datasets Linked in AAS Publications and a Qualitative Study of Data Practices among US Astronomers*, 9 PLOS ONE 1, 2 (2014); Christine L. Borgman, Andrea Scharnhorst & Milena S. Golshan, Digital Data Archives as Knowledge Infrastructures: Mediators of Data Sharing and Reuse 1 (Feb. 2, 2018) (unpublished manuscript), https://arxiv.org/abs/1802.02689 [https://perma.cc/S4AQ-SY7Z]; NAT'L SCI. BOARD, LONG-LIVED DIGITAL DATA COLLECTIONS: ENABLING RESEARCH AND EDUCATION IN THE 21ST CENTURY 34 (2005) ("Tracking is a challenge because links to the data in publications, Web sites, etc. may become obsolete. Finding the data that were previously available may be difficult for those outside the immediate project team.").

34. *See* BORGMAN, *supra* note 6, at 258 ("In practice, neither identity nor persistence is absolute. People change names, documents change versions, digital objects change locations when transferred from one computer to another, and they change in form when migrated over generations of software . . . ."); Borgman, *supra* note 29 (explaining that persistent identifiers must be able to "resolve to a location" online to facilitate access in addition to identification).

with other data. Accountability to taxpayers, in the case of public funding, is also mentioned frequently.[35]

The promises of open access to research data are vast, although mired in hyperbole. Vast stores of research data are predicted to accumulate through open access policies enforced by publishers, funding agencies, and government directives, as well as through voluntary participation. These stores can be mined and combined by anyone, at least in principle, leading to new research findings, new innovations, new companies, and new market sectors.[36] A European policy presentation at a recent Research Data Alliance meeting

35. Press Release, European Comm'n., Scientific Information in the Digital Age: Ensuring Current and Future Access for Research and Innovation (Feb. 15, 2007), https://ec.europa.eu/digital-single-market/en/news/scientific-information-digital-age-ensuring-current-and-future-access-research-and-innovation [https://perma.cc/9M7N-B3A5]; BORGMAN, *supra* note 21, at 77 ("Funding agencies are using the opportunities afforded by online access to reaffirm their responsibility to taxpayers . . . ."); Geoffrey Boulton, *Open Your Minds and Share Your Results*, 486 NATURE 441, 441 (2012) ("[A]bove all, we need scientists to accept that publicly funded research is a public resource."); BOULTON ET AL., *supra* note 22, 39 ("Access to data . . . is important for citizens' involvement in science and their pursuit of scholarship through data which, after all, for publicly funded science they have paid for through their taxes."); ORG. FOR ECON. COOPERATION & DEV., OECD PRINCIPLES AND GUIDELINES FOR ACCESS TO RESEARCH DATA FROM PUBLIC FUNDING 21–22 (2007), www.oecd.org/dataoecd/9/61/38500813.pdf [https://perma.cc/VS68-V32B]; John P. Holdren, Memorandum for the Heads of Executive Departments and Agencies: Increasing Access to the Results of Federally Funded Scientific Research 1 (Feb. 22, 2013), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/ostp_public_access_memo_2013.pdf [https://perma.cc/6SDZ-B3RB].

36. *See, e.g.*, Chris Anderson, *The End of Theory: The Data Deluge Makes the Scientific Method Obsolete*, WIRED (June 23, 2008, 12:00 PM), https://www.wired.com/2008/06/pb-theory/ [https://perma.cc/G2UL-C3JF] (explaining the relation between massive data and applied mathematics); Peter Arzberger et al., *An International Framework to Promote Access to Data*, 303 SCIENCE 1777, 1777 (2004) ("Open access . . . provides greater returns from the public investment in research, generates wealth through downstream commercialization of outputs, and provides decision-makers with facts needed to address complex, often transnational, problems."); Geoffrey Boulton et al., *Open Data in a Big Data World: An International Accord*, INT'L SCI. COUNCIL (2015), https://council.science/cms/2017/04/open-data-in-big-data-world_long.pdf [https://perma.cc/DHP2-QHZF]; Kenneth Cukier, *Data, Data Everywhere*, ECONOMIST (Feb. 25, 2010), http://www.economist.com/node/15557443 [https://perma.cc/9TA6-JPGB]; Dawn Field et al., *'Omics Data Sharing*, 326 SCIENCE 234, 234–35 (2009); Brooks Hanson, Andrew Sugden & Bruce Alberts, *Making Data Maximally Available*, 331 SCIENCE 649 (2011); Holdren, *supra* note 35; Scott D. Kahn, *On the Future of Genomic Data*, 331 SCIENCE 728, 728 (2011); John Palfrey & Jonathan Zittrain, *Better Data for a Better Internet*, 334 SCIENCE 1210, 1210 (2011); O. J. Reichman, Matthew B. Jones & Mark P. Schildhauer, *Challenges and Opportunities of Open Data in Ecology*, 331 SCIENCE 703, 703–04 (2011); Global Alliance for Genomics & Health, *A Federated Ecosystem for Sharing Genomic, Clinical Data*, 352 SCIENCE 1278, 1278–79 (2016).

suggested that "[b]y 2020, the European Data Economy in the most favourable scenario could contribute up to 4% of EU GDP."[37]

In practice, however, considerable investment is required to make research data useful to anyone beyond the original data collectors. Whereas most scholarly documents can be read and understood as independent units, the same is not true of data. A dataset alone, without accompanying documentation of the research methods by which it was created, analysis and interpretation of the findings, and associated context such as instruments, models, and software, may be little more than a string of numbers. The better documented and curated, the more useful any given set of data will be to others.[38]

B. GREY DATA: ACADEMIC, ADMINISTRATIVE, AND INSTRUCTIONAL

"Grey data" is proposed as an umbrella term to describe the vast array of data that universities accumulate outside the research realm. Analogous to grey literature, explained above, these are useful data that have not been vetted by peer review, or perhaps by any other governance mechanism of the university. Grey data have become critical to a university's ability to "innovate, enhance, and execute [its] core missions of education, research, and service."[39] Some of these data are collected for mandatory reporting obligations such as enrollments, diversity, budgets, grants, and library collections. Many types of data about individuals are collected for operational and design purposes, whether for instruction, libraries, travel, health, or student services. Universities are increasingly aware of the asset value of data about their communities. Some of these data have legal encumbrances for compliance purposes, but many are collected for reasons of internal management and external competitiveness. Outside entities also see the value in these data, whether through explicit partnerships with universities to exploit data, or by collecting data on users of their products.

The drivers of data collection in universities are many, not the least of which is "market-based solutions" as a response to the lack of funding for public colleges and universities. Higher education reform is being defined in "highly economistic terms" leading to "measurement panic."[40] University

37. CELINA RAMJOUÉ, BUILDING A EUROPEAN DATA ECONOMY: THE ROLE OF RESEARCH DATA 6 (2017).

38. *See* BORGMAN, *supra* note 6, at 4, 48; Irene V. Pasquetto, Bernadette M. Randles & Christine L. Borgman, *On the Reuse of Scientific Data*, 16 DATA SCI. J. 1, 4 (2017) ("[T]he dataset is of little value without associated documentation, and often software, code, and associated scientific models.").

39. UCLA DATA GOVERNANCE TASK FORCE, *supra* note 5, at 3.

40. Sanford F. Schram, *The Future of Higher Education and American Democracy: Introduction*, 36 NEW POL. SCI. 425, 427–30 (2014).

administrators may be given statistical benchmark targets for enrollments, time to degree, retention, diversity, and other countable factors, not unlike performance targets in private business. When higher education is viewed more as a job track than as an investment in a democratic citizenry, market-driven measurement may be an inevitable result. Competition looms everywhere.

1. Collecting Grey Data

Universities always have collected data about their communities, their operations, and their services—as do businesses, governments, and public service sectors. As daily activities of teaching, learning, research, and operations have moved online, the "volume, velocity, and variety" of data collection have exploded.[41] The uses of digital data from online networks differ from those of data collected offline in at least two respects. One is that discrete data elements become far more valuable when combined with other data. Information gathered about student performance in a single course, once aggregated with data on performance in other courses, test scores, social media activity, library usage, and dietary habits, for example, yield rich profiles on individuals. The other difference between offline and online collection is that many more people have access to online data. In the past, an individual instructor knew little about students enrolled in her course beyond the list provided by the registrar. Now the instructor may be given profiles on each student to track progress. Academic counselors, student advising staff, instructional designers, registrars, department chairs, deans, provosts, and many others may also have access to these data.

The pervasiveness of information technologies has accelerated over the course of several decades, much of which originated in university environments. Today's senior faculty have lived through eras of mainframe computers, minicomputers, desktop personal computers, and ubiquitous mobile devices such as laptops, tablets, and smart phones. They have adapted their research and teaching practices to accommodate, if not to incorporate these technologies. Instrumentation large and small is deeply embedded in the practice of many domains, ranging from space telescopes to sensor networks to nanotech devices. In the early days of portable technologies, instruction practices excluded these devices from the classroom, asking students to leave their calculators, cell phones, and laptops at home, or at least out of sight. Although some faculty continue to bar mobile technologies from classrooms,

41. Doug Laney, *3D Data Management: Controlling Data Volume, Velocity and Variety*, META GROUP RES. NOTE (Feb. 6, 2001), https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf [https://perma.cc/ENC3-AUBU].

most have embraced tools such as learning management systems (LMS) that support course websites, links to reading materials, discussion groups, and authentication to library and enrollment services. Pedagogy has shifted rapidly over the last decade from rejecting or ignoring students' uses of information technologies to embracing "cyberlearning," both for the analytical data generated and for the ability to adapt instruction to students' behavior.[42]

2. Opportunities in Grey Data

As cited above, data have become the new "oil" that drives commerce and competition.[43] Google, Amazon, Facebook, and many other companies have built financial empires by collecting and combining personal data. These data are used to profile individuals, segment the population into discrete units, and present information highly selectively. They can also be used to monitor or predict behavior, resulting in closer observation for illicit or suspicious activities, or for auspicious moments to present advertisements, news, or other content. Many decisions are made about people on the basis of their online traces.

Universities, often with commercial partners, are exploiting data about individuals in similar ways. By collecting detailed data on individual student performance, some universities are creating an individualized "learning path" for each student, with various benchmarks toward degree completion.[44] Other institutions are constructing profiles that assign students to one of three categories that predict success, such as the green, yellow, and red "Stoplight" system. Some profiles incorporate data from social networks to assess a student's social connectedness algorithmically.[45] These profiles may be used to

42. *See, e.g.*, BEN WILLIAMSON, BIG DATA IN EDUCATION: THE DIGITAL FUTURE OF LEARNING, POLICY AND PRACTICE 196–97 (1st ed. 2017); Goldie Blumenstyk, *As Big-Data Companies Come to Teaching, a Pioneer Issues a Warning*, CHRON HIGHER EDUC. (Feb. 23, 2016), www.chronicle.com/article/As-Big-Data-Companies-Come-to/235400 [https://perma.cc/6YTM-E8JC]; Paul Voosen, *Big-Data Scientists Face Ethical Challenges After Facebook Study*, CHRON. HIGHER EDUC. (Dec. 15, 2014), www.chronicle.com/article/Big-Data-Scientists-Face/150871 [https://perma.cc/LS2K-2H4G]; CHRISTINE L. BORGMAN ET AL., FOSTERING LEARNING IN THE NETWORKED WORLD: THE CYBERLEARNING OPPORTUNITY AND CHALLENGE 35–45 (2008), https://www.nsf.gov/pubs/2008/nsf08204/nsf08204.pdf [https://perma.cc/6T48-B4XK].

43. ECONOMIST, *supra* note 1.

44. Sarah Brown, *Where Every Student Is a Potential Data Point*, CHRON. HIGHER EDUC. (Apr. 9, 2017), https://www.chronicle.com/article/Where-Every-Student-Is-a/239712 [https://perma.cc/P5ND-YU3D].

45. Evan Selinger, *With Big Data Invading Campus, Universities Risk Unfairly Profiling Their Students*, CHRISTIAN SCI. MONITOR (Jan. 13, 2015), http://www.csmonitor.com/World/Passcode/Passcode-Voices/2015/0113/With-big-data-invading-campus-universities-risk-unfairly-profiling-their-students [https://perma.cc/LQX2-2F5A].

make decisions about students, often without their knowledge, about jobs, scholarships, financial aid, choice of majors, counseling, and other matters.

Integrating data from multiple sources and systems is a nontrivial matter for reasons of technology, measurement, and inference.[46] The higher education community, via an EDUCAUSE initiative funded by the Gates Foundation, has proposed a "Next Generation Digital Learning Environment" that will provide greater interoperability and a freer flow of data between applications that gather data about students.[47]

III. UNIVERSITY RESPONSIBILITIES FOR DATA

The massive data collection by universities creates vast opportunities for research, teaching, learning, service, outreach, and strategic management. These data collections expose universities to new risks and create responsibilities that may converge and diverge in unexpected ways. Four categories of responsibilities are outlined here: stewardship and governance, and protecting privacy, academic freedom, and intellectual property. As a means to focus this vast territory, the discussion draws out issues that are common to research data and to grey data. Because privacy concerns are central to this Article, academic freedom and intellectual property are discussed in privacy contexts.

A. STEWARDSHIP AND GOVERNANCE

By collecting data, institutions assume responsibility for managing those data in the short and long term. Among the many descriptions of these roles, such as sustainability, curation, access, and preservation, "stewardship" has become the overarching term. Although "stewardship" is used in nuanced ways in the scientific, library, archival, and policy communities, stewardship encompasses a commitment to managing data in ways that they remain findable, accessible, and useful.[48] For some kinds of data, stewardship requires

46. *See generally* Franke Kreuter & Roger D. Peng, *Extracting Information from Big Data: Issues of Measurement, Inference, and Linkage*, *in* PRIVACY, BIG DATA, AND THE PUBLIC GOOD: FRAMEWORKS FOR ENGAGEMENT 257 (Julia Lane et al. eds., 1 ed. 2014).

47. *See* MALCOLM BROWN, JOANNE DEHONEY & NANCY MILLICHAP, THE NEXT GENERATION DIGITAL LEARNING ENVIRONMENT: A REPORT ON RESEARCH 3–4 (2015), https://library.educause.edu/~/media/files/library/2015/4/eli3035-pdf.pdf [https://perma.cc/9FQM-C46U].

48. *See, e.g.*, Mark D. Wilkinson et al., *The FAIR Guiding Principles for scientific data management and stewardship*, 3 SCI. DATA (2016); BROWN ET AL., *supra* note 47, at 4; Ge Peng et al., *A Unified Framework for Measuring Stewardship Practices Applied to Digital Environmental Datasets*, 13 DATA SCIENCE JOURNAL 231, 234–36 (2015); *About the National Digital Stewardship Alliance*, NAT'L DIG. STEWARDSHIP ALL., https://ndsa.org/about/ [https://perma.cc/GQG5-W4FJ] (last visited Aug. 15, 2018); Myron P. Gutmann et al., *Stewardship Gap Project*,

indefinite preservation; for others, stewardship requires regular cycles of record disposal.[49] However, given the dynamic nature of these data collections, traditional archival approaches to sustaining access to static resources are unlikely to suffice. In an "age of algorithms" where datasets are in constant flux and can be disaggregated and reaggregated continuously for multiple analytical purposes, new approaches are sorely needed.[50]

Although universities have broad responsibilities for stewarding the data they collect, acquire, and hold, some individual persons, offices, committees, or other entities must take specific actions, make investments, and manage the daily operations of data stewardship. Determining which entities have which responsibilities, based on what criteria and policies, is the process of governance. The UC Privacy and Information Security Initiative (PISI), discussed in framing this Article, was among the first to address this process in U.S. higher education. The PISI principles explicitly acknowledge the "distributed nature of information stewardship at UC, where responsibility for privacy and information security resides at every level."[51] Universities are unlikely to appoint "data czars" responsible for all manner of research and grey data. More feasible is for an office or committee to wrangle generalized policies, agreements, and governance mechanisms.

1. Research Data

Responsibility for research data in universities generally defaults to the researchers who collected those data. These researchers have a vested interest in exploiting and protecting these data. They also are the people who know most about the data's content and context. Local knowledge is essential to data management, given the vast array of data types, domain expertise, policies, and practices. Along with the benefits of local control come limitations in expertise and continuity. In domains with external funding, graduate students and post-doctoral fellows conduct most data collection and perform most of the

http://www.colorado.edu/ibs/cupc/stewardship_gap/ [https://perma.cc/SC6X-CZSW] (last visited Aug. 15, 2018); *see also generally* NAT'L ACAD. SCI., ENSURING THE INTEGRITY, ACCESSIBILITY AND STEWARDSHIP OF RESEARCH DATA IN THE DIGITAL AGE (2009).

49. *See Records Retention & Disposition Guidelines*, UCLA CORP. FIN. SERS., https://www.finance.ucla.edu/tax-records/records-management/records-retention-disposition-guidelines [https://perma.cc/7AF6-D8MN] (last visited Aug. 15, 2018); Special Section on Selection, Appraisal, and Retention of Digital Scientific Data, 3 DATA SCIENCE JOURNAL 191–232 (2004); CAROL BLUM, COUNCIL ON GOVERNMENTAL RELATIONS, ACCESS TO, SHARING AND RETENTION OF RESEARCH DATA: RIGHTS & RESPONSIBILITIES (2012), https://www.cogr.edu/sites/default/files/access_to_sharing_and_retention_of_research_data-_rights_%26_responsibilities.pdf [https://perma.cc/4AFR-CBVB].

50. *See* Clifford Lynch, *Stewardship in the "Age of Algorithms"*, 22 FIRST MONDAY (2017).

51. UC PRIVACY & INFO. SEC. INITIATIVE STEERING COMM., *supra* note 3, at 8.

management tasks. Students and post-docs often write software code, scripts, and algorithms to analyze those data. Although experts in a research domain, students and post-docs rarely are also experts in data management or software engineering. They perform essential research tasks but are short-term employees who are replaced every few years as students graduate, fellowships end, and grant projects are completed.[52]

As papers are submitted for publication and grant closure looms, many authors and investigators are responsible for releasing associated data. If so, they need to find (and often to fund) ways of sustaining access to their data for some specified number of years after the granting period. The preferred solution is usually to deposit datasets in a data archive or repository, whether organized by discipline, data type, or institution, as these entities tend to have long-term commitments and staff responsible for curation. Archiving of digital research data has been under way for at least fifty years by entities such as the World Data Systems,[53] IQSS,[54] and ICPSR.[55] Some agencies fund research and data archives to sustain access to findings, such as the National Institutes of Health (U.S.) and Economic and Social Research Council (U.K.). Other funding agencies may require universities to maintain their own data archives as a condition of receiving grants.[56] Many public archives, however, are funded by research grants, which limits their ability to make indefinite commitments.

2. Grey Data

Responsibility for grey data is highly diffuse in universities. Those who collect data may become the stewards of those data or may pass them to other stewards inside or outside the institution. Among the many data collectors and stewards of grey data are libraries, registrars, undergraduate and graduate divisions, schools and departments, instructional development, individual faculty and staff, and administrators of housing, food services, student stores, and many more. Here too, students and other limited-term staff may have

52. *See* BORGMAN, *supra* note 6.

53. *See Trusted Data Services for Global Science*, ICSU WORLD DATA SYS., https://www.icsu-wds.org/ [https://perma.cc/6KBA-BHYU] (last visited Aug. 15, 2018).

54. *See* HARVARD INST. FOR QUANTITATIVE SOC. SCI., https://www.iq.harvard.edu/home [https://perma.cc/TR2X-W4TZ] (last visited Aug. 15, 2018); HARVARD DATAVERSE, https://dataverse.harvard.edu/ [https://perma.cc/6SS3-Z9N9] (last visited Aug. 15, 2018).

55. *See* INTER-UNIVERSITY CONSORTIUM FOR POLITICAL AND SOCIAL RESEARCH (ICPSR), http://www.icpsr.umich.edu/icpsrweb/ICPSR/ [https://perma.cc/9WZC-C4PV] (last visited Aug. 15, 2018).

56. *Expectations*, U.K. ENG'G & PHYSICAL SCI. RESEARCH COUNCIL, www.epsrc.ac.uk/about/standards/researchdata/expectations/ [https://perma.cc/MHQ4-5J8U] (last visited Aug. 15, 2018).

substantial responsibility for day-to-day data collection and management. Many of these data have transient value, but many may be kept indefinitely, whether for potential later use as stores cumulate or because it is often easier to keep them than to invest the labor necessary to discard records selectively.

Where compliance rules for data protection and management clearly apply, universities will implement those rules. The larger problem is the growing collections of grey data where few rules are explicitly applicable and data stewards must exercise discretion.

B. PRIVACY

Privacy is an essential but elusive concept, as Chemerinsky,[57] Solove,[58] Nissenbaum,[59] and others have eloquently explained. It lacks a single core essence and is best understood as a pluralistic construct that spans information collection, processing, dissemination, accessibility, autonomy, and certain types of intrusion. Privacy is best understood in a context, such as a university's relationship to the data it collects, acquires, and holds. Somewhat different considerations apply to research and to grey data, although even this boundary is porous and mutable.

Privacy issues associated with data usually involve records collected about individuals—a foundational area of privacy law and policy. The Code of Fair Information Practice, known as FIPS (or FIPPS for Fair Information Practice Principles), generally applies, regardless of the intended purpose for data collection. FIPS was formulated in the early days of digital records and incorporated in the foundational U.S. laws about government data collection in the 1970s. The U.S. FIPS became the basis for the OECD principles in 1980, updated in 2013, which are widely promulgated and adopted.[60] HIPAA

57. *See* Erwin Chemerinsky, *Rediscovering Brandeis's Right to Privacy*, 45 BRANDEIS L.J. 643, 644–45 (2006).

58. *See* DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 1–11 (2010 ed.).

59. *See* HELEN NISSENBAUM, PRIVACY IN CONTEXT: TECHNOLOGY, POLICY, AND THE INTEGRITY OF SOCIAL LIFE 2–4 (1st ed. 2009).

60. *See* ORG. FOR ECON. COOPERATION & DEV., THE OECD PRIVACY FRAMEWORK 69–71 (2013), http://www.oecd.org/internet/ieconomy/privacy-guidelines.htm [https://perma.cc/526E-365M] [hereinafter OECD PRIVACY FRAMEWORK]; ORG. FOR ECON. COOPERATION & DEV., OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (1980), http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm [https://perma.cc/9GZC-PS8H] [hereinafter OECD 1980 GUIDELINES]; OFFICE OF THE ASSISTANT SEC'Y FOR PLANNING & EVALUATION, U.S. DEP'T OF HEALTH & HUMAN SERVS. RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS (1973), https://aspe.hhs.gov/report/records-computers-and-rights-citizens [https://perma.cc/CN94-XMZW].

(medical patient records) and FERPA (educational records), for example, incorporate most of the FIPS principles.

Requirements for notice of data collection and consent to acquire specific kinds of data are the most widely implemented of the FIPS principles. These two principles continue to be required not only in research contexts, but in credit, housing, social media, and any online service that collects data about individuals—even if the notice and consent contract is buried in the fine print of "click through" agreements.[61] Other OECD FIPS principles provide important privacy guidance, such as the Data Quality Principle, which says "personal data should be relevant to the purposes for which they are to be used, and . . . should be accurate, complete, and kept up-to-date"; the Purpose Specification Principle, which requires that the intended uses for collection be specified in advance; and the Use Limitation Principle, that subsequent uses should be limited to those specified and not repurposed without consent of the data subject, unless by other legal authority.[62] Other FIPS principles include security safeguards, openness, individual participation, and accountability.[63]

Protecting privacy by maintaining confidentiality is among the central concerns in human subjects research. Rules for the treatment of human subjects were developed in the same era as the FIPS principles. The Belmont Report, a FIPS-era foundational document, established three premises for protection of human subjects: respect for persons, beneficence, and justice. The Belmont principles, in turn, are the basis for Institutional Review Boards (IRB) at universities and other research institutions, which are administered with U.S. government oversight.[64]

Investigators who conduct human subjects research intentionally, as in much of the social sciences, health, and medical domains, submit their research proposals and protocols to the appropriate Institutional Review Board. The IRB determines whether the study complies with federal regulations and the amount of oversight required. Some studies are exempt, while others require

61. *See, e.g.*, Jeffrey Kenneth Hirschey, *Symbiotic Relationships: Pragmatic Acceptance of Data Scraping*, 29 BERKELEY TECH. L.J. 897, 916–17 (2014); TERMS AND CONDITIONS MAY APPLY (Hyrax Films 2013) (explaining how notice and consent may be obfuscated in the fine print of click through agreements).

62. OECD PRIVACY FRAMEWORK, *supra* note 60, at 75.

63. *See id.* at 14–15.

64. *See* NAT'L COMM'N FOR THE PROT. OF HUMAN SUBJECTS OF BIOMEDICAL & BEHAVIORAL RESEARCH ET AL., THE BELMONT REPORT: ETHICAL PRINCIPLES AND GUIDELINES FOR THE PROTECTION OF HUMAN SUBJECTS OF RESEARCH 4–6 (1979) [hereinafter BELMONT REPORT], https://www.hhs.gov/ohrp/sites/default/files/the-belmont-report-508c_FINAL.pdf [https://perma.cc/7V9J-DAV8].

extensive and continuing review.[65] If human subjects data are to be released upon publication or conclusion of the study, de-identification and anonymization of individuals normally is required, following protocols for best practice in a given domain.

Despite the long history of privacy regulations and best practices in universities, many privacy issues are emerging in areas not clearly covered by FIPS, Institutional Review Boards, or regulations such as HIPAA, FERPA, and PII (Personally Identifiable Information). These include research projects that capture records of human activity, whether traces of online or offline activity, historical records, or incidental observations of individuals with technologies such as cameras, audio recorders, drones, or other sensors during investigations for other purposes.

Learning analytics are a primary example of grey data that contains sensitive and often personally identifiable data about individuals, but that is not subject to IRB rules for confidentiality and data protection. Some universities insist on explicit notice and consent to collect data about students' online behavior, but many assume that students have given implicit consent by enrolling in the university. Students may not know what is being collected about them, much less what is being done with those data or who has access to them.[66] FERPA provides little guidance in using or protecting these data, as learning analytics appear to fall in the generally allowable category of educational uses.[67]

The UC Privacy and Information Security Initiative and the UCLA Data Governance Task Force both addressed data privacy issues by distinguishing

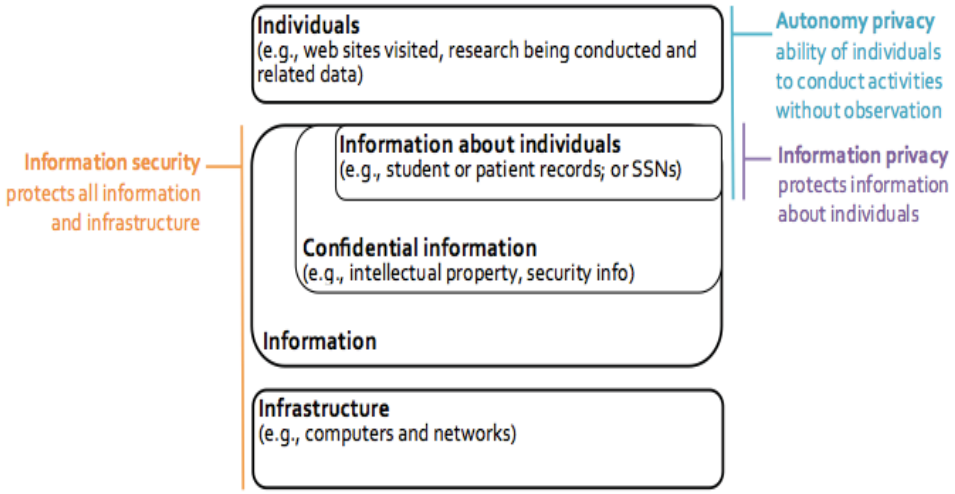
65. *See* NAT'L RESEARCH COUNCIL, PROPOSED REVISIONS TO THE COMMON RULE: PERSPECTIVES OF SOCIAL AND BEHAVIORAL SCIENTISTS, WORKSHOP SUMMARY 26–27 (Robert Pool ed. 2013).

66. *See generally* Brown, *supra* note 44; Lisa Ho, *Naked in the Garden: Privacy and the Next Generation Digital Learning Environment*, EDUCAUSE REV. (July 31, 2017), https://er.educause.edu:443/articles/2017/7/naked-in-the-garden-privacy-and-the-next-generation-digital-learning-environment [https://perma.cc/9PRN-X3K4] (last visited Sep 27, 2017); *Asilomar II: Student Data and Records in the Digital Era*, STANFORD, https://sites.stanford.edu/asilomar/ [https://perma.cc/FF7G-XYPN] (last visited Aug. 15, 2018); *The Asilomar Convention for Learning Research in Higher Education*, ASILOMAR CONVENTION (June 13, 2014), http://asilomar-highered.info/asilomar-convention-20140612.pdf [https://perma.cc/E5XC-AN2L]; Selinger, *supra* note 45; Sharon Slade & Paul Prinsloo, *Learning Analytics: Ethical Issues and Dilemmas*, 57 AM. BEHAVIORAL SCIENTIST 1509 (2013).

67. *See* Steven J. McDonald, *A Few Things about E-FERPA*, EDUCAUSE REV. (Jan. 28, 2013), https://er.educause.edu:443/blogs/2013/1/a-few-things-about-eferpa [https://perma.cc/K5RC-DVJK]; Diana Orrick, *An Examination of Online Privacy Issues for Students of American Universities*, *in* INTERNATIONAL CONFERENCE ON INTERNET COMPUTING 330 (2003), https://www.educause.edu/ir/library/pdf/CSD4039.pdf [https://perma.cc/4E9L-937M].

between two types of privacy and the security necessary to protect them, as illustrated in Figure 1.

Figure 1: Relationships Between Autonomy Privacy, Information Privacy, and Information Security[68]



Information privacy is narrowly drawn to include specific information about individuals, such as those elements in the legal definitions of PII. In the California law, PII includes a specific list of data elements,[69] whereas the U.S. federal code is more general: "PII means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual."[70]

Autonomy privacy, or the ability of individuals to conduct activities without observation, is a larger category that subsumes PII. It includes safeguards from surveillance and other kinds of monitoring of behavior. Autonomy privacy overlaps with academic freedom concerns, as discussed in the next Section, because it includes the ability to conduct research without being observed. Information security, the third category in the PISI and DGTF reports, protects the confidentiality, integrity, and availability of information, and thus includes the protection of intellectual property. These committees were comprised of multiple, and sometimes competing, stakeholders. Both committees debated their issues for many months to reach consensus. Separating the concepts of autonomy privacy, information privacy,

68. UCLA DATA GOVERNANCE TASK FORCE, *supra* note 5, at 11; UC PRIVACY & INFO. SEC. INITIATIVE STEERING COMM., *supra* note 3, at 3.

69. *See* Assemb. B. 1541, 2014–2015 Leg., Reg. Sess. (Cal. 2015).

70. *See* 2 C.F.R. § 200.79 (2017).

and information security led the committees to a broader framing of privacy, security, and governance and to more concise recommendations. These categories are loosely based on legal distinctions between informational and autonomy privacy; security is necessary because current technologies have led to an "unprecedented ability to learn the most intimate and personal things about individuals . . . [and] unprecedented access to information about individuals."[71]

C. ACADEMIC FREEDOM

Like privacy, academic freedom is a complex and elusive concept. In considering university responsibilities for data, it intersects with privacy and with freedom of speech. The most succinct, and most widely adopted, statement of academic freedom is that "[t]eachers are entitled to full freedom in research and in the publication of the results"[72] because academic freedom is "fundamental to the advancement of truth."[73] It is not an absolute right to free speech; rather, the formal statement of academic freedom distinguishes between speech on one's area of expertise and speech as a private citizen, and includes conditions such as adequate performance of other academic duties.[74]

Protecting autonomy privacy is essential to protecting academic freedom. In research contexts, faculty need to be able to protect research in progress, including research data, in the free pursuit of inquiry. Scholars often "test ideas in extreme form" as a means to develop hypotheses, brainstorm with collaborators, or provoke internal debate.[75] Releasing private communications risks mischaracterizing the research and the individuals involved, and thus limits the free pursuit of truth and inquiry. Research data are part of the research process, and thus similarly subject to protection on the grounds of academic freedom and autonomy privacy.[76]

Academic freedom protection is normally associated with academic tenure.[77] Autonomy privacy, however, applies more broadly to the university

71. *See* Chemerinsky, *supra* note 57, at 656.

72. *1940 Statement of Principles on Academic Freedom and Tenure*, AM. ASS'N OF UNIV. PROFESSORS 14 (1940), https://www.aaup.org/file/1940%20Statement.pdf [https://perma.cc/Y76E-P923].

73. *See id.*

74. *See id.*

75. *Statement on the Principles of Scholarly Research and Public Records Requests*, UCLA JOINT SENATE-ADMIN. TASK FORCE ON ACAD. FREEDOM (July 2012), https://apo.ucla.edu/policies-forms/academic-freedom [https://perma.cc/Z3EZ-4ZBN].

76. UCLA DATA GOVERNANCE TASK FORCE, *supra* note 5, at 3; UC PRIVACY & INFO. SEC. INITIATIVE STEERING COMM., *supra* note 3, at 2.

77. *See* AM. ASS'N OF UNIV. PROFESSORS, *supra* note 72; *see also generally* Erwin Chemerinsky, *Is Tenure Necessary to Protect Academic Freedom?*, 41 AM. BEHAV. SCIENTIST 638

community. Non-tenured faculty, research staff, and students also conduct research and those data deserve similar protections. Autonomy privacy goes beyond the scope of academic freedom, which covers research and teaching, to include "the ability of individuals to conduct activities without observation . . . ."[78] These recent UC initiatives reinforce long-standing university policy on protecting electronic communications and media: "[t]he University recognizes that principles of academic freedom and shared governance, freedom of speech, and privacy hold important implications for the use of electronic communications."[79] With very limited exceptions, "[t]he University does not examine or disclose electronic communications records without the holder's consent."[80] These policies are strong protections against electronic surveillance. They also reinforce FIPS by requiring notice and consent to collect data about individuals.

Grey data, such as digital records about teaching and student learning, are similarly covered under the UC Electronic Communications Policy and the adopted recommendations about privacy, information security, and data governance. However, these policies appear to provide much stronger protections of privacy and academic freedom than are typical of U.S. institutions of higher education.

D. INTELLECTUAL PROPERTY

Making data open rests on the assumption that a data owner has the rights to release data and to grant reuse by others. Therein lies the rub. Data ownership in the realm of academic research rarely is made explicit, at least until disputes arise. Control of data often rests on agreements among collaborators, which may or may not be spelled out in grant proposals or publications.[81]

(1998) (addressing how the First Amendment protects the academic freedom of faculty and if there are alternatives that might provide equal safeguards).

78. UCLA DATA GOVERNANCE TASK FORCE, *supra* note 5, at 11; UC PRIVACY & INFO. SEC. INITIATIVE STEERING COMM., *supra* note 3, at 3.

79. *Electronic Communications Policy*, UNIV. OF CAL., OFFICE OF THE PRESIDENT 10 (2005), https://policy.ucop.edu/doc/7000470/ElectronicCommunications [https://perma.cc/T5L6-WMPC].

80. *Id.*

81. *See* BORGMAN, *supra* note 6, at 12, 84 (describing different approaches to data control among collaborators); *see also* Jillian Claire Wallis, The Distribution of Data Management Responsibility Within Scientific Research Groups (June 18, 2012) (unpublished Ph.D. dissertation, UCLA) https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2269079 [https://perma.cc/5EB5-S8KV] (examining data management tasks performed by members of six research groups and members' perception of data management responsibilities); PAUL A. DAVID & MICHAEL SPENCE, TOWARDS INSTITUTIONAL INFRASTRUCTURES FOR E-SCIENCE: THE SCOPE OF THE CHALLENGE 92 (2003) (articulating the nature and significance

Ownership of intellectual property carries a large set of rights and responsibilities, some which are associated with privacy protection and intrusion. Corporate owners of scholarly publishing, mass media, and social media content deploy "digital rights management" (DRM) technologies to track uses and users in minute detail.[82] These technologies have eroded traditional protections of privacy and intellectual freedom in libraries and other domains.[83] Universities, hospitals, and private businesses who own or control medical patient records are responsible for protecting the confidentiality of those records and limiting their dissemination. Despite regulations, the health industry has found ways to monetize these records, thus invading privacy and causing other harms to patients.[84] Universities have special responsibilities for managing their intellectual property in ways that protect the privacy of their communities and minimize harm.

Funding agencies usually hold principal investigators responsible for data management plans and other rules associated with intellectual products of research.[85] Journals hold authors responsible for releasing or depositing data when such rules apply.[86] Scholars acquire many kinds of data over the course

---

of non-technological issues that bear on infrastructures created to enable collaborations in e-Science); Paul A. David, *Can "Open Science" Be Protected from the Evolving Regime of IPR Protections?*, 160 J. INSTITUTIONAL & THEORETICAL ECON. 9 (2004) (explaining that in some fields, legal instituion innovations are undermining sharing of access to raw data-steams and documented database resources).

82. Julie E. Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L.J. 575 (2003).

83. *See generally* Julie E. Cohen, *A Right to Read Anonymously: A Closer Look at "Copyright Management" in Cyberspace*, 28 CONN. L. REV. 981 (1996) (discussing digital monitoring of individual reading habits for purposes of so-called "copyright management" in cyberspace); Clifford Lynch, *The Rise of Reading Analytics and the Emerging Calculus of Reader Privacy in the Digital World*, 22 FIRST MONDAY (2017) (illustrating the way reader privacy concerns are shifting from government to commercial surveillance and the interactions between government and the private sector).

84. *See* BEN GOLDACRE, BAD PHARMA: HOW DRUG COMPANIES MISLEAD DOCTORS AND HARM PATIENTS 283 (2012); Patrick Radden Keefe, *The Family That Built an Empire of Pain*, NEW YORKER (Oct. 30, 2017), https://www.newyorker.com/magazine/2017/10/30/the-family-that-built-an-empire-of-pain [https://perma.cc/9XNY-L9YX] (examining a specific case of two doctors whose "ruthless marketing of painkillers" lead to millions of addicted patients); James F. Peltz & Melody Petersen, *L.A. Billionaire Cancer Doctor Patrick Soon-Shiong Battles Business Turbulence*, L.A. TIMES (July 5, 2017, 3:00 AM), www.latimes.com/business/la-fi-soon-shiong-20170705-story.html [https://perma.cc/ME58-MK5H].

85. *See* Brian Westra, *Developing Data Management Services for Researchers at the University of Oregon*, *in* RESEARCH DATA MANAGEMENT: PRACTICAL STRATEGIES FOR INFORMATION PROFESSIONALS 375, 389 (Joyce M Ray ed., 2014).

86. COUNCIL OF SCI. EDITORS, CSE'S WHITE PAPER ON PROMOTING INTEGRITY IN SCIENTIFIC JOURNAL PUBLICATIONS 21–31 (2012), https://www.councilscienceeditors.org/wp-content/uploads/CSE-White-Paper_2018-update-050618.pdf [https://perma.cc/78SP-TZTY].

of their careers, often at great personal expense. As a consequence of these practices, faculty tend to hold research records, observations, physical samples, and other types of research data as their own property for most intents and purposes. For example, laboratory notebooks have special status in fields where patent protection may arise.[87] Strictly speaking, research data may be considered factual and thus not subject to copyright or to ownership.[88] However, the nature of "facts" is a subject of dispute among historians, philosophers, social scientists, and lawyers alike.[89]

Although many universities, including the University of California, claim ownership of research data, researchers may be largely unaware of these regulations unless disputes arise, or an individual faculty member wishes to take a substantial trove of data to another university when changing jobs.[90]

---

87. *See generally* Colin L. Bird, Cerys Willoughby & Jeremy G. Frey, *Laboratory Notebooks in the Digital Era: The Role of ELNs in Record Keeping for Chemistry and Other Sciences*, 42 CHEMICAL SOC'Y REV. 8157 (2013) (examining the foundations of the emerging opportunities for preserving and curating electronic records, focusing on ELNs); *see also* Jason T. Nickla & Matthew B. Boehm, *Proper Laboratory Notebook Practices: Protecting Your Intellectual Property*, 6 J. NEUROIMMUNE PHARMACOLOGY 4 (2011) (arguing that there is a need for research institutions to develop strict policies on the proper use and storage of research documentation); Kalpana Shankar, *Order from Chaos: The Poetics and Pragmatics of Scientific Recordkeeping*, 58 J. AM. SOC'Y FOR INF. SCI. 1457 (2007) (focusing on the process by which scientific records are created to reflect both personal need and professional norms).

88. *See* PETER BALDWIN, THE COPYRIGHT WARS: THREE CENTURIES OF TRANS-ATLANTIC BATTLE 318–83 (2014).

89. *See generally* ANN M. BLAIR, TOO MUCH TO KNOW: MANAGING SCHOLARLY INFORMATION BEFORE THE MODERN AGE (2010); Daniel Rosenberg, *Data Before the Fact*, *in* "RAW DATA" IS AN OXYMORON 15 (Lisa Gitelman ed., 2013) (sketching the early history of the concept of "data" in order to understand the way in which the space was formed).

90. *See, e.g.*, Bradley J. Fikes, *UC San Diego Sues USC and Scientist, Alleging Conspiracy to Take Funding, Data*, L.A. TIMES (July 5, 2015, 5:55 PM), http://www.latimes.com/local/education/la-me-ucsd-lawsuit-20150706-story.html [https://perma.cc/V88D-MTKT] (describing how the University of California, San Diego sued the University of Southern California and a nationally recognized Alzheimer's disease researcher alleging that they conspired to take federal funding, data and employees from a U.C. San Diego study center); Larry Gordon, Gary Robbins & Bradley J. Fikes, *What's Behind UCSD, USC Court Battle?*, SAN DIEGO UNION TRIB. (July 9, 2015, 9:15 AM), http://www.sandiegouniontribune.com/news/science/sdut-usc-ucsd-alzheimers-paul-aisen-court-legal-2015jul19-story.html [https://perma.cc/7VDM-CHRW]; Gary Robbins, *UC San Diego Wins Legal Battle in Dispute with USC Over Alzheimer's Project*, L.A. TIMES (July 24, 2015, 10:34 PM), http://www.latimes.com/local/california/la-me-0725-uc-sandiego-20150725-story.html [https://perma.cc/9V59-D4QL]; Gary Robbins & Bradley J. Fikes, *USC Siphons Away Most of Alzheimer's Program*, SAN DIEGO UNION TRIB. (Aug. 29, 2015, 12:45 PM), http://www.sandiegouniontribune.com/news/science/sdut-ucsd-usc-alzheimers-aisen-cooperative-study-2015aug29-htmlstory.html [https://perma.cc/Z3Z5-GVNY] (describing how a court ruled that USC could take over a prestigious Alzheimer's disease research program long run by U.C. San Diego after a researcher left with its data).

Little guidance exists for how data ownership policies apply to data release requirements. For example, the UC policy cited for data ownership is the last sentence of this paragraph in the Academic Personnel Manual:

> 5. Publicity of Results
>
> All such research shall be conducted so as to be as generally useful as possible. To this end, the right of publication is reserved by the University. The University may itself publish the material or may authorize, in any specific case, a member or members of the faculty to publish it through some recognized scientific or professional medium of publication. A report detailing the essential data and presenting the final results must be filed with the University. **Notebooks and other original records of the research are the property of the University.**[91]

Given the advances in research practice and digital records since the policy was established in 1958, these issues are receiving renewed attention by the Academic Senate and other UC bodies. Open access, data governance, and data ownership are among the agenda items for the UC Academic Computing and Communications Committee,[92] UC Committee on Libraries and Scholarly Communication,[93] and UC Committee on Research Policy,[94] for example.

Ownership and responsibility for grey data is particularly problematic. Although university records presumably are property of the university, many individuals and units may be involved in data collection, analysis, reporting, and management. As records are mined and combined, tracking sources and policies associated with individual datasets becomes more difficult. In principle, students own the intellectual property in their coursework, such as papers and assignments, yet some of that work and associated online activities may be captured by learning management systems or other educational technologies. When commercial partners are involved in data collection, either

91. ROBERT G. SPROUL, UNIVERSITY OF CALIFORNIA REGULATION NO. 4 (GENERAL UNIVERSITY POLICY REGARDING ACADEMIC APPOINTEES: SPECIAL SERVICES TO INDIVIDUALS AND ORGANIZATIONS) 3 (1958) (emphasis added), http://www.ucop.edu/academic-personnel-programs/_files/apm/apm-020.pdf [https://perma.cc/M3WA-9ZWC].

92. *University Committee on Academic Computing and Communications (UCACC)*, UNIV. OF CAL. ACAD. SENATE, http://senate.universityofcalifornia.edu/committees/ucacc/index.html [https://perma.cc/VJ8K-WTAJ] (last visited Aug. 15, 2018).

93. *University Committee on Library and Scholarly Communication (UCOLASC)*, UNIV. OF CAL. ACAD. SENATE, http://senate.universityofcalifornia.edu/committees/ucolasc/index.html [https://perma.cc/39Q7-GB34] (last visited Aug. 15, 2018).

94. *University Committee on Research Policy (UCORP)*, UNIV. OF CAL. ACAD. SENATE, http://senate.universityofcalifornia.edu/committees/ucorp/index.html [https://perma.cc/GZP6-S3Q3] (last visited Aug. 15, 2018).

via university contracts or software tools deployed by individual faculty, licensing and ownership of grey data may be unclear or opaque.[95]

IV. THE PRIVACY FRONTIER

The drive to collect data at ever greater volumes, velocity, and variety is moving universities into unknown territory—the "privacy frontier"—at a far faster rate than most administrators, faculty, researchers, or students are aware. Universities are competitive institutions, both internally and externally. Those who exploit data most effectively will gain research grants, awards, students, administrative efficiencies, and other rewards. Those who govern and steward their data most effectively are likely to gain greater long-term advantages. On shorter horizons, it is all too easy to exploit data in ways that risk violations of privacy. Protecting privacy adds a layer of complexity to exploiting data, but an essential layer. Institutions ignore privacy at their peril, and the perils are perhaps greatest for universities as guardians of public trust. Technologies tend to advance at a much faster pace than does the law or social practice.[96] When the technologies are in the realm of ideas and knowledge production, as is the case with research and grey data, the stakes for universities are especially high.

A. ACCESS TO DATA

Determining who has access to what data, by what criteria, when, and under what conditions is an overarching problem of data governance and stewardship. Competing values are often at stake. Openness promotes transparency and accountability, but can undermine privacy, confidentiality, and anonymity. Confidentiality is essential to protecting human subjects but can limit the uses of data and the ability to reuse data for other purposes. Trust derives from openness in some situations and confidentiality in others. Long-term stewardship is necessary for longitudinal research and for many kinds of data aggregation but may result in retaining sensitive records that should be purged regularly by law, policy, or ethical judgment. Access policies that apply to any given data collection may be multiple, conflicting, and change over time.

95. *See* UCLA DATA GOVERNANCE TASK FORCE, *supra* note 5.

96. *See generally, e.g.*, LAWRENCE LESSIG, CODE AND OTHER LAWS OF CYBERSPACE (1999) (arguing that cyberspace can be regulated by norms, markets, and technological architecture where law fails to keep pace with advancements); LAWRENCE LESSIG, THE FUTURE OF IDEAS: THE FATE OF THE COMMONS IN A CONNECTED WORLD (2001) (explaining how the internet revolution has produced a counterrevolution of creativity and how the legal landscape protected this free space); DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS (2017); SOLOVE, *supra* note 58; JULIE E. COHEN, CONFIGURING THE NETWORKED SELF: LAW, CODE, AND THE PLAY OF EVERYDAY PRACTICE (2012); ANITA ALLEN & MARC ROTENBERG, PRIVACY LAW AND SOCIETY (3d ed. 2015).

Privacy concerns abound at the intersection of research and grey data due to the vagaries of defining "research" and "research data." As discussed above, the boundaries of what is considered research are fluid. Materials collected for administrative or teaching purposes may later be considered useful for research. Conversely, data collected for research purposes might be put to practical use in university operations later.

One of the major difficulties in implementing policies for open access to research data is the lack of agreement on what content, formats, media, or artifacts are subject to release. Funding agencies and journals generally leave these specifics to investigators, as data may be released in varying states of processing. Rules and practices vary widely by agency and research domain. "Raw" data may be released, with or without sufficient documentation to make them useful to others. Conversely, highly processed data might be released, with or without sufficient documentation, software, and code to make them useful to others. Investigators may meet "the letter of the law" by releasing enough information to satisfy agency or journal requirements, while retaining control over proprietary materials that assure a competitive edge in research. Privacy protection may or may not be an issue, depending on the content of the data.[97]

When disputes arise between researchers, collaborators, funding agencies, or journals about what data are subject to release, universities may need to arbitrate in this unsettled territory. Particularly sensitive, for example, are data from grant projects that constitute dissertation research. To ensure that students can complete their degrees, that research subjects' confidentiality is protected, and that grant contracts are completed, balancing tests may be necessary. Among the reasons that research data are not released is that specific responsibility for depositing or posting data may be unclear. In most domains, data release is not part of regular scholarly practice. Rarely are the principles or mechanics of data management and dissemination covered in

97. *See generally* Christine L. Borgman et al., *Knowledge Infrastructures in Science: Data, Diversity, and Digital Libraries*, 16 INT'L J. ON DIGITAL LIBR. 207 (2015) (discussing the need for expertise in digital libraries, data science, and data stewardship); Christine L. Borgman, Jillian C. Wallis & Matthew S. Mayernik, *Who's Got the Data? Interdependencies in Science and Technology Collaborations*, 21 COMPUTER SUPPORTED COOPERATIVE WORK 485 (2012) (reporting on a long-term study of collaboration between environmental scientists, computer scientists, and engineering research teams as part of a five-university distributed science and technology research center devoted to embedded networked sensing); "RAW DATA" IS AN OXYMORON, *supra* note 89 (arguing that data are not natural resources, but rather cultural ones that need to be generated, protected, and interpreted); Pasquetto, Randles & Borgman, *supra* note 38; Wallis, *supra* note 81 (suggesting that including author contribution statements in publications would assist future users of those data in determining the appropriate contact person for questions about their creation and context).

graduate courses on research methods. Graduate students and post-doctoral fellows are the primary data-handlers in most research teams. They may not take, or be given, the data deposit responsibility by principal investigators, for example.[98]

Despite elaborate rules about what constitutes human subjects research, IRBs vary in their judgment of how sensitive any given study may be. For example, IRBs may disagree about necessary protections for records of online activity or historical records. A recent study conducted by researchers at Cornell University and Facebook that manipulated Facebook feeds raised a firestorm of ethical issues in mainstream and social media. A central question raised was when, and to what degree, did the university's IRB review the proposal. The study appears to be legal, per Facebook user agreements; experts disagree about the ethics of using information about individuals in this way.[99]

If an IRB decides that a project does not require IRB review, investigators and staff may have no alternative venue to consult. If sensitive data collection originates outside of the research realm, such as learning analytics, no consultation source may exist beyond the boundaries of the system or project. Only if and when someone wishes to publish findings from such studies does an IRB review them, by which time sensitive data may have been collected

98. *See* Wallis, *supra* note 81; *see also* Jillian C. Wallis, Elizabeth Rolando & Christine L. Borgman, *If We Share Data, Will Anyone Use Them? Data Sharing and Reuse in the Long Tail of Science and Technology*, 8 PLOS ONE e67332, e67332 (2013) (showing that releasing, sharing, and reusing data in CENS reaffirms "the gift culture of scholarship, in which goods are bartered between trusted colleagues rather than treated as commodities").

99. *See* Reed Albergotti & Elizabeth Dwoskin, *Facebook Study Sparks Soul-Searching and Ethical Questions*, WALL ST. J. (June 30, 2014, 9:01 PM), www.wsj.com/articles/facebook-study-sparks-ethical-questions-1404172292 [https://perma.cc/WCL5-BJC2] (detailing how Facebook and Cornell manipulated the news feeds of nearly 700,000 Facebook users for a week to gauge whether emotions spread on social media)); *see also* Chris Chambers, *Facebook Fiasco: Was Cornell's Study of 'Emotional Contagion' an Ethics Breach?*, GUARDIAN (July 1, 2014, 2:00 AM), http://www.theguardian.com/science/head-quarters/2014/jul/01/facebook-cornell-study-emotional-contagion-ethics-breach [https://perma.cc/4FB9-CKZM] (arguing that the Facebook and Cornell study violated ethical norms); Adam D. I. Kramer, Jamie E. Guillory & Jeffrey T. Hancock, *Experimental Evidence of Massive-Scale Emotional Contagion Through Social Networks*, 111 PNAS 8788 (2014) (describing results of the large-scale study on the use emotional manipulation); Robinson Meyer, *Everything We Know About Facebook's Secret Mood Manipulation Experiment*, ATLANTIC (June 28, 2014), https://www.theatlantic.com/technology/archive/2014/06/everything-we-know-about-facebooks-secret-mood-manipulation-experiment/373648/ [https://perma.cc/DX3V-NSFK] (outlining the information available from the study and if IRB review occurred); Gail Sullivan, *Cornell Ethics Board Did Not Pre-Approve Facebook Mood Manipulation Study*, WASH. POST (July 1, 2014), www.washingtonpost.com/news/morning-mix/wp/2014/07/01/facebooks-emotional-manipulation-study-was-even-worse-than-you-thought/ [https://perma.cc/UKN6-C3X5] (stating that the Cornell ethics board did not preapprove the Facebook study and that there was international outrage regarding the manipulation without consent).

inappropriately. These data could fall under open access release policies, depending on funding sources and publication venues. UCLA is unusual in providing an alternative consulting entity, which is the Privacy and Data Protection Board. That board is advisory and consists of faculty and administrators with a broad array of expertise in privacy matters.[100] The board has considered topics such as the content of administrative surveys of campus climate, requests to monitor online activity on campus networks, and policies for surveillance cameras and drones. Other UC campuses established similar boards as part of implementing the recommendations of the UC Privacy and Information Security Initiative.[101] The UC Academic Computing and Communications Committee is assessing ways to harmonize information technology and data governance across the UC campuses.[102]

Technological research that gathers sensitive data is a growing concern, especially when not submitted for IRB review. Researchers in engineering, for example, may have little experience with human subjects research and be unfamiliar with DHHS and IRB rules. When robotics students test image-recognition algorithms by scattering cameras around a campus, they are likely to capture all manner of human activity without notice or consent of the individuals whose images and actions are recorded. Drones are the current technology of concern, due to their surveillance capabilities and potential for harm to persons and property. Universities are beginning to grapple with ways to balance data protection with innovation in these areas.[103] Technical data such as these could be subject to open access policies and could inadvertently be released even though they are subject to PII or other protections.

B. USES AND MISUSES OF DATA

Among the greatest promises of "big data" is the ability to exploit data for innovative purposes, especially uses that were not anticipated at the time of data collection.[104] Data exploitation can lead to scientific breakthroughs,

100. *See About the UCLA Board on Privacy and Data Protection*, UCLA, http://privacyboard.ucla.edu/ [https://perma.cc/GME2-UMY8] (last visited Aug. 15, 2018).

101. *See* UC PRIVACY & INFO. SEC. INITIATIVE STEERING COMM., *supra* note 5.

102. UNIV. OF CAL. ACAD. SENATE, *supra* note 94.

103. *See* Brandon Stark, *UC Unmanned Aircraft System Safety*, UNIV. OF CAL., OFFICE OF THE PRESIDENT, http://www.ucop.edu/enterprise-risk-management/resources/centers-of-excellence/unmanned-aircraft-systems-safety.html [https://perma.cc/RD8W-7C5L] (last visited Aug. 15, 2018) (detailing safety guidance for unmanned aircraft).

104. *See* BORGMAN, *supra* note 6; *see also generally* Tom Kalil, *Big Data is a Big Deal*, WHITE HOUSE (Mar. 29, 2012, 9:23 AM), https://obamawhitehouse.archives.gov/blog/2012/03/29/big-data-big-deal [https://perma.cc/H3LQ-XXBR] ("By improving our ability to extract knowledge and insights from large and complex collections of digital data, the initiative promises to help accelerate the pace of discovery in science and engineering,

philosophical insights, and to new products and services. When data exist, clever people will find new uses for those data. The challenge is how to encourage innovation while protecting against inappropriate, privacy-invading uses of those data. Data systems subject to strict compliance regulations such as IRB, HIPAA, FERPA, and PII may be a declining portion of university data acquisition. The privacy frontier is the vast territory outside those regulated systems.

1. Anticipating Potential Uses and Misuses

When the Code of Fair Information Practices was developed nearly forty years ago, data collection was vastly smaller in scale and information systems were more discrete entities. At today's scale of data collection and aggregation, the original FIPS principles provide much less privacy protection. Revisions of FIPS issued in 2013 by the OECD addressed practical implementations based on risk management and improvements in interoperability of data systems.[105] Notice and informed consent, the foundational FIPS principles, remain necessary but are no longer sufficient.[106] When individuals consent to the collection of specific data elements, they may be giving much broader permissions than anticipated, especially when the stated purposes provide wide latitude for use in research, personalization, improving system performance, or other vagaries.

Broader data collection, for more generic purposes, increases the potential for misuses of data and for privacy risks. The benefits and risks of big data in universities can be balanced by two means. One way is to adhere more broadly to the FIPS principles, including collection limitation, data quality, use specification, and purpose specification principles. Common to both FIPS and the tenets of privacy by design is to limit data collection and to state an express justification for each data element to be acquired.[107] The second means is to

strengthen our national security, and transform teaching and learning."); ROB KITCHIN, THE DATA REVOLUTION: BIG DATA, OPEN DATA, DATA INFRASTRUCTURES AND THEIR CONSEQUENCES (1 edition ed. 2014) (offering an overview of big data, open data, and data infrastructures including analysis of the technical shortcomings of the data revolution and the implications for academic, business, and governemnt practices); PRIVACY, BIG DATA, AND THE PUBLIC GOOD: FRAMEWORKS FOR ENGAGEMENT xi (Julia Lane et al. eds., 1st ed. 2014) ("The book's authors paint an intellectual landscape that includes the legal, economic, and statistical context necessary to frame the many privacy issues [of data] . . . ."); MAYER-SCHÖNBERGER & CUKIER, *supra* note 8.

105. *See* THE OECD PRIVACY FRAMEWORK, *supra* note 60.

106. Susan Landau, *Control Use of Data to Protect Privacy*, 347 SCIENCE 504–06 (2015); UCLA DATA GOVERNANCE TASK FORCE, *supra* note 5; SOLOVE, *supra* note 58.

107. Philip E. Agre, *Institutional Circuitry: Thinking About the Forms and Uses of Information*, 14 INFO. TECH. & LIBR. 225 (1995); Bellotti & Sellen, *supra* note 9; ANN CAVOUKIAN, PRIVACY

govern uses of data once collected. Governance should include specifying who has access to what data, when, and under what circumstances, and identifying what uses are considered appropriate and inappropriate. As criteria for these judgments can change over time, governance processes to assure continuing oversight also are needed.[108]

Individual data elements that appear innocuous at the time of collection can become sensitive in later contexts. In a recent example, students' permanent addresses, which universities maintain in case of emergency, may reveal legal residency status to immigration authorities. Recent changes in the status of "Dreamers" (undocumented students who were brought to the United States as minors) made this information extremely sensitive.[109] Similarly, most universities provide minimal information about students in public directories out of concern for stalking and other harms.

Potential misuse of research data is a concern often mentioned by those reluctant to release data associated with grants or publications.[110] Data can be taken out of context to make misleading or incorrect inferences, as when health and climate data are used selectively to make claims that run counter to those of the investigators.[111]

2. Reusing Data

One person's good use or reuse of data may be seen by others as a misuse. The ability to reuse data effectively depends on factors such as the quality of the original data collection, the degree of documentation provided to interpret protocols and context, and the availability of associated software, code, and

BY DESIGN: THE 7 FOUNDATIONAL PRINCIPLES (2011), https://www.ipc.on.ca/wp-content/uploads/Resources/7foundationalprinciples.pdf [https://perma.cc/4RGR-FPUY] (arguing that mere compliance with regulatory frameworks is insufficient to protect privacy, and that organizations should instead implement privacy-protective features as a default element); OECD PRIVACY FRAMEWORK, *supra* note 60.

108. *See* UCLA DATA GOVERNANCE TASK FORCE, *supra* note 5; *see also* UC PRIVACY & INFO. SEC. INITIATIVE STEERING COMM., *supra* note 3.

109. *See* Adam Harris, *Colleges Deplore Trump's Threat to DACA. How Far Can They Go to Fight It?*, CHRON. HIGHER EDUC. (Sept. 6, 2017), http://www.chronicle.com/article/Colleges-Deplore-Trump-s/241110 (demonstrating how colleges can be "safe zones" for undocumented students).

110. Wallis, Rolando & Borgman, *supra* note 98; *see also* BORGMAN, *supra* note 6.

111. *See generally* Paul N. Edwards, *Global Climate Science, Uncertainty and Politics: Data-Laden Models, Model-Filtered Data*, 8 SCI. AS CULTURE 437 (1999) (examining how data is important in legitimizing political activity around global climate change); PAUL N. EDWARDS, A VAST MACHINE: COMPUTER MODELS, CLIMATE DATA, AND THE POLITICS OF GLOBAL WARMING (2010) (tracing the history of efforts to gather weather and climate records for the whole planet and the resulting "data friction"); BEN GOLDACRE, BAD SCIENCE: QUACKS, HACKS, AND BIG PHARMA FLACKS (2008); GOLDACRE, *supra* note 84.

instrumentation.[112] Whether research data or grey data, problems arise in measurement because collecting good data is hard to do. Considerable sophistication in the design of research or other protocols is necessary, combined with expertise in statistics and methods of data cleaning.[113] Surveys, for example, are far more complex to design, execute, analyze, and interpret than is apparent to the novice researcher—or to the staff member assigned to evaluate a service or system. Problems also arise in interpreting and drawing inferences from data because much must be known about the purposes and context in which the data were collected.

The potential for misuse and abuse multiply when data elements are aggregated, whether from one data resource or many. Variable names, units of measurement, research protocols, and circumstances of data collection introduce errors that are difficult to assess when combining data. Reliability and validity concerns abound. Estimates of the amount of labor required to "clean" data for aggregation are hard to find; one source suggests devoting about eighty percent of the work to cleaning and integration.[114] Data science is an inexact science, at best.

Despite these cleaning and analysis problems, data scientists have been remarkably effective at reidentifying individuals by aggregating records from multiple sources.[115] Researchers who wish to use sensitive data about individuals, such as medical records or certain types of surveys, often are required to sign agreements that they will not attempt to re-identify the research subjects.[116]

---

112. *See, e.g.*, Pasquetto, Randles & Borgman, *supra* note 38; Matthew S. Mayernik, *Research Data and Metadata Curation as Institutional Issues*, 67 J. ASS'N FOR INFO. SCI. & TECH. 973 (2016) (examining variability in data and metadata practices using "institutions" as the key theoretical concept); BORGMAN, *supra* note 6.

113. *See* Kreuter & Peng, *supra* note 46, at 267–69 (describing the statistical changes of integrating big data); *see also* WILLIAM R SHADISH, THOMAS D. COOK & DONALD T. CAMPBELL, EXPERIMENTAL AND QUASI-EXPERIMENTAL DESIGNS FOR GENERALIZED CAUSAL INFERENCE (2002).

114. MAYER-SCHÖNBERGER & CUKIER, *supra* note 8.

115. *See, e.g.*, Boris Lubarsky, *Re-Identification of "Anonymized Data"*, 1 GEO. L. TECH. REV. 202, 211–12 (2017); *see also* Yves-Alexandre de Montjoye et al., *Unique in the Shopping Mall: On the Reidentifiability of Credit Card Metadata*, 347 SCIENCE 536 (2015); *see also* Latanya Sweeney, *k-Anonymity: A Model for Protecting Privacy*, 10 INT'L J. ON UNCERTAINTY FUZZINESS & KNOWLEDGE-BASED SYS. 557 (2002) (suggesting methods of keeping released data ambiguous to prevent reidentification); Latanya Sweeney, Matching Known Patients to Health Records in Washington State Data (July 5, 2013) (unpublished manuscript), https://arxiv.org/abs/1307.1370 [https://perma.cc/N8J9-JSK3].

116. Jared A. Lyle, George C. Alter & Ann Green, *Partnering to Curate and Archive Social Science Data*, *in* RESEARCH DATA MANAGEMENT: PRACTICAL STRATEGIES FOR INFORMATION PROFESSIONALS (2014); NAT'L RESEARCH COUNCIL, *supra* note 65.

Intellectual property concerns also arise in aggregating data from multiple sources, whether from research, administrative, or external sources. Although any individual dataset may carry documentation about ownership and licensing, maintaining intellectual property information in provenance records through multiple generations of use is proving to be a frontier problem in the data sciences. Despite attaching licenses to datasets that protect privacy, that information can be lost downstream.[117]

3. Responsibilities for Data Collections

Responsibility for data is particularly diffuse in universities, although similar issues arise in all institutions. Research data collections are scattered across labs and stored on laptops or local servers. Multiple generations of students and staff may have access to these data, which can cumulate over long periods of time. Few of these data may involve human subjects and few of these data may be privacy-sensitive, especially when used alone. Similarly, vast collections of grey data are scattered across universities and cumulated over time. Many are purged regularly on a records-retention cycle, but many are not. Access to campus collections may be limited to the few staff who are certified for their use. In other cases, generations of student workers and other transient labor may use grey data daily in their jobs.

As universities outsource more computing systems and services to commercial entities, they relinquish a substantial degree of control over the data collected by their online systems. When universities purchase licenses for access to digital resources such as publications and grey literature, those contracts may allow data providers to track usage by identifiable individuals, in ways that undermine libraries' abilities to protect traditional rights to read anonymously.[118] Similar problems arise when universities partner with vendors for shared usage of data about individuals, such as analytics on learners or patients, whether for graduation rates or treatment outcomes. Universities are becoming more sophisticated about building privacy and security protections

117. Chaitanya Baru, *Sharing and Caring of eScience Data*, 7 INT'L J. DIGITAL LIBR. 113 (2007); Jane Hunter & Kwok Cheung, *Provenance Explorer-A Graphical Interface for Constructing Scientific Publication Packages from Provenance Trails*, 7 INT'L J. DIGITAL LIBR. 99 (2007); Mayernik, *supra* note 112; Andrew E. Treloar & Mingfang Wu, *Provenance in Support of the ANDS Four Transformations*, 11 INT'L J. DIGITAL CURATION 183 (2016); Michael Wright et al., *Connecting Digital Libraries to eScience: The Future of Scientific Scholarship*, 7 INT'L J. DIGITAL LIBR. 1 (2007); Paul Groth et al., *Requirements for Provenance on the Web*, 7 INT'L J. DIGITAL CURATION 39 (2012); James Cheny et al., *Requirements for Provenance on the Web*, W3C PROVENANCE INCUBATOR GROUP (Dec. 7, 2010, 11:52 PM), http://www.w3.org/2005/Incubator/prov/wiki/User_Requirements [https://perma.cc/2BH8-6MPL].

118. Lynch, *supra* note 83; Cohen, *supra* note 83; *An Interpretation of the Library Bill of Rights*, AM. LIBRARY ASS'N (July 1, 2014), http://www.ala.org/advocacy/intfreedom/librarybill/interpretations/privacy [http://perma.cc/Y8Z5-WBKG].

into contracts, especially where vendors have offered to sell universities data about their users.

Yet harder problems arise when faculty or staff require students to use third-party online tools that are not licensed by the university. These "free" online tools are attractive because they offer sophisticated activities, content, or evaluation capabilities suitable for a particular course. However, these tools collect personal data about their users that are shared with outside partners, barring contracts to the contrary. Students may have little choice but to opt-in to usage agreements if the software is required for course activities. A growing concern is liability when such vendors breach confidential student or faculty data, especially when no contract exists between the university and the vendor to ensure protections. Instructors and students too often are unaware of the privacy and security risks such as these. Despite university policies and warnings by technology professionals not to install such software, usage can be difficult to detect, especially by understaffed tech support offices. A shadow network of risky technology lurks on many campuses.

C. PUBLIC RECORDS REQUESTS

Given the continuing advances toward open access to publications and to data over the last several decades, it is counter-intuitive to place public records requests on the privacy frontier. Public access laws are essential to democratic societies, and university researchers often avail themselves of these laws in gaining access to information.[119] However, these laws are being used in political and frivolous ways that threaten academic freedom and privacy.[120]

Law and policy about university data collections are often ambiguous, which raises two related questions. One is that the more data that universities collect, the larger the pool of resources subject to public records requests. Hence the principle, "if you can't protect it, don't collect it." Research data on controversial topics such as climate change, guns, tobacco, and abortion are among the most common records requests.[121] Releasing data and

119. JON WIENER, GIMME SOME TRUTH: THE JOHN LENNON FBI FILES (1st ed. 2000).

120. UCLA JOINT SENATE-ADMIN. TASK FORCE ON ACAD. FREEDOM, *supra* note 75.

121. Larry Bell, *Michael Mann and the ClimateGate Whitewash: Part One*, FORBES (June 28, 2011, 1:30 PM), www.forbes.com/sites/larrybell/2011/06/28/michael-mann-and-the-climategate-whitewash-part-one/ [https://perma.cc/PE2R-QFQW]; Suzanne Goldenberg, *Virginia Court Rejects Sceptic's Bid for Climate Science Emails*, GUARDIAN (Mar. 2, 2012, 1:01 PM), http://www.theguardian.com/environment/2012/mar/02/virginia-court-sceptic-access-climate-emails [perma.cc/MX6M-DBCH]; Florence Olsen, *Historian Resigns After Report Questions His Gun Research*, CHRON. HIGHER EDUC. (Nov. 8, 2002), www.chronicle.com/article/Historian-Resigns-After-Report/35132 [https://perma.cc/Y7J7-UX6G]; Peter Schmidt, *Dispute Over Climate Scientist's Records Pits Academe Against Media Groups*, CHRON.

communications about research in progress threatens academic freedom and autonomy privacy. State public records laws vary in the degree to which they allow exceptions for research material.

Grey data also can be requested, such as information on the demographics of the student body, marital status of individuals in an academic department, or email correspondence of individual faculty or administrators.[122] As public records requests to universities have become more sophisticated, so have the responses of university counsel.[123]

The second issue is that state public records act requests in the United States apply to public universities but not to private universities or corporations. Faculty, students, and staff at public universities thus carry a higher burden in managing their data and in responding to public records requests. Responding to such requests can be extremely time-consuming and expensive, in addition to the risks to academic freedom and privacy. Researchers at public and private universities frequently collaborate with each other, which can expose the data of private universities to these requests. As a result, members of public universities may seek protections of their research materials and communications comparable to those at private universities, which also protects collaborations.[124]

An emerging area of concern is whether trends toward open access to data in some fields may undermine a university's ability to protect data from public records requests in other fields. In some domains of the biosciences, physical

---

HIGHER EDUC. (Jan. 9, 2014), http://www.chronicle.com/article/Dispute-Over-Climate/143881 [https://perma.cc/B7UC-SM47].

122. UCLA JOINT SENATE-ADMIN. TASK FORCE ON ACAD. FREEDOM, *supra* note 75; *Public Records Request*, UNIV. OF N.M., https://publicrecords.unm.edu/ [http://perma.cc/7JDA-3CX5] (last visited Aug. 15, 2018); *Public Records Requests*, UNIV. OF S. MISS., https://www.usm.edu/university-communications/public-records [https://perma.cc/GD94-7QVB] (last visited Aug. 15, 2018); *Open Records Requests*, UNIV. OF TEXAS AT AUSTIN, https://financials.utexas.edu/resources/open-records-requests [http://perma.cc/NN84-4GAF] (last visited Aug. 15, 2018); *Request a Public Record*, UNIV. OF WASH., http://www.washington.edu/publicrecords/request-a-public-record/ [http://perma.cc/DCC4-3BTQ] (last visited Aug. 15, 2018).

123. *See, e.g.*, Letter from John C. Dowling, Senior Univ. Legal Counsel, Univ. of Wis.-Madison, to Stephan Thompson, Republican Party of Wis. (Apr. 1, 2011), http://news.wisc.edu/letter-from-uw-madison-legal-counsel-regarding-cronon-emails/ [http://perma.cc/7HK2-4UKS]; Anthony Grafton, *Wisconsin: The Cronon Affair*, NEW YORKER (Mar. 28, 2011), https://www.newyorker.com/news/news-desk/wisconsin-the-cronon-affair [http://perma.cc/GK3Y-7P5U]; Sara Hebel, *Wisconsin-Madison to Release Professor's E-Mails but Withhold Those Said to Be Private*, CHRON. HIGHER EDUC. (Apr. 1, 2011), http://www.chronicle.com/article/Wisconsin-Madison-to-Release/126994 [https://perma.cc/HWS6-2YUH].

124. UCLA JOINT SENATE-ADMIN. TASK FORCE ON ACAD. FREEDOM, *supra* note 75.

sciences, and social sciences, open data is the default condition at the time of publishing research. Some researchers in some domains attempt to work completely in the open, releasing data continuously. In most academic disciplines, however, researchers maintain control of their data and records indefinitely.[125]

D. CYBER RISK AND DATA BREACHES

Universities are the third highest sector for data breaches, constituting about ten percent of reported breaches; healthcare and retail are the top two sectors.[126] From 2005 to late-2017,[127] colleges and universities reported about 800 breaches, affecting more than twenty-five million records.[128] Institutions of higher education have extensive data resources and may be perceived as more vulnerable to attack than hospitals, banks, governments, retail, or other entities. Research universities are commonly targeted for the intellectual property manifest in research content. Those with medical centers are targeted for patient records, which are valuable resources for identity and insurance theft. Student records have become high value targets because logon credentials provide access to expensive licensed content from publishers and other sources. Intruders seeking one kind of information may wander through other databases along the way. Data on individuals that are held by third parties, such as collaborating universities or outside contractors, also are vulnerable to breach.

Education is the institutional sector facing the greatest challenges in balancing access and protection. Universities are heterogeneous institutions that acquire many kinds of data and need sophisticated, layered approaches to cyber security. Whereas the financial and intelligence sectors, for example, may prioritize cyber risk protection in the extreme, universities are open by design, encouraging the free flow of information throughout their communities. Individuals partner with collaborators from other institutions, countries, and cultures, which requires shared access to online resources. Campus visitors are vast in number and need access to networks to participate in local activities. Student and staff turnover is high due to short courses and short-term contracts. As a result of these operating conditions, universities must secure their systems and networks without crippling their missions of research,

125. BORGMAN, *supra* note 6, at 276.

126. SYMANTEC, ISTR20: INTERNET SECURITY THREAT REPORT 17 (2015), https://www.symantec.com/content/en/us/enterprise/other_resources/21347933_GA_RPT-internet-security-threat-report-volume-20-2015.pdf [https://perma.cc/2WHW-DVHX].

127. For purposes of this Article, the time period of analysis extends to November 3, 2017.

128. *Data Breaches*, PRIVACY RIGHTS CLEARINGHOUSE, https://www.privacyrights.org/data-breaches [http://perma.cc/DG2S-E8Z8] (last visited Aug. 15, 2018).

teaching, and service. Research data must flow to students for use in class projects, albeit in a controlled manner. Network security must not become ubiquitous with surveillance.

Cyber risk takes many forms, such as phishing attacks on individuals, viruses, bots, ransomware, data breaches, and distributed denial of service attacks. The list grows by the day. Some risks are obvious, such as the need for many layers of protection on patient data. Others are less obvious, such as attacking a student admissions database for competitive information. Systems are only as well protected as their weakest link. The Target Store breach of credit card records resulted from a successful hack of their HVAC system.[129] A distributed denial of service attack on Netflix was launched by mobilizing networked household devices, most notably baby monitors.[130] The ability to mobilize small devices for big attacks will grow as the Internet of Things expands, potentially becoming the "Internet of Terror."[131]

Universities are following the lead of the public and private sectors in enhancing security of their systems, training their communities, and promoting good practices for "cyber health." Deleterious computer-related events are difficult to anticipate, and no sector of the economy is immune to attack.[132]

---

129. Jaikumar Vijayan, *Target Attack Shows Danger of Remotely Accessible HVAC Systems*, COMPUTERWORLD (Feb. 7, 2014, 6:52 AM), www.computerworld.com/article/2487452/cybercrime-hacking/target-attack-shows-danger-of-remotely-accessible-hvac-systems.html [http://perma.cc/GSE3-GXD3].

130. Haley Sweetland Edwards, *How Web Cams Helped Bring Down the Internet, Briefly*, TIME (Oct. 25, 2016), http://time.com/4542600/internet-outage-web-cams-hackers/ [http://perma.cc/Z6XX-RVHL].

131. George V. Neville-Neil, *IoT: The Internet of Terror*, 60 COMM. ACM 36 (2017).

132. *See* Peter G. Neumann, *Far-Sighted Thinking About Deleterious Computer-Related Events*, 58 COMM. ACM 30 (2015); Taylor Armerding, *The 17 Biggest Data Breaches of the 21st Century*, CSO ONLINE (Jan. 26, 2018, 3:44 AM), https://www.csoonline.com/article/2130877/data-breach/the-16-biggest-data-breaches-of-the-21st-century.html [http://perma.cc/39QF-EWBP]; Waqas Amir, *Unprotected S3 Cloud Bucket Exposed 100GB of Classified NSA Data*, HACKREAD, (Nov. 29, 2017), https://www.hackread.com/unprotected-s3-cloud-bucket-exposed-100gb-of-classified-nsa-data/ [http://perma.cc/8FYA-8DVJ] (describing a breach that made public classified information for political leaders and U.S. military); David Greene, *NSA's Hackers Were Themselves Hacked in Major Cybersecurity Breach*, NPR (Nov. 14, 2017, 5:00 AM), https://www.npr.org/2017/11/14/564006460/nsas-hackers-are-hacked-in-major-cybersecurity-breach [http://perma.cc/9YVF-2UF6]; Andy Greenberg, *He Perfected a Password-Hacking Tool—Then the Russians Came Calling*, WIRED (Nov. 9, 2017, 7:00 AM), https://www.wired.com/story/how-mimikatz-became-go-to-hacker-tool/ [http://perma.cc/N6XW-QU7C] (describing a Russian hacker attempting to steal a French programmer's source code in a hotel lobby in Moscow); Julie Angwin, *How Journalists Fought Back Against Crippling Email Bombs*, WIRED (Nov. 9, 2017, 7:00 AM), https://www.wired.com/story/how-journalists-fought-back-against-crippling-email-bombs/ [http://perma.cc/SV3J-8PF5]; Susan Landau, *The Real Security Issues of the iPhone Case*, 352 SCIENCE 1398 (2016).

No online system ever can be completely secure, any more than any building is completely secure from physical attack. By analogy, security comes in layers of locks, cameras, sensors, and alerts.[133] Resilience and recovery also have become watchwords for cybersecurity. The severity of attacks must be minimized, but backup and recovery plans also are necessary.[134] The costs and benefits of each tactic must be evaluated, lest funds spent on protection lessen the investment in the mission of the institution.

A looming challenge on the privacy frontier is how to secure the privacy of human subjects once data are collected. IRBs focus on the design of studies, confidentiality, notice and consent, and good practices for data storage and backup. Their membership is drawn from researchers across campus who have expertise in research design and methods. IRBs, and the university staff that support them, are not necessarily experts in security, cyber risk, cryptography, or in the open data policies to which research projects may be subject. Investigators are required to report on research progress at regular intervals. However, short of known data breaches, IRBs have few mechanisms to follow up on data security. Data management practices vary widely by domain, thus IRBs lack common standards to enforce across campuses.[135] Governance models need to promote more engagement between IRBs, investigators, cyber security units, and other parts of the research enterprise. Among the concerns that universities and other sectors must address are methods of anonymization; responsibilities for data protection, release, and stewardship; and accountability for secure and responsible data management practices.

E. CURATING DATA FOR PRIVACY PROTECTION

Data management is an expensive endeavor, and one that has come to the fore in the research data arena.[136] Any entity that collects data must make

133. BRUCE SCHNEIER, SECRETS & LIES: DIGITAL SECURITY IN A NETWORKED WORLD (2000).

134. *See* Matthew Goche & William Gouveia, *Why Cyber Security Is Not Enough: You Need Cyber Resilience*, FORBES (Jan. 15, 2014, 8:14 AM), www.forbes.com/sites/sungardas/2014/01/15/why-cyber-security-is-not-enough-you-need-cyber-resilience/ [http://perma.cc/V7CX-FMEU]; IGOR MIKOLIC-TORREIRA ET AL., A FRAMEWORK FOR EXPLORING CYBERSECURITY POLICY OPTIONS (2016), https://www.rand.org/pubs/research_reports/RR1700.html [https://perma.cc/3AAM-VDAB]; NAT'L INST. OF STANDARDS & TECH., FRAMEWORK FOR IMPROVING CRITICAL INFRASTRUCTURE CYBERSECURITY 1–39 (2014), https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf [https://perma.cc/RZ55-ER8U].

135. Shankar, *supra* note 87; Melissa H Cragin & Kalpana Shankar, *Scientific Data Collections and Distributed Collective Practice*, 15 COMPUTER SUPPORTED COOPERATIVE WORK 185 (2006).

136. *See generally* FRANCINE BERMAN ET AL., SUSTAINABLE ECONOMICS FOR A DIGITAL PLANET: ENSURING LONG-TERM ACCESS TO DIGITAL INFORMATION 61 (2010),

conscious decisions about which data are worth sustaining, which can be discarded, and which might be allowed to fade away.[137] Maintaining privacy protections and reducing risks is essential to accomplishing these goals.

Digital data do not survive by benign neglect. Continuous investments are required to refresh computers, storage devices, software, and websites. Regular technology maintenance is but a baseline for longer term data curation, however. Larger challenges arise when software is updated, is no longer available, or is not supported; when computer ports and drivers are not compatible with current equipment; when data processing pipelines are poorly documented; and when those with critical expertise graduate or leave the university. Thus, digital data remain useful only through investments in curation, documentation, and migration to new formats and systems. Systems and data collections need to be assessed on a cyclical basis, purging sensitive data based on retention rules and refreshing data collections worthy of continuing access. Maintaining provenance records is essential, lest data collections be separated from information about origins; licensing and ownership; applicable regulations; records of notice, consent, and acceptable uses; authorizations for access; and other contexts.[138] Archivists, records managers, and librarians should be closely involved in these processes.[139]

Responsibility for data collections is highly distributed in universities, which complicates curating data collections in the short and long term. A researcher with expertise in data management or with the resources to invest in long-term sustainability of research data is rare. Even more rare is the researcher with expertise in data archiving, records management, and the legal

---

http://brtf.sdsc.edu/biblio/BRTF_Final_Report.pdf [https://perma.cc/4P3K-XV4D]; Berman & Cerf, *supra* note 15; BORGMAN, *supra* note 6.

137. Christine L. Borgman, *Not Fade Away: Social Science Research in the Digital Era*, PARAMETERS (June 23, 2016), http://parameters.ssrc.org/2016/06/not-fade-away-social-science-research-in-the-digital-era/ [https://perma.cc/8JSQ-YDE9].

138. Miriam Ney, Guy K. Kloss & Andreas Schreiber, *Using Provenance to Support Good Laboratory Practice in Grid Environments*, *in* DATA PROVENANCE AND DATA MANAGEMENT IN ESCIENCE 157, 157–59 (Qing Liu et al. eds., 2011); Lucian Carata et al., *A Primer on Provenance*, 57 COMM. ACM 52, 52 (2014) ("[D]iscussing not only existing systems and the fundamental concepts needed for using them in applications today, but also future challenges and opportunities."); Jinfang Niu, *Provenance: Crossing Boundaries*, 41 ARCHIVES & MANUSCRIPTS 105 (2013) (surveying different provenance practices for different subject matters, data types, and professional field specializations); PROVENANCE AND ANNOTATION OF DATA (Ian Foster & Luc Moreau eds., 2006); Clifford A. Lynch, *When Documents Deceive: Trust and Provenance as New Factors for Information Retrieval in a Tangled Web*, 52 J. AM. SOC'Y FOR INFO. SCIENCE & TECH. 12 (2001); Jun Zhao et al., *Linked Data and Provenance in Biological Data Webs*, 10 BRIEFINGS IN BIONFORMATICS 139 (2009).

139. Ney, Kloss & Schreiber, *supra* note 138; Carata et al., *supra* note 138, at 52–60; Niu, *supra* note 138; FOSTER & MOREAU, *supra* note 138; Lynch, *supra* note 138; Zhao et al., *supra* note 138.

vagaries of records retention cycles. Similarly, few of the administrative staff involved in collecting and analyzing grey data are records management experts. All of these individuals and offices need somewhere to turn for guidance and responsibility to ensure that universities make wise choices for what to keep, what to discard, how, and when.

Institutions more readily claim ownership of data than take responsibility for curating those data. Ownership and stewardship need to be more tightly coupled in universities, and probably in most other types of institutions.

V. CONCLUSIONS AND RECOMMENDATIONS

Universities are as enamored of "big data" as other sectors of the economy and are similarly effective in exploiting those data to competitive advantage. They have privileged access to research data and to data about their communities, all of which can be mined and combined in innovative ways. Universities also have a privileged social status as guardians of the public trust, which carries additional responsibilities in protecting privacy, academic and intellectual freedom, and intellectual property. They must be good stewards of the data entrusted to them, especially when conflicts arise between community practices and values. For some kinds of data, good stewardship requires that access to data be sustained indefinitely, and in ways that those data can be reused for new purposes. For other kinds of data, good stewardship requires that they be protected securely for limited periods of time and then destroyed. Factors that distinguish data worth keeping or discarding vary widely by domain, content, format, funding source, potential for reuse, and other circumstances.[140] Criteria for data protection and access also can change over time, whether due to different uses of a data collection, such as grey data being mined for research or research data being deployed for operations; transfer of stewardship within and between institutions; changes in laws and policies; or new externalities.

The rate of data collection has grown exponentially over the last decade through both research and grey data within universities, along with data collection in the other economic sectors with which universities partner. These include government and business, social media, sensor networks, the Internet of Things, and much more. As the ability to mine and combine data improves, and technologies become more interoperable, the boundaries between data types and origins continue to blur. Responsibilities for stewardship and exposure to cyber risk increases accordingly. Risks to privacy invasion, both information privacy and autonomy privacy, accelerate as most of these data can be associated with individuals, whether as content or creators of data.

140. BORGMAN, *supra* note 6, at 271–87.

Anonymity, which is fundamental to most methods of privacy protection, has become extremely difficult to sustain as methods of re-identifying individuals become more sophisticated. Notice and informed consent remain necessary but are far from sufficient for maintaining privacy in universities or in other sectors.

Open access to publications and to data are social policies that promote transparency and accountability in the research enterprise. Adoption is uneven because costs, benefits, and incentives for open access, especially to data, are aligned in only a few fields and domains. For most researchers, releasing data involves considerable costs, with benefits going to others. These costs may include curation (e.g., providing metadata, documentation, and records of provenance and licensing), computer storage and maintenance, software acquisition and maintenance, migration to new software and hardware, and fees for data deposit. Disposal of data also involves costs to assess what to keep and what to discard, and to ensure safe destruction of confidential or proprietary materials. Individual researchers, their employers, or their funders may bear the costs of data stewardship and responsibilities for protecting privacy, academic and intellectual freedom, intellectual property, and other values.

None of these frontier challenges is easily addressed, nor will appropriate responses be consistent across the university sector in the U.S., much less in other countries and cultures. Data are valuable institutional assets, but they come at a price. Individuals and institutions must be prepared to protect the data they collect. These recommendations, which draw heavily on experiences in the University of California, are offered as starting points for discussion.

A. BEGIN WITH FIRST PRINCIPLES

Universities should focus on their core missions of teaching, research, and services to address priorities for data collection and stewardship. Tenets of privacy by design, the Code of Fair Information Practice, the Belmont Report,[141] and codifications of academic and intellectual freedom are established and tested. Implementation is often incomplete, however. For faculty, students, staff, research subjects, patients, and other members of the university community to enjoy protection of information and autonomy privacy, more comprehensive enforcement of principles such as limiting data collection, ensuring data quality, and constraining the purposes for each data element is necessary. Digital data do not survive by benign neglect, nor are records destroyed by benign neglect. Active management is necessary. Notice and consent should never be implicit. When institutions ask for permission to

141. BELMONT REPORT, *see supra* note 64, provides the basis for human subjects regulation by Institutional Review Boards, as governed by the DHHS. *See supra* Section II.A.1.

acquire personal data, are transparent, and are accountable for uses of data, they are more likely to gain respect in the court of public opinion.

B. EMBED THE ETHIC

Data practices, privacy, academic and intellectual freedom, intellectual property, trust, and stewardship all are moving targets. Principles live longer than do the practices necessary to implement those principles. Universities are embedding data science and computational thinking into their curricula at all levels. This is an opportune moment to embed data management, privacy, and information security into teaching and practice as well. By encouraging each individual to focus on uses of data, the problem becomes personal. Rather than collecting all data that could conceivably be collected, and exploiting those data in all conceivable ways, encourage people to take a reflective step backwards. Consider the consequences of data collection about yourself and others, and how those data could be used independently or when aggregated with other data, now and far into the future. Think about potential opportunities and risks, for whom, and for how long. Study data management processes at all levels and develop best practices. Collect data that matter, not just data that are easy to gather. Interesting conversations should ensue. The Golden Rule still rules.

C. PROMOTE JOINT GOVERNANCE

The successes of the University of California in developing effective principles for governing privacy and information security have resulted from extensive deliberations between faculty, administrators, and students. These can be long and arduous conversations to reach consensus but have proven constructive at creating communication channels and building trust. Many years of conversations about information technology policy at UCLA, for example, have resulted in much deeper understanding between parties. Faculty have learned to appreciate the challenges faced by administrators who need to balance competing interests, keep systems running, and pay for infrastructure out of fluctuating annual budgets. Administrators, in turn, have learned to appreciate the challenges faced by faculty who have obligations to collaborators, funding agencies, and other partners scattered around the world, and daily obligations to support students who have disparate skills and access to disparate technologies. Institutional learning is passed down through generations of faculty, students, and administrators through joint governance processes. These mechanisms are far from perfect and can be slow to respond at the pace of technological change. However, echoing Churchill's assessment of democracy, it works better than any other system attempted to date.

D. PROMOTE AWARENESS AND TRANSPARENCY

The massive data breaches of Equifax, Target stores, J.P. Morgan Chase, Yahoo, the National Security Agency, and others have raised community awareness about data tracking, uses of those data by third parties, and the potential for exposure.[142] This is an ideal time to get the community's attention about opportunities and risks inherent in data of all kinds. Individuals, as well as institutions, need to learn how to protect themselves and where to place trust online. People may react in anger if they suspect that personal data are being collected without notice and consent or think they are being surveilled without their knowledge.[143] Universities are at no less cyber risk than other sectors but are still held to higher standards for the public trust. They have much to lose when that trust is undermined.

E. DO NOT PANIC

Panic makes people risk-averse, which is counterproductive. Locking down all data lest they be released under open access regulations, public records requests, or breaches will block innovation and the ability to make good use of research data or grey data. The opportunities in exploiting data are only now becoming understood. Balanced approaches to innovation, privacy, academic and intellectual freedom, and intellectual property are in short supply. Patience and broad consultation of stakeholders is needed.

142. *See* Armerding, *supra* note 132; Amir, *supra* note 132; Greene, *supra* note 132.

143. Steve Lohr, *At Berkeley, a New Digital Privacy Protest*, N.Y. TIMES (Feb. 1, 2016), https://www.nytimes.com/2016/02/02/technology/at-uc-berkeley-a-new-digital-privacy-protest.html [https://perma.cc/F6CN-CAEG]; The Associated Press, *Online Attacks at UCLA Health Exposed 4.5 Million*, N.Y. TIMES (July 17, 2015), https://www.nytimes.com/2015/07/18/business/online-attacks-at-ucla-health-exposed-4-5-million.html [http://perma.cc/WE56-LB4Y].

PATENT LITIGATION IN CHINA: CHALLENGING CONVENTIONAL WISDOM

Renjun Bian†

ABSTRACT

The People's Republic of China has become a world leader in both patent applications and patent litigation after the Chinese government enacted new policies to stimulate domestic innovation and patent activities. These major developments have made China an integral venue of international patent protection for inventors and entrepreneurs. However, due to the lack of judicial transparency before 2014, most people had virtually no access to Chinese patent litigation data and knew little about how Chinese courts adjudicated patent cases. Instead, outside observers were left with a variety of impressions and had to guess how the courts adjudicates these cases based on the plain texts of the Chinese Patent Law and the limited number of cases released by the press. However, starting January 1, 2014, China mandated public access to all judgments via a database called China Judgements Online (CJO), making empirical studies possible. This Article analyzes all publicly available final patent infringement cases decided by local People's Courts in 2014. Surprisingly, findings in this Article contradict the long-standing beliefs held by many people about patent enforcement in China. One prominent example is that foreign patent holders were as likely as domestic patent holders to litigate and foreign patent holders received noticeably better results—specifically, higher win rates, injunction rates, and average damages. Another example is that plaintiffs won in 80.16% of all patent infringement cases and automatically got permanent injunctions in 90.25% of cases where courts found patent infringement. These new findings indicate that patent protection in China is stronger than once believed.

DOI: https://doi.org/10.15779/Z382J6846W

† Renjun Bian is a J.S.D. candidate at University of California Berkeley School of Law. She would like to thank Robert Merges for helpful suggestions that greatly improved the manuscript and Ning Zheng for technical support. She also would also like to thank Brian Wright, Rachel Stern, Lauren Edelman, Mark Lemley, Mark Cohen, Robert Berring, Kurtis MacFerrin, and her J.S.D colleagues for valuable discussions and comments.

TABLE OF CONTENTS

I. INTRODUCTION

The number of patent applications filed with and granted by the State Intellectual Property Office (SIPO) of the People's Republic of China has increased dramatically as a result of recent policies to stimulate domestic innovation.[1] The SIPO received more than 1.33 million filings for invention patents in 2016—a 21.5% increase from 2015—and, for the sixth consecutive year, SIPO received more patent applications than any other patent office worldwide.[2] Moreover, China is becoming a more important and attractive venue for foreign parties to pursue patent cases. A notable example was in 2016, when a subsidiary of WiLAN, a Canadian-based company, filed a lawsuit against Sony, a Japanese electronics company, in Nanjing, a city situated in east China, for alleged patent infringement.[3]

All these major developments in the Chinese patent system have made China an integral venue of international patent protection for foreign inventors and entrepreneurs. In order to protect their intellectual property rights in China more effectively, stakeholders and their lawyers are eager to know how Chinese courts adjudicate patent cases. Due to the lack of judicial transparency in China prior to 2014, there had been virtually no access to patent litigation data. Before 2014, all public knowledge about Chinese patent lawsuits was obtained from either interpreting the plain text of Chinese law and regulations, or analyzing a limited number of published cases that the Supreme People's Court (SPC) considered to have significant social impact. The limited amount of information may not have reflected an accurate landscape of patent litigation in China, which may have resulted in misleading impressions. For

1. *Patents, Yes; Ideas, Maybe*, ECONOMIST (Oct. 14, 2010), http://www.economist.com/node/17257940 [https://perma.cc/G4UB-9H2C] ("Anxious to promote domestic innovation, the Chinese government has created an ecosystem of incentives for its people to file patents. Professors who do so are more likely to win tenure. Workers and students who file patents are more likely to earn a *hukou* (residence permit) to live in a desirable city. For some patents the government pays cash bonuses; for others it covers the substantial cost of filing. Corporate income tax can be cut from 25% to 15% for firms that file many patents. They are also more likely to win lucrative government contracts. Many companies therefore offer incentives to their employees to come up with patentable ideas. Huawei, a telecoms-equipment manufacturer that craves both government contracts and global recognition, pays patent-related bonuses of 10,000-100,000 yuan ($1,500-15,000).").

2. Press Release, State Intellectual Prop. Office of China, The Statistical Data of the State Intellectual Prop. Office's Work in 2016 (Jan. 19, 2017), http://www.gov.cn/xinwen/2017-01/19/content_5161227.htm#1 [https://perma.cc/PN5L-B3YM].

3. *See* Juro Osawa, *China's Patent-Lawsuit Profile Grows*, WALL ST. J. (Nov. 7, 2016), www.wsj.com/articles/chinas-patent-lawsuit-profile-grows-1478535586 [https://perma.cc/EA4D-B93J] ("WiLAN's lawsuit is a rare case of a foreign patent-holding entity suing a non-Chinese company in China. It is an indication of how China is becoming a more attractive place to seek legal action for companies that accumulate patents for litigation and licensing purposes.").

example, there was an impression that Chinese courts had a strong bias toward domestic companies over foreign ones to protect the local economy; that injunctions, either preliminary or permanent, were difficult to obtain under Chinese law; that monetary damages granted by Chinese courts were extremely low and insufficient to compensate patent holders; etc.

This Article aims to evaluate these impressions by exploring a critical question: whether and how the outcome of patent infringement cases in China—the finding of infringement, the granting of injunctions, and the award of damages[4]—can be explained on the basis of observable legal and extra-legal factors. The increase in judicial transparency in China, including the explosion in the public availability of its judicial documents, has made answering this question through concrete empirical data, instead of hearsay, feasible for the first time. On July 1, 2013, the SPC launched China Judgements Online (CJO) and required that all judicial opinions issued on and after January 1, 2014, with a few exceptions, be uploaded to the website.[5] So far, the number of judgments and other judicial documents published on CJO has reached 50,658,073.[6] Although it is still far from complete,[7] an empirical study of this unprecedentedly large volume of judgments will provide many valuable inferences regarding how Chinese courts adjudicate patent infringement to inventors, practitioners, scholars, and anyone who is interested in China and its patent system.

The statistics presented in this Article tell only half of the story of how Chinese courts adjudicate patent cases, because this Article only examines

4. Unless otherwise specified, case outcome always indicates these three measures in this Article.

5. *See* Zuigao Renmin Fayuan Guanyu Renmin Fayuan zai Hulianwang Gongbu Caiban Wenshu de Guiding (最高人民法院关于人民法院在互联网公布裁判文书的规定) [Provisions of the Supreme People's Court on the Issuance of Judgments on the Internet by the People's Courts] (promulgated by the Sup. People's Ct., Nov. 21, 2013, effective Jan. 1, 2014), art. 4, CLI.3.213603(EN) [hereinafter ZUIGAO FAYUAN GUIDING] http://www.lawinfochina.com/display.aspx?id= 15918&lib=law [https://perma.cc/89CK-MVF6] ("An effective judicial document of a people's court should be issued on the Internet, except under any of the following circumstances: (1) It involves any state secret or individual privacy; (2) It involves any juvenile delinquency; (3) The case is closed by mediation; or (4) Any other circumstance under which it is inappropriate to issue the judgment on the Internet.").

6. *See* CHINA JUDGEMENTS ONLINE, http://wenshu.court.gov.cn [http://archive.is/Mzj5t] (last visited Aug. 15, 2018).

7. *See* Chao Ma, Xiaohong Yu & Haibo He, *Da Shuju Fenxi: Zhongguo Sifa Caipan Wenshu Shangwang Gongkai Baogao (大数据分析：中国司法裁判文书上网公开报告) [Data Analysis: Report on the Publication of Chinese Judicial Decisions on the Internet]*, 12 CHINA L. REV. 195, 208 (2016) (listing the ratios of the number of judicial documents of each province publicly available on CJO to the number of cases adjudicated in each province, ranging from 15.17% to 78.14%).

infringement litigation. China currently has a bifurcated patent litigation system, in which infringement and validity of a patent are brought in separate proceedings in different courts. Thus, the data presented in this Article depict an incomplete picture of patent enforcement in China and should always be viewed jointly with the information on patent validity cases.

Beyond the brief introduction Part I of this Article provides, Part II explores the contemporary knowledge in two existing academic bodies—the empirical study of patent litigation and the Chinese patent system. The literature review situates this Article at the intersection of these two areas, and demonstrates this Article's unique contribution to these bodies of literature. Part III explains the methodology used, defines the population studied in this article, and presents legal and extra-legal factors implicated in the study. It specifies the potential limitations and challenges of this Article, and the efforts to manage them. Part IV enumerates all findings in the form of detailed descriptive statistics. It also tests hypotheses regarding the relationship between the legal and extra-legal factors, as well as the final case outcome. Lastly, Part V summarizes the key findings from the descriptive and inferential statistics and reaches a conclusion on the question as to which factors really matter in the case of a Chinese court finding infringement, granting injunctions, and determining damages.

II. LITERATURE REVIEW

The research here focuses on producing empirical data to explore how courts adjudicate patent infringement cases in China. It builds on and contributes to two separate but theoretically overlapping bodies of academic scholarship: the empirical study of patent litigation and the Chinese patent system. This Part first summarizes the existing research in these two fields, then reviews an article that lies at the intersection of these two bodies of literature and is most relevant to the research presented here, and finally formulates a novel theoretical argument.

A. THE EMPIRICAL STUDIES OF PATENT LITIGATION

Over the past twenty to thirty years, a rapidly growing body of empirical data has been developed to study patent litigation in the United States. Based on their various goals, these studies can be divided into three different types: research to provide basic facts, research to lift the veil on adjudication, and research to answer normative questions. A detailed literature review of each type is presented below.

In the early years of this period, research studies were quite general and simple. Their goals were usually to develop basic information about what a court or a set of courts had done with regard to a particular issue. In his 1989

study, Ronald B. Coolley tried to establish what the Federal Circuit had done during the first six years of its existence by analyzing 322 judicial opinions.[8] His observations incorporated the number of opinions and dissents written by each judge, the number of judgments originally decided by each lower tribunal that were affirmed or reversed by the Federal Circuit, and the number of judgments involving different subjects of appeal that were affirmed or reversed by the Federal Circuit. In another article, Coolley conducted useful research focused on supplementing the well-understood legal theories behind damage awards by calculating the number, amount, and components of patent damages in 152 decisions.[9] Although this kind of pure counting work did not answer any specific normative questions, it assisted practitioners with making decisions regarding litigation and client counseling, and it benefited academic study by forming the foundation for more advanced empirical research in the future.

Subsequently, empirical studies became more sophisticated and question-focused. Some scholars began to use empirical techniques to explore how courts adjudicated cases, with a view to establishing what the relationship was between various identifiable factors and the final case outcome. John R. Allison and Mark A. Lemley examined how patents survived validity challenges.[10] They produced a database of 299 patents litigated in 239 lawsuits between 1989 and 1996 and used this database to develop descriptive statistics to test hypotheses. They proposed that patent validity may be influenced by factors such as the grounds for attacking validity, the finder of fact, subject matter of the invention, nationality of inventors, claim disaggregation, prior art citations, cited and uncited art, elapsed time, appeals, multiple patents in suit, and where the case is litigated.[11] Disappointingly, but not surprisingly, they found that only one factor—the finder of fact—displayed a significant predicative value to the final outcome.[12] Michael J. Mazzeo, Jonathan Hillel, and Samantha Zyontz undertook further important research to predict patent infringement awards.[13] They conducted a large-scale econometric analysis of award values, together with certain characteristics of litigants and patents at

8. *See* Ronald B. Coolley, *What the Federal Circuit Has Done and How Often: Statistical Study of the CAFC Patent Decisions - 1982 to 1988*, 71 J. PAT. & TRADEMARK OFF. SOC'Y 385, 385–86 (1989).

9. *See* Ronald B. Coolley, *Overview and Statistical Study of the Law on Patent Damages*, 75 J. PAT. & TRADEMARK OFF. SOC'Y 515, 515 (1993).

10. *See generally* John R. Allison & Mark A. Lemley, *Empirical Evidence on the Validity of Litigated Patents*, 26 AIPLA Q.J. 185 (1998).

11. *Id.* at 198–201.

12. *Id.* at 213.

13. *See* Michael J. Mazzeo, Jonathan Hillel & Samantha Zyontz, *Explaining The "Unpredictable": An Empirical Analysis of U.S. Patent Infringement Awards*, 35 INT'L REV. L. & ECON. 58 (2013).

issue, including identifiers,[14] dates,[15] location,[16] other case information,[17] general assignee,[18] NBER assignee,[19] assignee identifiers,[20] assignee patent identifiers,[21] SIC codes,[22] general patent,[23] and patent classification.[24] They

14. *Id.* at 65 (defining "identifiers" as "[v]ariables including a unique ID assigned by the authors, the docket number of the case, and the full names of the first listed plaintiff and defendant in the case").

15. *Id.* (defining "dates" as "[v]ariables including the year of the original award in district court, date the complaint for case was filed, the earliest start date of trial on validity, infringement, or damages, and the number of days between the trial start date and the complaint date").

16. *Id.* (defining "location" as "[v]ariables including where the case was litigated, including state, circuit, and court").

17. *Id.* (defining "other case information" as "[v]ariables determining if the case contained a summary judgment for the patent holder on validity and/or infringement, if the case involved an invalidated patent-at-issue, and if the patent holder was successful in its patent claims").

18. *Id.* (defining "general assignee" as "[i]nclud[ing] number of patent assignees associated with the patents-at-issue in the case, the names of the assignees, if one of the assignee(s) is the first named plaintiff or defendant in the case (can be both), if the plaintiff name listed is an assignee (patent holder), and if the patent holder markets or manufactures its technology covered by the patent").

19. *Id.* (defining "NBER assignee" as "[d]ummy variables from the 2002 NBER database which coded the Assignee(s) as 'Unassigned,' 'US, Non-Government,' 'Non-US, Non-Government,', 'US, Individual,' 'Non-US, Individual,' 'US Government,' or 'Non-US, Government'").

20. *Id.* (defining "assignee identifiers" as "[i]nclud[ing] the variables determining whether or not the first named plaintiff or defendant are an individual, private entity, public entity, university, part of the U.S. government, a domestic entity, foreign entity, part of the 2009 Fortune 500 list, part of the 2009 Fortune 1000 list, a subsidiary of a parent company").

21. *Id.* (defining "assignee patent identifiers" as "[v]ariables for the parent companies of the plaintiff or defendant listed if it was a subsidiary that include whether or not the parent company is a private entity, public entity, domestic entity, foreign entity, part of the 2009 Fortune 500 list, part of the 2009 Fortune 1000 list, if the first named plaintiff or defendant is owned by a joint venture (2 parents or more)").

22. *Id.* (defining "SIC codes" as "[v]ariables identifying the 2-, 3-, and 4- digit SIC codes for the potential infringers").

23. *Id.* (defining "general patent" as "[v]ariables identifying the number of patent(s) at issue in the case and their type as either utility, reissue, design, or application number").

24. *Id.* (defining "patent classification" as "[i]nclud[ing] variables for all patents-at-issue such as application year calculated for minimum and maximum (minimums and maxima differ for cases with multiple patents-at-issue and are the same for cases with only one patent-at-issue); grant date year calculated for minimum and maximum; grant date calculated for minimum and maximum; age of the oldest and youngest patent-at-issue in a case calculated for minimum and maximum; number of claims calculated for minimum, maximum, average and total; number of forward citations through 2002 from the NBER 2002 data, calculated for minimum, maximum and average; number of forward citations through 2010 if the 2002 forward citations were not available, calculated for minimum, maximum and average; the IPC4 classification listed first on the patent; and the PTO main classification for each patent listed in the case").

carried out this work based on 340 cases decided by federal courts from 1995 to 2008, and found that infringement awards were not unpredictable, as was commonly thought.[25] Instead, such awards could be predicted on the basis of several critical ex ante identifiable factors collectively.[26]

Other scholars addressed normative problems via comprehensive empirical studies. In 2013, Brian. J. Love conducted very interesting research to identify a way to destroy patent trolls without impairing actual inventors.[27] After analyzing the infringement claims of a group of recently expired patents, Love found product-producing companies and nonpracticing entities (NPEs) chose to enforce their patent rights at significantly different stages of infringement: producing companies usually commenced their enforcement activities soon after issuance and completed them in the middle of their patent term, while NPEs started relatively late and would not end enforcement until their patent expired.[28] Based on these findings, he then proposed that patent trolls could be eradicated by reducing patent terms.

No matter what particular category the aforementioned studies fall into, they are all tailored to the patent litigation system in the United States. The use of empirical data to analyze patent lawsuits in other jurisdictions, such as China,[29] could be regarded as untrodden territory. However, as China's patent system has become increasingly important to the whole international patent system, practitioners, scholars, and policymakers around the world are showing profound interest in whether and how courts in China protect patent rights. To fill this gap, this Article will follow the practice of producing empirical data—which U.S. scholars have used to reveal valuable insights about how courts adjudicate cases in the United States—to study patent litigation in China.

B. THE CHINESE PATENT SYSTEM

The language barrier and an unfamiliar legal system impede most U.S. scholars and lawyers in their attempts to learn and understand China's patent law and practice directly from Chinese documents. Therefore, research papers introducing the recent developments in patent law and regulations in China, as

25. *Id.* at 69.

26. *Id.*

27. *See generally* Brian J. Love, *An Empirical Study of Patent Litigation Timing: Could a Patent Term Reduction Decimate Trolls Without Harming Innovators?*, 161 U. PA. L. REV. 1309 (2013).

28. *Id.* at 1331.

29. There are only a few scholarly works analyzing patent litigation lawsuits using empirical data. *See, e.g.*, Brian J. Love, Christian Helmers & Markus Eberhardt, *Patent Litigation in China: Protecting Rights or the Local Economy?*, 18 VAND. J. ENT. & TECH. L. 713 (2016) (using five years of data, between 2006 and 2011, on patent suits litigated in Chinese intellectual property courts to analyze the patent system in China).

well as interesting Chinese cases, by authors with first-hand knowledge have been emerging to make Chinese patent law more accessible to English-speaking audiences. For example, soon after the revision of Patent Law of the People's Republic of China ("Patent Law of China") in 1992, David Hill and Judith Evans drafted a paper to illustrate the major changes adopted in this revision.[30] They concluded that the revision had strengthened patent rights in China and encouraged foreign patent holders to stimulate investment in China.[31] Xintian Yin undertook a similar analysis of how the patent system in China has been improved after the 1992 revision.[32] His work was distinguished from that of Hill and Evans by also addressing patent protection and the practice of patent application and examination in China.[33]

As basic knowledge of China's patent system increased, comparative research was conducted to compare and contrast specific patent policies in China to their counterparts in the western countries, such as the United States. In a 2013 article,[34] Timothy Lau explored the rationale for and against the prior art defense[35] based on the Chinese approach which ties the prior art defense to the doctrine of equivalents. He then suggested that the United States might benefit from introducing the prior art defense.[36] Other research, undertaken by Haitao Sun, compared the post-grant patent invalidation system in China with the relatively successful invalidation systems in the United States, the European Patent Convention, and Japan.[37] Sun found that the Chinese system closely resembled the others and predicted that Pfizer's case regarding its Chinese patent for Viagra might be fairly resolved in a Chinese court.[38]

The introductive and comparative research referred to above has enriched the knowledge of patent law in China for scholars who are not well-versed in

30. *See* David Hill & Judith Evans, *Chinese Patent Law: Recent Changes Align China More Closely with Modern International Practice*, 27 GEO. WASH. J. INT'L L. & ECON. 359 (1993–1994).

31. *Id.* at 392–93.

32. *See generally* Xintian Yin, *A Brief Introduction to the Patent Practice in China*, 9 DUKE J. COMP. & INT'L L. 253 (1998). Xintian Yin was the Deputy Principle Director of Administrative Department for Patent Examination at SIPO. His viewpoints on how much the patent system has been improved may be biased in light of his background.

33. *Id.* at 256–57.

34. *See* Timothy Lau, *Defensive Use of Prior Art to Exonerate Accused Act in U.S. and Chinese Patent Litigation*, 27 COLUM. J. ASIAN L. 51, 67–77 (2013).

35. The prior art defense is a defense to an assertion of patent infringement by arguing that the accused acts fall within the prior art. *See id.* at 55.

36. *Id.* at 78. ("We concluded that the United States would benefit from an introduction of the practicing the prior art defense, and that the Chinese linkage of the existing technology defense with equivalence is a well-calibrated approach.").

37. *See generally* Haitao Sun, *Post-Grant Patent Invalidation in China and in the United States, Europe, and Japan: A Comparative Study*, 15 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 273 (2004).

38. *Id.* at 330.

Mandarin Chinese. However, empirical study, as a helpful tool to supplement these widely studied legal theories, has rarely been applied. This Article aims to fill this gap by transplanting the empirical techniques used by U.S. scholars to answer how courts in China adjudicate patent infringement cases.

C. MOST RELEVANT RESEARCH

The research in this Article lies at the intersection of the two literature streams referred to above: the empirical study of patent litigation and the Chinese patent system. Although comparatively little research has been conducted in this area, it is not completely unexplored. There is, for example, an article co-authored by Brian J. Love, Christian Helmers, and Markus Eberhardt published in 2016 that evaluates the long-standing belief that patent litigation in China acts primarily to facilitate domestic industries at the expense of foreign firms.[39] After analyzing 471 patent suits in China, the authors found that Chinese patent litigation cases were frequently brought in several major urban areas instead of smaller inland cities where protectionism is alleged to occur. They also found that foreign companies often appeared as patent holders, rather than infringers, in Chinese patent lawsuits and had similar win rates to domestic Chinese companies. Their findings challenged the conventional belief of protectionism and suggested an opposite conclusion: China has created a system that benefits foreign interests at the expense of domestic ones.[40]

While the Love article provides new insights to this research, it has at least three clear drawbacks. First, the judgments it collected and analyzed—471 judicial opinions decided between 2006 and 2011—constitute only a small part of all patent litigation cases adjudicated in China and are rather out of date. Things have changed dramatically over the past six years. One prominent example is the increasing number of publicly available judicial opinions. Second, the article provided descriptive statistics only with regard to the cases it gathered, without making any predictions relating to the overall picture of patent litigation in China. This Article addresses these two problems by collecting a much larger number of written judgments, 1,663, decided in a more recent year, 2014, and using statistical testing to make predictions. Third, Love limited his research objectives to disputes over invention patents only. He did this on the basis of the legal convention that the term "patents" usually refers to invention patents.[41] However, the two other types of patents recognized by Chinese patent law, utility model patents and design patents, comprise a much larger part of patent infringement litigation in China than

39. *See* Love et al., *supra* note 29.
40. *Id.* at 739–40.
41. *Id.* at 714 n.1.

invention patents. This Article covers all three patent types and aims to achieve a more comprehensive understanding of patent litigation in China.

D. THEORETICAL ARGUMENT

The reason empirical research was rarely conducted when studying China's patent litigation is obvious: publicly available judgments in China, a prerequisite for producing empirical data, were scattered because the collection and publication of judicial opinions was not customary in China prior to 2014. However, with the ongoing judicial reform in China, this obstacle has to some extent been removed. In 2013, the SPC took a groundbreaking step in launching CJO, an online database gathering and providing existing judicial opinions. It then mandated public access, via this database, to all judgments made on and after January 1, 2014.[42] Although it will take some time for this policy to be fully implemented, approximately half of the cases which should be made public can now be found on CJO.[43]

The research for this Article aims to take advantage of this unprecedentedly enormous number of available judgments to explore a basic but crucial question: how Chinese courts adjudicate patent infringement cases. It provides two major categories of information: descriptive statistics relating to the 1,663 patent infringement cases collected from CJO, and an examination of how patent infringement cases in general, based on the superpopulation of the 1,663 cases gathered, are decided in China. Based on the existing empirical literature of patent lawsuits, this Article assembles various sets of data, including both dependent variables—case outcomes, and independent variables—factors that could potentially explain those outcomes. A list of variables that have been considered important by existing literature, as well as variables discussed in this Article, is presented below. Some variables that have been considered important by existing literature are excluded in this Article based on the reasons provided below.

42. *See* ZUIGAO FAYUAN GUIDING, *supra* note 5.
43. *See* Ma et al., *supra* note 7.

Table 1: Variables Not Covered in This Research

Variables	Sources	Reasons for Exclusion
Specific Judges	Coolley (1989)	Unlike Coolley's article, which studied a set of cases decided by a single court, this Article analyzes cases decided by all Chinese courts in 2014, meaning hundreds or even thousands of judges may be involved.
Subject of Appeal	Coolley (1989)	Since this Article only focuses on patent infringement cases, all appealed cases included in in the superpopulation have the same subject: finding of infringement.
Breakdown of Damages	Coolley (1993)	These data are missing for some judgments.
Finder of Facts	Allison (1998)	There is no jury system in China.
Multiple Claims	Allison (1998)	Though claim disaggregation may make a difference in validity cases, it does not affect infringement cases that much.
Prior Art Citations	Allison (1998)	Though prior art citations may make a difference in validity cases, they do not affect infringement cases that much.
Cited vs. Uncited Prior Art		Though whether to invalidate a patent on the basis of cited or uncited prior art may make a difference in validity cases, it does not affect infringement cases that much.
Multiple Patents in Suits	Allison (1998)	As a technical issue, Chinese courts usually draft multiple judgments, with different docket numbers for multiple patents brought in one infringement suit. Thus, this variable cannot be directly recognized from written judgments.

Table 2: Variables Covered in This Research

	Variables	Previous Research[44]
Dependent Variables	Ruling	Coolley (1989), Allison (1998), and Love (2016)
	Damages	Coolley (1993) and Love (2016)
	Injunctions	Love (2016)
Independent Variables	Subject Matters	Allison (1998), and Love (2016)
	Inventors	Allison (1998)
	Assignees	Love (2016)
	Elapsed Time	Allison (1998), and Love (2016)
	Appeals	Allison (1998) and Love (2016)
	Locations	Coolley (1989), Allison (1998), Love (2016)

This Article will contribute both to the existing empirical literature on patent litigation by focusing on a new and attractive jurisdiction, China, and to the current study of Chinese patent law system by adducing empirical insights. This Article aims to assist entrepreneurs and their lawyers to make better decisions when facing Chinese patent issues, as well as creating fertile ground for scholars around the world who are interested in the subject matter to conduct further empirical studies relating to patent litigation in China.

III. STUDY DESIGN

This Part is organized as follows: First, it breaks the methodology used in this Article into four major steps. Then, it defines the population studied in this article and presents legal and extra-legal factors implicated in the study. Finally, this Part specifies the potential limitations and challenges of this Article and the efforts to manage them.

A. METHODOLOGY

The methodology used in this Article involves four major steps. In Step I, I gather all the decisions included in the defined population from CJO and

44. This Figure uses the last name of first author and the year published to identify which article considered a certain variable important. Coolley, *supra* note 8; Coolley, *supra* note 9; Allison & Lemley, *supra* note 10; Love, *supra* note 27.

their corresponding patent files from SIPO's database. In Step II, I order the cases and variables to be studied by creating a data matrix and fill in the value for every case-variable combination. Incomplete cases, which are missing one or more variables, are not excluded from the data matrix in this step. However, they may have to be removed when presenting data, if such presentation requires a complete data matrix.

In Step III, I present the information in the data matrix by creating tables and graphs according to the levels of measurement to provide some basic ideas about how the 1,663 patent infringement cases included in the judgment pool were decided. In most cases, frequency tables are provided to illustrate how the values of a categorical variable, such as patent type, are distributed. For quantitative variables, such as elapsed time, I recode their values and build new ordinal categories.[45] These descriptive statistics may be reported one variable at a time. They may also be cross-tabulated in several different ways to emphasize certain interesting patterns.

In Step IV, I provide general predictions of how patent infringement cases are decided by Chinese courts. By taking the defined population as a subset of a superpopulation—all past and future final decisions of patent infringement cases in China—Step IV tests several hypotheses to evaluate the statistics produced in Step III. All hypotheses tested in this Article are in the null form, positing no relationship between a certain variable and a case's final outcome—the finding of infringement, the granting of injunctions, and the awarding of damages. If the p-value[46] is .05 or less,[47] then the hypothesis can be rejected with sufficient confidence, indicating that any relationships observed are statistically significant.

B. POPULATION

The population for this Article contains all final patent infringement cases decided by local people's courts in 2014 and publicly available on CJO. By including all cases within this definition, this Article constitutes a population

45. For example, to evaluate how elapsed time influences the final outcome of patent infringement cases in China, I recode quantitative time information collected into several intervals; that is, each piece of time information is arranged into one of two time intervals—"short" or "long"—based on whether it is shorter than the average time of its own category. Although some information may be lost in the recoding process, the process provides a better overview.

46. The p-value is a measure of the confidence with which a null hypothesis can be rejected.

47. This is called the significance level, i.e., how small the p-value needs to be to reject the null hypothesis. The most commonly used significance level is 0.05. *See, e.g.*, John R. Allison et al., *How Often Do Non-Practicing Entities Win Patent Suits?*, 32 BERKELEY TECH. L.J. 237, 259 nn.90–91 (2017).

study rather than a sample study.

1. Units of Observation

Data are collected and analyzed on a case-by-case basis. Here, a case is defined as a patent infringement lawsuit documented in one judicial opinion with a unique docket number and involved one disputed patent. Of all the cases downloaded from CJO, twenty-three did not comply with this definition, as they related to more than one docket number or disputed patent. Rather than attempting to divide cases by the included patent, this Article excludes these cases from the analyzed judgments.[48]

2. Source of Cases

There are several existing judicial databases in China. Theoretically, each could serve as the source of judgments for the purpose of this research. However, when taking authority, transparency, and accessibility into consideration, CJO stands out. Below is a table comparing and contrasting CJO to two major Chinese databases: CIELA[49] and IPHouse:[50]

Table 3: Comparison of Databases

	CJO	**IPHouse**	**CIELA**
Owner	SPC	Private Company	Law Firm
Number of Judgments[51]	Available	Not Available	Available
Accessible Judgments[52]	All	Top 300	None

48. For cases with multiple patents at issue, the hardest part of breaking up those opinions is to divide damages. Taking Lianyi Dianzi (Huizhou) Youxian Gongsi, Shenzhen Shiyuan Chuangshidai Keji Youxian Gongsi (联毅电子（惠州）有限公司诉深圳市元创时代科技有限公司) [Lianyi Electronics, Ltd. v. Shenzhen Shiyuan Chuangshidai Tech. Ltd.], CHINA JUDGMENT ONLINE (Shenzhen Interm. People's Ct. June. 14, 2014) as an example, four different patents were involved, while only the total damages were given. For cases with multiple docket numbers, the hardest part is assigning defendants. For example, Tang Yongzhu, Guilin Hongcheng Kuangshan Shebei Zhizao Youxian Zeren Gongsi (唐永竹诉桂林鸿程矿山设备制造有限责任公司) [Tang v. Guilin Hongcheng Kuangshan Equip. Mfg.], CHINA JUDGMENT ONLINE (Shandong Higher People's Ct. July. 16, 2014) was brought against two defendants and have multiple docket numbers. There is no way to establish whether both of them were sued in all three cases.

49. CIELA is the database that other scholars, such as Professor Love, have used when drafting empirical work on Chinese patent litigation. *See* Love et al., *supra* note 29, at 723.

50. IPHouse is a commercial database providing statistics on IP-related litigation in China. *See* IPHOUSE, http://en.iphouse.cn/ [https://perma.cc/B2FC-A86U] (last visited Sept. 26, 2018).

51. When an advanced search is conducted, this variable indicates whether the database provides the number of judgments found.

52. When an advanced search is conducted, this variable indicates how many judgments are accessible to the general public.

As the only database created and operated by the SPC, CJO collects judicial documents directly from all levels of People's Courts, making it more authoritative than commercial databases, which gather documents indirectly from other databases. Meanwhile, CJO shows a higher level of transparency and accessibility in its search function compared to IPHouse and CIELA. When an advanced search is executed, CJO provides both the number of judgments found and the full text of every single document satisfying the criteria. In contrast, IPHouse keeps the number of results found secret and displays only the first 300 judgments that satisfy the criteria. CIELA is a little different; it provides charts and tables of different characteristics of a group of cases and does not provide access to the texts of judgments.

3. Patent Infringement Cases

My research focuses on patent infringement cases decided by Chinese courts. Administrative appeals—whether resulting from the rejection of patent applications by SIPO, from patent validity decisions made by the Patent Reexamination Board of SIPO, or from administrative decisions concerning patent infringement actions made by local intellectual property offices—are beyond the scope of this Article. Nor are cases asking for non-infringement confirmation of others' patent rights or declaratory judgments included. This is not to say that administrative appeals and non-infringement confirmation cases are less valuable than infringement cases. Rather, they are so numerous that a separate, independent research project should be conducted. Expanding the current research to include these types of cases would render it too broad, and important details could be missed.

4. Final Decisions

"Final decisions" here refer to at least two things. First, only cases finally adjudicated by a court are included. Cases settled before a final judgment are not considered due to the lack of publicly available records. Second, with regard to cases not appealed, their first instance judgments are taken as their final decisions, whereas a second judgment following an appeal prevails.

It should be noted that in this Article, all first instance judgments whose second instance decisions cannot be found on CJO are regarded as not appealed. This definition may raise several problems (see Section III.D), but it seems to be the only choice with no available alternatives. Meanwhile, all second instance judgments downloaded directly from CJO are deemed to be final decisions.[53] Since second instance decisions usually summarize an inferior

53. *See* Minshi Susong Fa (民事诉讼法) [Law on Civil Procedure] (promulgated by the Standing Comm. Nat'l People's Cong., April 9, 1991), art. 175 ("The judgments and rulings of

court's opinion in the first instance trial, it is not necessary to collect information from related first instance judgments—at least for the purpose of this Article.

5. Cases Decided by Local People's Courts

Since cases decided by the SPC have been widely examined before and are better studied on a case-by-case basis, this Article focuses only on cases decided by local People's Courts. As most cases are solved at the lower court level, I believe that cases decided by local courts are as important as, if not more important than, cases adjudicated by the SPC. "Local People's Courts" here refer to the first three levels of courts in China's four-level court system: (1) Basic-level People's Courts (at the level of counties and municipal districts), (2) Intermediate People's Courts (at the level of cities), (3) Higher People's Courts (at the level of the provinces), and (4) the Supreme People's Court (at the highest level of the court system whose cases this Article will not address).[54]

6. Date Range

In order to achieve the highest level of inclusiveness, the time range of the cases analyzed is limited to the year 2014. In accordance with the SPC's decision, only cases decided after the date when the decision came into force—January 1, 2014—are mandated to be published on CJO.[55] The vast majority of judgments in 2013 and preceding years were not reported since Chinese courts had no tradition of disclosing their decisions on a regular basis.[56] Meanwhile, it takes two years for courts of every level to upload their judicial opinions.[57] Thus when the judgments were collected for the purpose of this research in 2016, it was reasonable to infer that only cases decided in 2014 would be completely published.

Studying cases decided in one calendar year also makes it possible to observe trends across time. By conducting further research on cases adjudicated in subsequent years and comparing the data to the statistics produced in this Article, many interesting and important questions may be answered, such as whether patent protection in China has been strengthened over time, or whether foreign patent holders are more willing to enforce their

a people's court of second instance shall be final.").

54. As may be surmised, the fourth level of court in China is the Supreme People's Court in Beijing.

55. *See supra* note 5.

56. *See* Ma et al., *supra* note 7, at 207 fig.5 (showing that the number of judicial opinions available on CJO consistently increased from 2001 to 2013, then jumped from 2013 to 2014).

57. *See id.* at 224 tbl.31 (showing that 92.73% of decisions were uploaded within a year of being made; 7.18% of decisions were uploaded after a year but within two years of being made).

rights in China as legal transparency is growing.

C. DATA COLLECTED

For every single case included in the population defined above, this Article collects information both legal and extra-legal variables, which can be categorized into three major types. The first type includes the dependent variables this Article tries to explain: infringement found, injunctions granted, and damages awarded. The second type represents independent variables that comprise several potentially explanatory factors that can be used to explain a court's decisions in patent infringement lawsuits. The third type contains data that have nothing to do with the explanatory relationship, but are technically indispensable.

Table 4: Variables Covered in This Research

Variables	Explanation	Notes
Dependent Variables		
Infringement	Whether there was a finding of infringement by the court.	Always explicitly stated in the judgments.
Injunctions	Whether there was an injunction granted by the court after infringement was found.	This variable is limited to permanent injunctions, since whether a preliminary injunction was granted cannot be determined from a written judgment.
Damages	Whether damages were awarded by the court after infringement was found and in what amount.	Includes compensation for infringement and compensation for reasonable expenses paid by patent holder, such as attorney fees, to stop infringement activities.
Independent Variables/Explanatory Factors		
Subject Matter	To which International Patent Classification class the litigated invention patent or utility model belongs; To which Locarno Classification class the litigated design patent belongs.	Identified by the International Patent Classification number[58] or Locarno Classification number[59] listed on patent files.
Patent Types	Whether the patent concerned is an invention patent, utility model, or design patent.[60]	Always explicitly stated in the patent files.

58. *See International Patent Classification (IPC)*, WORLD INTELLECTUAL PROP. ORG., http://www.wipo.int/classifications/ipc/ipcpub [https://perma.cc/M8TK-ZNCK] (last visited Aug. 17, 2018).

59. *See Locarno Classification*, WORLD INTELLECTUAL PROP. ORG., http://www.wipo.int/classifications/locarno/locpub [https://perma.cc/VB5A-A6T5] (last visited Aug. 17, 2018).

60. There are three types of patents available in China: invention patent, utility model, and design patent. *See infra* note 84.

Residency of the Plaintiff	Whether the plaintiff resides in mainland China or in a foreign country.	The addresses of plaintiffs who are patentees of the patent concerned are always recorded in the patent files; The addresses of plaintiffs who are assignees of the patent concerned can be found in the assignment record in SIPO's database.
Elapsed Time	How long the patent concerned spent in each phase, including the length of time it spent in prosecution, the length of time elapsed between issuance and the final court decision, and the overall time from filing to final decision.	The dates of filing and issuance of the patent concerned are listed in patent files. The date of the final decision by the court can be discerned from the judgment. Calculations are needed.
Jurisdiction	In which province the case was litigated.	Can be identified directly from the final judgments.
Other Variables		
Identifier	The docket number of the case.	Starts with a four-digit number indicating the year, and ends with a Chinese character Hao ("number"). Usually appears at the beginning of a judicial opinion right under the title Min Shi Pan Jue Shu ("civil judgment").

D. LIMITATIONS

This project involves several major limitations and challenges. This Section demonstrates what those potential limitations might be and how they are managed in the course of this research.

1. Population Biases

Perhaps the most controversial part of this Article's study design is its definition of the population. Ideally, to answer the questions of whether and how legal and extra-legal factors influence the final outcomes in Chinese patent lawsuits, the population should be defined as all patent infringement cases ever adjudicated by local People's Courts in China. However, this is not feasible due to the huge numbers of missing judicial documents from cases adjudicated in China before 2014 and the post-2014 judicial reform, which has yet to fully achieve its goal.[61]

Another population bias may be introduced by limiting the population to final decisions. If there is no second instance judgment of a case from CJO, this study assumes the case was never appealed and includes its first instance judgment in the judgment pool as its final decision. However, this may not be the case when missing documents are taken into account. There might be certain appealed cases for which no second instance documents are publicly available and whose first instance results are wrongfully treated as final results. Nevertheless, based on the affirmance and reversal data illustrated in Table 35, the appellate courts affirmed lower courts' verdicts in a significant portion (85.03%) of second instance cases. Therefore, it might be reasonable to conclude that the missing documents will not bring strong bias to this research.

2. Inherent Limitations

The variables this Article tests are limited to legal and extra-legal factors that can be identified in written judgments and patent files. However, there might be other variables that cannot be observed directly from such printed documents yet affect the final case outcome. An obvious example is the numerous characteristics of people involved in a case, including but not limited to the competence of each party's lawyers and the personal background and experience of judges. This does not imply that the study design of this research project is problematic, however. It simply means that further research is needed to tell the whole story of how Chinese courts adjudicate patent infringement.

Meanwhile, making predictions about the superpopulation based on the previously defined population rests on the assumption that all conditions remain the same and will continue to be the same. This is not always the case. Science and technology are developing extremely rapidly, as are people's perceptions and social norms. Laws and regulations, while they always take time to respond, are changing over time as well. This research project, by its very nature, cannot reflect these important changes when making predictions

61. *See* Ma et al., *supra* note 7.

of how patent infringement cases are generally decided in China. However, the goal of this research is not to provide exact predictions regarding what happened in a certain historical period or what will happen in the future. I merely aim to offer some basic material on the basis of which people can make their own, more accurate, predictions when taking these changes into consideration.

Finally, some people might question the subjectivity problem inherent in coding. When converting written judgments into hard numbers by reading and analyzing natural language, personal judgments are often involved, which might cause bias. I adopt at least three different strategies to reduce this risk. First, I code by myself without hiring any outside coders, which raises no inter-coder reliability issue. Second, I code the judgments by writing a computer program and generating patterns to scrape the data, which diminishes personal inconsistency that might occur with time. Third, I use concrete rules, especially existing rules, to delimit different subcategories. For example, I use the International Patent Classification number shown on patent documents, rather than subjective judgments, to characterize litigated patents into different subject matter areas.

At minimum, this Article is a statistical analysis report on patent infringement cases currently available on CJO. All the descriptive statistics can serve as a great aid for those who are trying to get a deeper understanding of patent litigation in China.

IV. OBSERVATIONS

This Part presents the information in the data matrix by discussing how various factors influence the outcome of patent infringement cases in China. It also tests several interesting hypotheses to identify potential explanatory variables of infringement, injunctions, and damages.

A. DEPENDENT VARIABLE I—INFRINGEMENT

Of the 1,663 cases included in the population, infringement was found in 1,333 (80.16%) decisions by the court and non-infringement was found in 330 (19.84%) decisions. Table 5 below lists the detailed results:

Table 5: Infringement

	Total	No. Infringed	No. Not Infringed
Total	1,663 (100%)	1,333 (80.16%)	330 (19.84%)
1st Instance	1,055 (100%)	856 (81.14%)	199 (18.86%)
2nd Instance	608 (100%)	477 (78.45%)	131 (21.55%)

For the 1,055 cases whose first instance judgments were included in the judgment pool as their final decision, infringement was found in 856 (81.14%) decisions and non-infringement was found in 199 (18.86%) decisions. For the 608 second instance judgments included, infringement was found in 477 (78.45%) decisions and non-infringement was found in 131 (21.55%) decisions.[62] These startlingly high win rates[63] might be the result of the gradual maturity of China's judicial patent enforcement system. That is, when such system was weak in the past, patent holders refrained from pursuing litigation. Thus, a great amount of high quality patents piled up and were not litigated until the patent enforcement system in China matured to some extent. Another possible explanation is that the parties err significantly in estimating case outcome due to the long history of lack of judicial transparency in China. According to the Priest-Klein hypothesis, plaintiff victories will eventually converge to 50% as both party's error in estimating the outcome diminishes.[64] If this proves to be the case,[65] plaintiff win rates after 2014 should drop as entrepreneurs' and lawyers' experience with patent infringement litigation in China accumulates.

62. These similar win rates among first and second instance cases indicate that the potentially missing second instance judgments may not cause significant biases, at least for this variable.

63. "Plaintiff win" here is defined as cases terminated with infringement found for at least one claim. Plaintiff win rates in China were higher than those in many major countries. For example, from 2006 to 2012, the average plaintiff win rates in first instance patent infringement litigations in Germany, another bifurcated country, was sixty-six percent. The win rate for unified patent lawsuits in the United States was sixty percent. *See* BLOOMBERG BNA, ANNUAL GLOBAL PATENT LITIGATION REPORT 2014 (2015), https://www.darts-ip.com/newsletter/201508/AnnualGlobalPatentLitigationReport2014.pdf [https://perma.cc/QN3P-ZXXA]. It should be emphasized that this Article focuses on final written judgments only. In other words, cases in which actions were dismissed by plaintiffs are not included due to the lack of publicly available records. Based on the White Paper released by China's Supreme Court, more than seventy percent of intellectual property cases filed in China in 2014 were ended by voluntary dismissal. *See* WORLD INTELLECTUAL PROP. ORG., WHITE PAPER ON THE STATUS OF THE JUDICIAL PROTECTION OF INTELLECTUAL PROPERTY RIGHTS IN CHINESE COURTS IN 2014 (2015), http://www.wipo.int/wipolex/en/details.jsp?id=15689 [https://perma.cc/4XE8-FT2N].

64. *See* George L. Priest & Benjamin Klein, *The Selection of Disputes for Litigation*, 13 J. LEGAL STUD. 1, 18–22 (1984).

65. *See generally* Jason Rantanen, *Why Priest-Klein Cannot Apply to Individual Issues in Patent Cases* (Univ. Iowa Legal Studies Research Paper No. 12–15, 2012), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2132810 [https://perma.cc/5PH7-2WBE] (criticizing the application of the Priest-Klein hypothesis to individual issues in patent law).

B. DEPENDENT VARIABLE II—INJUNCTIONS

According to relevant articles in the General Principles of the Civil Law of the People's Republic of China ("General Principles")[66] and Tort Law of the People's Republic of China ("Tort Law"),[67] together with practical observations, the remedies granted by Chinese courts in patent infringement cases can be divided into three major categories: injunctions, damages, and other remedies, including destroying infringing products and apologies.

Injunctions are often considered as falling into two categories: preliminary and permanent. However, preliminary injunctions, a powerful weapon in patent infringement litigation which sometimes leads to early resolution, are excluded from this Article for two reasons. First, whether a preliminary injunction was granted cannot be inferred from written final judgments. Second, preliminary injunctions are rarely requested and granted in patent infringement lawsuits in China.[68] Therefore, the term "injunctions" in this article refers to permanent injunctions unless otherwise specified.

Among the 1,333 decisions in which infringement was found by courts, injunctions were granted in 1,203 (90.25%) cases. For the 856 first instance final decisions included, courts granted injunctions in 766 (89.49%) cases. For the 477 second instance decisions included, courts granted injunctions in 437 (91.61%) cases.

---

66. *See* Minfa Tongze (民法通则) [The General Principles of Civil Law] (promulgated by the Standing Comm. Nat'l People's Cong., April 12, 1986, effective Jan. 1, 1987), art. 118 ("If the rights of authorship (copyrights), patent rights, rights to exclusive use of trademarks, rights of discovery, rights of invention or rights for scientific and technological research achievements of citizens or legal persons are infringed upon by such means as plagiarism, alteration or imitation, they shall have the right to demand that the infringement be stopped, its ill effects be eliminated and the damages be compensated for"); *Id.* at art. 134 ("The main methods of bearing civil liability shall be: (1) cessation of Infringements; (2) removal of obstacles; (3) elimination of dangers; (4) return of property; (5) restoration of original condition; (6) repair, reworking or replacement; (7) compensation for losses; (8) payment of Breach of Contract damages; (9) elimination of ill effects and rehabilitation of reputation; and (10) extension of apology . . .").

67. *See* Qinquan Zeren Fa (侵权责任法) [Tort Law] (promulgated by the Standing Comm. Nat'l People's Cong., Dec. 26, 2009, effective July 1, 2010), art. 15 ("The methods of assuming tort liabilities shall include: (1) cessation of infringement; (2) removal of obstruction; (3) elimination of danger; (4) return of property; (5) restoration to the original status; (6) compensation for losses; (7) apology; and (8) elimination of consequences and restoration of reputation . . . .").

68. *See* Benjamin Bai, *Preliminary Injunctions in China: The Pendulum Has Swung Back!*, KLUWER PAT. BLOG (Apr. 30, 2014), http://kluwerpatentblog.com/2014/04/30/preliminary-injunctions-in-china-the-pendulum-has-swung-back [https://perma.cc/MFN6-S5P5] (arguing "most IP suits in China do not involve an application for a PI" by providing a snapshot of PI statistics for 2010–2013).

Table 6: Injunctions Granted[69]

	Total	No. Injunctions	No. Non-Injunctions
Total	1,333	1,203 (90.25%)	130 (9.75%)
First Instance	856	766 (89.49%)	90 (10.51%)
Second Instance	477	437 (91.61%)	40 (8.39%)

According to relevant articles in General Principles,[70] and Tort Law,[71] and the statistical observations above, injunctions are automatically granted in most cases based on a finding of infringement in China. Unlike in the United States, where plaintiffs have to prove that the issue satisfies a four-factor test,[72] plaintiff-brought patent infringement cases in China merely have to demonstrate infringement in order to receive a permanent injunction. Table 7 below illustrates why injunctions were not granted in 130 cases.

69. Only cases in which infringement was found by courts are included.

70. *See* Minfa Tongze, *supra* note 66, art. 118 ("If the rights of authorship (copyrights), patent rights, rights to exclusive use of trademarks, rights of discovery, rights of invention or rights for scientific and technological research achievements of citizens or legal persons are infringed upon by such means as plagiarism, alteration or imitation, they shall have the right to demand that the infringement be stopped, its ill effects be eliminated and the damages be compensated for.").

71. *See* Qinquan Zeren Fa, *supra* note 67, art. 15 ("The methods of assuming tort liabilities shall include: (1) cessation of infringement; (2) removal of obstruction; (3) elimination of danger; (4) return of property; (5) restoration to the original status; (6) compensation for losses; (7) apology; and (8) elimination of consequences and restoration of reputation . . . .").

72. eBay Inc. v. MercExchange, L.L.C., 547 U.S. 388, 392 (2006) (holding that after a finding of patent infringement, an injunction should not be automatically granted, and the plaintiff bears the responsibility of demonstrating that their suit satisfies the four-factor test to receive an injunction).

Table 7: Reasons for Not Granting Injunctions

Rank	Reason	No. Cases	Percentage
1	Not Requested by Plaintiff	50	38.46%
2	Patent Expired	38	29.23%
3	Equity & Public Interest	20	15.38%
4	Not Mentioned	9	6.92%
5	Infringing Activities Stopped	5	3.85%
5	Already Issued by Previous Procedure	5	3.85%
7	Wrongly Drafted	2[73]	1.54%
8	Patentee Changed	1	0.77%

The two most common reasons explaining why the court did not grant an injunction were that an injunction was not requested by the plaintiffs (38.46%) and that the asserted patent had expired at the time of adjudication (29.23%). Such expiration can result from the patent term's natural termination or non-payment of maintenance fees. Therefore, when considering cases where plaintiffs request injunctions and the patents at issue are not expired, the rate of injunctions granted are higher, at 96.85%. This reveals that under Chinese law, permanent injunctions are given in almost all cases of infringement.

Courts sometimes refused to grant injunctions due to equity and public interest considerations (15.38% of non-injunctions). Most cases in this category involved an infringing product that was a part of a building or other construction. Because dismantling the infringing product might lead to safety issues and waste of resources, courts usually ordered royalties instead of injunctions in such cases. Courts also rejected requests for injunctions when infringing activities had stopped (3.85%) or when previous judicial or administrative procedures had already offered such remedies (3.85%). For nine judgments in which no discussion of injunctions was offered (6.92%) and the two judgments which display discrepancies with regard to reasoning and conclusion, the reason that injunctions were not granted cannot be discerned.

73. In these two cases, courts mentioned that injunctions should be granted in the reasoning section, but did not say anything about injunctions in the decision part. *See* Lelingshi Meiyitian Shipin Youxian Gongsi, Lelingshi Huachang Tiaowei Shipin Youxian Gongsi (乐陵市美亿天食品有限公司诉乐陵市华畅调味食品有限公司) [Leling Meiyitian Foods Ltd. v. Leling Huachang Flavored Foods Ltd.], CHINA JUDGMENT ONLINE (Jinan Interm. People's Ct. Nov. 24, 2014), Luoyang Yixing Shihua Dianqi Yibiao Shebei Youxian Gongsi, Xinxiangshi Shengda Guolv Jinghua Jishu Youxian Gongsi (洛阳毅兴石化电器仪表设备有限公司诉新乡市胜达过滤净化技术有限公司) [Luoyang Yixing Petrochemical Elec. Appliance & Instrumentation Co. v. Xinxiang Shengda Filtration Technique Co.] CHINA JUDGMENT ONLINE (Henan Higher People's Ct. July 23, 2014).

C. DEPENDENT VARIABLES III—DAMAGES

In addition to injunctions, damages are another major remedy for infringement provided by Chinese patent law. In the 1,333 decisions in which infringement was found by courts, damages were awarded in 1,281 (96.17%) cases. For the 856 first instance final decisions included, damages were awarded in 820 (95.79%) cases. For the 477 second instance decisions included, damages were awarded in 462 (96.85%) cases.

Table 8. Damages Awarded[74]

	Total	Damages Awarded	Damages not Awarded
Total	1,333	1,282 (96.17%)	51 (3.83%)
First Instance	856	820 (95.79%)	36 (4.21%)
Second Instance	477	462 (96.86%)	15 (3.14%)

When compared to the rates of injunctions granted, 90.25% for all cases in which infringement was found, and 93.76% for those excluding the cases in which the plaintiffs did not request a permanent injunction, damages appear to be an even more frequently granted remedy by Chinese courts. The table below sets out the reasons that plaintiffs were not awarded damages in the other 51 (3.83%) cases.

Table 9. Reasons for Not Awarding Damages[75]

Rank	Reason	No. Cases	Rate
1	Infringing products were obtained from a legitimate source.	42	82.35%
2	Damages were already awarded in a previous procedure.	5	9.80%
3	The plaintiff did not request damages.	4	7.84%
4	The infringers did not acquire profits from their infringing activity.	2	3.92%
5	The plaintiff could not prove infringing activities.	1	1.96%

74. Only cases with a finding of infringement are included.

75. The sum of the percentages in Table 9 exceeds 100% because three cases are double counted due to more than one reasons for not awarding damages involved.

Unlike the diverse reasons given for not granting injunctions, the courts' explanations for awarding no damages after infringement was found were more concentrated.[76] The large majority of decisions with no damages awarded (82.35%) were because defendants raised the "legitimate source" defense successfully. In terms of Article 70 of the Patent Law of China, a defendant shall not be liable for damages if the defendant obtained the infringing products from a legitimate source, without knowing that such products were infringing products.[77]

Table 10 below reports the mean and median of all damages awarded to first and second instance cases respectively.[78]

Table 10: Damages Awarded[79]

	No. Cases	Mean	Median
All	1,281[80]	￥75,853.83 ($12,354.04)	￥30,000.00 ($4,885.99)
First Instance	819[81]	￥52,596.07 ($8,566.14)	￥22,000.00 ($3,583.06)
Second Instance	462	￥117,329.04 ($19,108.96)	￥50,000.00 ($8,143.32)

76. The concentration here might be a result of the smaller number of cases (51 for damages versus 130 for injunctions).

77. *See* Zhuanli Fa (专利法) [Law on Patent] (promulgated by the Standing Comm. Nat'l People's Cong., Dec. 27, 2008, effective Oct. 1, 2009), art. 70 ("Where any person, for the purpose of production and business operation, uses, offers to sell or sells a patent-infringing product without knowing that such product is produced and sold without permission of the patentee, he shall not be liable for compensation provided that the legitimate source of the product can be proved.").

78. As many decisions did not distinguish between compensation for infringement and reasonable expenses, damages in this Article are defined as including both compensation for infringement and reasonable expenses.

79. Only cases in which damages were awarded by courts are included. All damages awarded in Chinese yuan (CNY) are changed into U.S. dollars (USD) based on the average exchange rate (1.00 USD to 6.14 CNY) in the year of 2014. *See China Statistical Yearbook 2015*, NAT'L BUREAU OF STATISTICS OF CHINA, http://www.stats.gov.cn/tjsj/ndsj/2015/indexeh.htm [https://perma.cc/9ERP-SAFY] (last visited Sept. 29, 2017).

80. An outlier case has been removed from the calculation for exceedingly low damage award (8 CNY). *See* Cao Liantao v. Shi Bin (曹连涛诉石滨), CHINA JUDGMENT ONLINE (Shandong Province Jinan Interm. People's Ct. Sept. 26, 2014). Besides that, all damages awarded were above 1,000CNY.

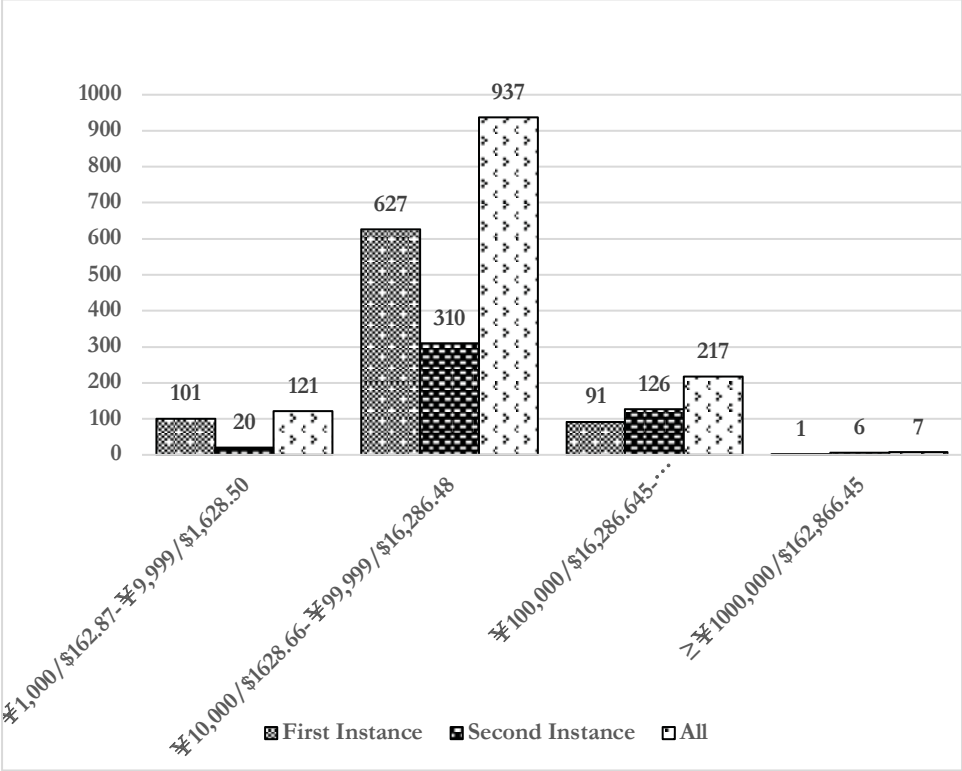
81. *See id.*

The average damages awarded to plaintiffs by the Chinese courts was ¥ 75,853.83 (approximately US$12,354.04). The median was even lower, at approximately ¥ 30,000.00 (US$4,885.99). Though second instance courts tended to award higher damages than first instance courts,[82] the above figures confirmed the commonly held view that damages awarded by the Chinese courts are frustratingly low. According to statistics released by PricewaterhouseCoopers, the median damages awarded in 2014 by the U.S. courts—although the second-lowest figure in 20 years—was US$2.0 million, which is hundreds of times larger than the median damages awarded by the Chinese courts.[83] Figure 1 below summarizes the distribution of the damages awarded by the Chinese courts.

82. One potential explanation is that only cases with significant damages are worth appealing.

83. *See* PRICEWATERHOUSECOOPERS, 2015 PATENT LITIGATION STUDY: A CHANGE IN PATENTEE FORTUNES 4 (2015), https://www.pwc.com/us/en/forensic-services/publications/assets/2015-pwc-patent-litigation-study.pdf [https://perma.cc/M8D2-48VK].

Figure 1: Range of Damages Awarded by Chinese Courts



Damages awarded in most cases (937, or 73.09%) fell in the range of between ￥10,000 (approximately US$1,628.66) and ￥99,999 (approximately US$16,286.48). While there were some decisions (217, or 16.93%) with higher damages of between ￥100,000 (approximately US$16,286.64) and ￥999,999 (approximately US$162,866.29), the Chinese courts awarded damages in excess of ￥1 million in only seven cases (0.55%). For the sake of interest, these seven cases are listed in Table 11 below.

Table 11: Cases with Damages in Excess of ￥1 Million

Rank	Plaintiff	Defendant	Damages
1	Keihin Thermal Tech. Corp.	FAW-Valeo Climate Control Sys. Co. Ltd., et al.	￥4.84M ($0.79M)
2	Hunan CHINASUN pharm. Mach. Co., Ltd.	Shandong Xinhua Med. Apparatus and Instruments Co., Ltd., et al.	￥2.05M ($0.34M)
3	Buluke (Chengdu) Eng'g Co., Ltd.	Hengshui Qijia Eng'g Materials Co., Ltd., et al.	￥2M ($0.33M)
4	ZTE Corp.	Huawei Tech. Co., Ltd., et al.	￥1M ($0.16M)
4	Hangzhou Grascent Co., Ltd.	Hangzhou Youbang Flavors & Fragrances Co., Ltd., et al.	￥1M ($0.16M)
4	ZTE Corp.	Huawei Tech. Co., Ltd., et al.	￥1M ($0.16M)
4	Huawei Tech. Co., Ltd.	ZTE Corp., et al.	￥1M ($0.16M)

D. INDEPENDENT/EXPLANATORY FACTOR I—PATENT TYPES

The Chinese patent law provides protection for three distinct types of patents: invention patents, utility model patents, and design patents.[84] Invention patents[85] and design patents[86] in China are respectively comparable to utility patents and design patents in the United States. Utility model patents ("utility models"), while sounding similar to utility patents, are totally different from the latter. Chinese patent law defines "utility models" as "new technical solutions proposed for the shape and structure of a product"[87]—these are commonly known as "petty patents" and are more similar to the European or Japanese style utility patents.

84. *See* Zhuanli Fa (专利法) [Law on Patent] (promulgated by the Standing Comm. Nat'l People's Cong., Dec. 27, 2008, effective Oct. 1, 2009) art. 2 ("For the purposes of this Law, invention-creations mean inventions, utility models and designs.").

85. *Id.* ("Inventions mean new technical solutions proposed for a product, a process or the improvement thereof.").

86. *Id.* ("Designs mean, with respect to a product, new designs of the shape, pattern, or the combination thereof, or the combination of the color with shape and pattern, which are rich in an aesthetic appeal and are fit for industrial application.").

87. *Id.* ("Utility models mean new technical solutions proposed for the shape and structure of a product, or the combination thereof, which are fit for practical use.").

The vast majority of the 1,660 cases included in the population (1,022, or 61.57%) were design patents. The second most common type of patents involved were utility models (420, or 25.30%). Cases relating to invention patents constituted only a very small proportion (218, or 13.13%). Meanwhile, first and second instance cases did not share a similar patent type distribution. The percentage of design patents involved in second instance cases, (48.27%), was notably smaller than in first instance cases (69.23%). By contrast, the proportions of utility models and invention patents involved in second instance cases (34.10% and 17.63%, respectively) were much larger than those involved in first instance cases (20.23% and 10.54%, respectively). These figures may to some extent reflect that utility model and invention patent cases have higher appeal rates than design patent cases do.[88]

88. Again, this discrepancy of case distribution by patent types may be caused by potentially missing judgments.

Table 12: Patent Types

	Total	Invention Patents	Utility Models	Design Patents
Total	1,660[89]	218 (13.13%)	420 (25.30%)	1,022 (61.57%)
First Instance	1,053[90]	111 (10.54%)	213 (20.23%)	729 (69.23%)
Second Instance	607[91]	107 (17.63%)	207 (34.10%)	293 (48.27%)

As illustrated in Figure 2 below, the comparison between the above data and the distribution of patents in force was quite illuminating.[92] Surprisingly, the largest category of litigated patents, design patents (61.57% of all litigated patents), constituted only 24.87% of the patents in force by the end of 2014. Conversely, invention patents and utility models accounted for a much larger portion of patents in force than litigated patents. One possible explanation for these differences might be that design patent owners are more likely to enforce their issued patents than the owners of invention patents and utility models. Alternatively, these differences may imply that less infringement occurs for the other two types of patents than design patents because they are easier to design

89. Only 1,660 cases are used in this Section. *See infra* notes 94, 95.

90. Only 1,053 cases are included. Two cases are excluded because the title of the patents and the number assigned to the applications do not match. *See* Guangdong Aofei Dongman Wenhua Gufen Youxian Gongsi, Qingzhen Jiahui Chaoshi Youxian Zeren Gongsi (广东奥飞动漫文化股份有限公司诉清镇佳惠超市有限责任公司) [Alpha Grp. v. Qingzhen Jiahui Market LLC] CHINA JUDGMENT ONLINE (Guiyang Interm. People's Ct. Nov. 14, 2014) and Guangdong Aofei Dongman Wenhua Gufen Youxian Gongsi, Wang Liangming (广东奥飞动漫文化股份有限公司诉王亮明) [Alpha Grp. v. Wang] CHINA JUDGMENT ONLINE (Guiyang Interm. People's Ct. Nov. 11, 2014) are excluded since the title of the patents and the number assigned to the applications do not match.

91. Only 807 cases are counted in this part. Zhangzhoushi Dongqing Jinshu Zhipin Youxian Gongsi, Xiamen Wansheng Wujin Zhipin Youxian Gongsi (漳州市东庆金属制品有限公司诉厦门万晟五金制品有限公司) [Zhangzhou Dongqing Metal Prod. Ltd. v. Xiamen Wansheng Hardware Co.] CHINA JUDGMENT ONLINE (Gujian Higher People's Ct. Dec. 20, 2014) is excluded since based on the information revealed in the opinion, the patent at issue cannot be found in SIPO's database.

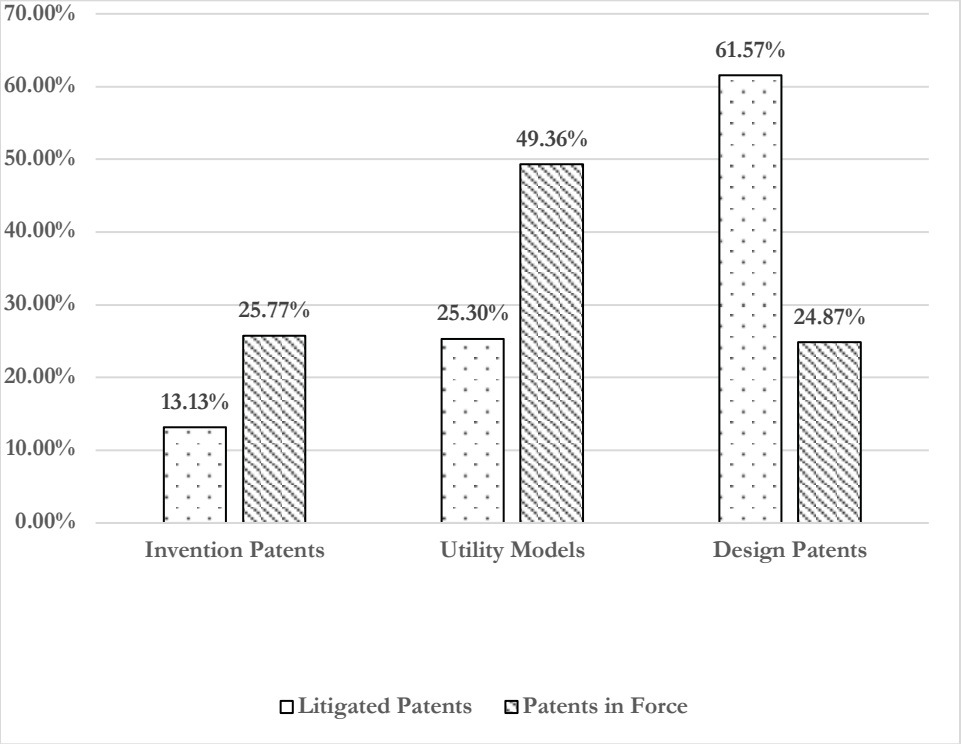
92. The number and percentage of patents of each type in force by the end of 2014 are listed below:

Patents in Force, by Patent Types			
Total	Invention Patents	Utility Models	Design Patents
4,642,506	1,196,497 (25.77%)	2,291,326 (49.36%)	1,154,683 (24.87%)

See STATE INTELLECTUAL PROP. OFF., GUONEIWAI SANZHONG ZHUANLI YOUXIAO ZHUANGKUANG (国内外三种专利有效状况) [DISTRIBUTION OF PATENTS IN FORCE FOR THREE KINDS RECEIVED FROM HOME AND ABROAD] (2015), http://www.sipo.gov.cn/tjxx/jianbao/year2014/c/c1.html [https://perma.cc/J6FU-577C].

around.

Figure 2: Percent of Patents Litigated and In Force by Patent Type



In an attempt to examine how different types of patents fared in patent infringement litigation in China, this study collects data on the number and the percentage of cases where infringement was found, an injunction was granted, and the amount of damages awarded by patent type, as summarized below:

Table 13. Cases Where Infringement Was Found, by Patent Type[93]

Patent Type	All Cases	Winning Cases	Percentage
Invention Patents	218	157	72.02%
Utility Models	420	325	77.38%
Design Patents	1,022	848	82.97%

Table 14. Injunctions Granted in Winning Cases, by Patent Type[94]

Patent Type	Winning Cases	Injunctions	Percentage
Invention Patents	157	148	94.27%
Utility Models	325	275	84.62%
Design Patents	848	779	91.86%

The likelihood of the Chinese courts finding infringement and granting injunctions displayed notable differences between patent types. For both first and second instance cases, the win rates on infringement were between 71% and 84% respectively, with invention patents having the lowest infringement rate (72.02%) and design patents the highest (82.97%). This discrepancy indicates that cases involving invention patents are more challenging and

93. A breakdown of win rates across different instances of trial is presented below:

Win rates on Infringement, by Patent Type II						
Patent Type	1st Instance			2nd Instance		
	All Cases	Winning Cases	%	All Cases	Winning Cases	%
Invention Patents	111	81	72.97%	107	76	71.03%
Utility Models	213	169	79.34%	207	156	75.36%
Design Patents	729	604	82.85%	293	244	83.28%

94. A breakdown of injunction rates across different instances of trail is presented below:

Injunctions in Winning Cases, by Patent Type II						
Patent Type	1st Instance			2nd Instance		
	Winning Cases	Injunctions	%	Winning Cases	Injunctions	%
Invention Patents	81	75	92.59%	76	73	96.05%
Utility Models	169	145	85.80%	156	130	83.33%
Design Patents	604	546	90.40%	244	233	95.49%

unpredictable for both parties than those of utility models and design patents, due to the complex technologies patented. Meanwhile, the rates of granting injunctions after infringement was found fell between 83% and 97%, with invention patents and design patents both having high injunction rates above 90%, and utility models having a slightly lower injunction rate of approximately 84%.

Table 15. Damages, by Patent Type[95]

Patent Types	Mean	Median	Minimum	Maximum
Invention Patents	￥259,154.64 ($42,207.60)	￥120,000.00 ($19,543.97)	￥6,000.00 ($977.20)	￥4,840,000.00 ($788,273.62)
Utility Models	￥83,620.94 ($13,619.05)	￥50,000.00 ($8,143.32)	￥1,000.00 ($162.87)	￥670,000.00 ($109,120.52)
Design Patents	￥39,167.20 ($6,379.02)	￥30,000.00 ($4,885.99)	￥1,000.00 ($162.87)	￥900,000.00 ($146,579.80)

The amounts of damages awarded by the Chinese courts differed significantly based on patent type. Invention patent holders enjoyed the highest amount of average damages (￥259,154.64, or US$42,207.60), which was approximately three times higher than the average damages awarded to utility model holders and seven times higher than those awarded to design patent holders. These numbers confirm the conventional wisdom that the value of an invention patent is generally higher than the value of the other two types of patents due to a higher inventiveness requirement[96] and a mandate

95. Only cases in which damages were awarded by courts are included.

96. *See* Zhuanli Fa (专利法) [Law on Patent] art. 22, § 3. ("Creativity means that, compared with the existing technologies, the invention possesses prominent substantive features and indicates remarkable advancements, and the utility model possesses substantive features and indicates advancements."); *id.* at art. 23, § 2 ("Designs for which the patent right is to be granted shall be ones which are distinctly different from the existing designs or the combinations of the features of existing designs.").

substantive examination,[97] which warrants a longer protection term.[98]

To make predictions about the superpopulation, this Article tests the following hypotheses:

Hypothesis I-A: There is no difference between the likelihood that infringement will be found by a Chinese court in patent infringement cases involving an invention patent, a utility model, and a design patent. (Rejected)

Hypothesis I-B: There is no difference between the likelihood that injunctions will be granted after infringement is found by a Chinese court in patent infringement cases involving an invention patent, a utility model, and a design patent. (Rejected)

Hypothesis I-C: There is no difference between the average amount of damages awarded by a Chinese court in patent infringement cases involving an invention patent, a utility model, and a design patent. (Rejected)

The G-square p-values[99] for the above three tests were .0004, .0003, and .0000 [100] respectively—all smaller than .001. [101] The results of patent infringement cases in China can therefore be predicted with great confidence[102]

97. *See id.* at art. 35 ("Within three years from the date an invention patent application is filed, the patent administration department under the State Council may, upon request made by the applicant at any time, carry out substantive examination of the application. If the applicant, without legitimate reasons, fails to request substantive examination at the expiration of the time limit, such application shall be deemed to have been withdrawn. The patent administration department under the State Council may carry out substantive examination of its own accord, as it deems it necessary."); *id.* at art. 39 ("If no reason for rejection is discerned after an invention patent application is substantively examined, the patent administration department under the State Council shall make a decision on granting of the invention patent right, issue an invention patent certificate, and meanwhile register and announce the same. The invention patent right shall become effective as of the date of announcement."); *id.* at art. 40 ("If no reason for rejection is discerned after preliminary examination of a utility model or design patent application, the patent administration department under the State Council shall make a decision on granting of the utility model or design patent right, issue a corresponding patent certificate, and meanwhile register and announce the same. The utility model patent right and the design patent right shall become effective as of the date of announcement.").

98. *See id.* at art. 42. ("The duration of the invention patent right shall be 20 years and that of the utility model patent right and of the design patent right shall be 10 years respectively, all commencing from the date of application.").

99. I test the hypotheses using both G-square p-values (the "likelihood-ratio statistic") and chi-square p-values (the "Pearson statistic"). While I report the results of both in Appendix A, for brevity, I refer to G-square p-values in the Observation part. They provide approximately the same results.

100. To make the numbers shorter and simpler, I round all decimals to the nearest ten-thousandth when calculating p-values.

101. This indicates that we can reject each null hypothesis with 99.999% confidence.

102. The choice of significance level at which the hypothesis can be rejected is arbitrary.

based on the type of patents litigated. That is, owners of invention patents are less likely to win than owners of utility models and design patents when they bring a patent infringement lawsuit to a Chinese court. Owners of invention patents are also more likely to get injunctions and higher damages after infringement is found.

E. INDEPENDENT/EXPLANATORY FACTOR II—SUBJECT MATTER

Since different classification standards apply when classifying invention patents, utility models, and design patents, based on the technologies involved, this study divides the 1,660 cases included in the population into two data sets and measure the patents litigated in each data set by subject matter separately.[103]

1. Subject Matter of Invention Patents and Utility Models

The data set to be studied in this Section covers 218 cases of invention patents and 420 cases of utility models. For each case included, the International Patent Classification (IPC) number from each patent file was discerned, and then the case was assigned to one of three mutually exclusive subject matter areas—mechanical (or "general"), electrical, and chemical—based on my own evaluation of the IPC-Subject Matter concordance. If more than one IPC number was identified in a patent, only the main IPC number was considered. The classification results are summarized in Table 16 below.

Conventionally, statisticians treat $p < 0.05$ as indicating statistical significance, and $p < 0.001$ as indicating high statistical significance.

103. *See supra* note 92. Only cases whose disputed patents can be clearly identified and found in SIPO's database are included.

Table 16: Patent Subject Matter

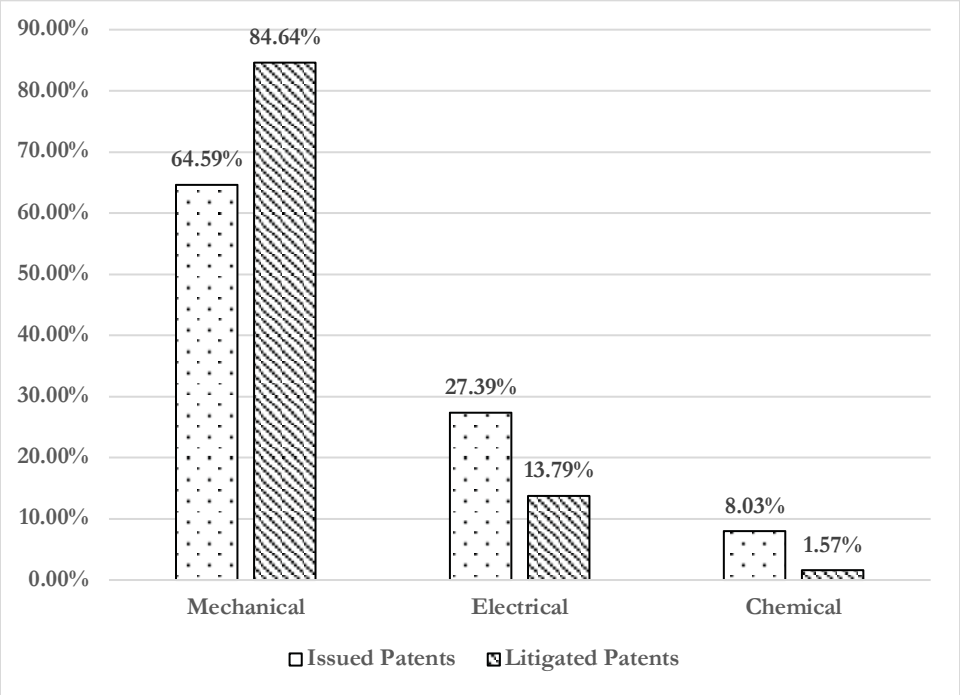
Subject Matter	Number and Percentage of Cases	IPC Class	Number and Percentage of Cases
Mechanical (General)	540 (84.64%)	A. Human Necessities	143 (22.41%)
		B. Performing Operations	135 (21.16%)
		D. Textiles	23 (3.61%)
		E. Fixed Constructions	133 (20.85%)
		F. Mechanical Engineering	106 (16.61%)
Electrical	88 (13.79%)	G. Physics	31 (4.86%)
		H. Electricity	57 (8.93%)
Chemical	10 (1.57%)	C. Chemistry	10 (1.57%)

It is surprising to find that the overwhelming majority of decisions involved mechanical patents (540, or 84.64%). Whereas electrical (88, or 13.79%) and chemical (10, or 1.57%) patents, which provide protection for leading-edge technologies, such as biotechnologies, pharmaceuticals, and software-related inventions, made up a rather small portion of patent infringement lawsuits. These counterintuitive observations may be explained by several potential reasons.

First, the number of electrical and chemical patents issued might only make up a small portion of all patents issued,[104] which is consistent with the following graph that contrasts the percentage of patents litigated with the percentage of patents issued in each subject matter area. Though electrical and chemical patents accounted for a higher percentage of issued patents than of litigated cases, they constituted a significantly smaller portion of all patents issued in 2014, when compared to mechanical patents.

104. Though it might make more sense to compare litigated patents to all patents in force in 2014, no such statistics are publicly available. The best alternative data available relate to the number of invention patents and utility models of each IPC class issued in 2014.

Figure 3: Issued Patents vs. Litigated Patents by Subject Matter



Second, the counterintuitive phenomenon referred to above may be caused by the dynamic nature of electrical and chemical technologies. Rapid development and iteration might cause patents in these leading-edge fields to lose value before their protection terms expire. On one hand, because there is certainly no incentive for patent holders to pay maintenance fees for worthless patents, the number and percentage of patents in force in these two areas could drop significantly over time. Therefore, that could account for the low number and percentage of patent litigation in these subject matter areas. On the other hand, due to time concerns, companies holding electrical and chemical patents might prefer settling disputes to litigating in courts. Time-consuming litigation could block their development process and lead to significant losses.

Third, the huge amount of attention paid to electrical and chemical patents may have less to do with the number of cases litigated than with the value these patents represent. Table 17 below summarizes the patent types of litigated patents by subject matter areas. It indicates that the percentage of invention patents litigated in electrical and chemical cases was much higher than in mechanical cases and demonstrates that cases in leading-edge fields frequently involved higher value patents than normal cases.

Table 17: Patent Types, by Subject Matter

Subject Matter	No. of Cases	No. and Percentage of Cases involving Invention Patents	No. and Percentage of Cases involving Utility Models
Mechanical	540	169 (31.30%)	371 (68.70%)
Electrical	88	41 (46.59%)	47 (53.41%)
Chemical	10	8 (80.00%)	2 (20.00%)

Turning to the comparison between the final outcomes of cases in different subject matter areas, summarized in Table 18, all three measures—win rates, injunction rates, and average damages—were fairly constant for mechanical and electrical cases. Chemical cases, however, had a significantly lower win rate (50.00%) and a slightly lower injunction rate (80.00%). Chemical patent holders also received noticeably higher average damages (￥239,000.00, or US$38,925.08) than mechanical (￥137,338.00, or US$22,367.75) and electrical (￥165,457.56, or US$26,947.49) patent holders, which might provide additional evidence in favor of the third explanation above—that patents belonging to leading-edge fields receive greater attention because they are more valuable than general patents. However, since the number of cases in the chemical field was so small, no robust conclusions should be drawn from the difference identified.

Table 18: Case Results, by Subject Matter

Subject Matter	No. Cases	Infringed	Injunctions	Avg. Damages
Mechanical	540	408 (75.56%)	357 (87.50%)	￥137,338.00 ($22,367.75)
Electrical	88	69 (78.42%)	62 (89.86%)	￥165,457.56 ($26,947.49)
Chemical	10	5 (50.00%)	4 (80.00%)	￥239,000.00 ($38,925.08)

The differences observed above are not statistically significant. That is, none of the hypotheses below can be rejected with confidence:

Hypothesis II-A: There is no difference between the likelihood that infringement will be found by a Chinese court in patent infringement cases involving a mechanical patent, an electrical patent, and a chemical patent. (Not Rejected)

Hypothesis II-B: There is no difference between the likelihood that injunctions will be granted after infringement is found by a Chinese court in patent infringement cases involving a mechanical patent, an electrical patent, and a chemical patent. (Not Rejected)

Hypothesis II-C: There is no difference between the average amount of damages awarded by a Chinese court to patent infringement cases involving a mechanical patent, an electrical patent, and a chemical patent. (Not Rejected)

Therefore, although inventors, companies, practitioners, and scholars have been devoting much attention to patents in certain subject matter areas, no statistical evidence can be found regarding the relationship between the subject matter and the outcome of infringement cases.

2. Subject Matter of Design Patents

This study also examines whether and how different subject matter areas of design patents influence the final outcomes of infringement lawsuits in China. The data set studied in this Section includes 1,022 design patent cases. Every case is categorized into one of 32 Locarno Classification ("LOC") classes based on the LOC number listed in each file. The win rates, injunction rates for cases where infringement was found, and average damages were then calculated for each LOC class. Table 19 below summarizes these categorization and calculation results.

Table 19: Design Patents, by Subject Matter[105]

LOC Classes	No. Cases	% Infringed	% Injunctions	Avg. Damages
2. Articles of Clothing and Haberdashery	17	88.24%	100.00%	￥37,978.57
3. Travel Goods, Cases, Parasols and Personal Belongings, not Elsewhere Specified	7	85.71%	100.00%	￥29,333.33
4. Brushware	3	66.67%	100.00%	￥35,000.00
5. Textile Piecegoods, Artificial and Natural Sheet Material	53	92.45%	100.00%	￥18,777.14
6. Furnishing	100	83.00%	100.00%	￥45,790.71
7. Household Goods, not Elsewhere Specified	51	70.59%	100.00%	￥50,934.29
8. Tools and Hardware	83	85.54%	98.59%	￥38,033.01
9. Packages and Containers for the Transport or Handling of Goods	98	81.63%	95.00%	￥23,086.02
10. Clocks and Watches and Other Measuring Instruments, Checking and Signaling Instruments	37	56.76%	95.24%	￥58,850.00
11. Articles of Adornment	21	66.67%	100.00%	￥20,000.00
12. Means of Transport or Hoisting	24	91.67%	86.36%	￥95,000.00
13. Equipment for Production, Distribution or Transformation of Electricity	26	73.08%	100.00%	￥45,000.00
14. Recording, Communication or Information Retrieval Equipment	64	85.94%	92.73%	￥47,878.76

105. Only the LOC classes with at least one categorized case are included.

15. Machines, not Elsewhere Specified	20	55.00%	72.73%	¥46,795.45
16. Photographic, Cinematographic and Optical Apparatus	10	90.00%	44.44%	¥36,114.29
19. Stationery and Office Equipment, Artists' and Teaching Materials	14	78.57%	100.00%	¥31,636.36
20. Sales and Advertising Equipment, Signs	9	100.00%	100.00%	¥57,833.33
21. Games, Toys, Tents and Sports Goods	147	95.24%	70.71%	¥19,584.32
23. Fluid Distribution Equipment, Sanitary, Heating, Ventilation and Air-Conditioning Equipment, Solid Fuel	75	78.67%	96.61%	¥49,144.07
24. Medical and Laboratory Equipment	1	0.00%	NA	NA
25. Building Units and Construction Elements	46	78.26%	91.67%	¥58,075.43
26. Lighting Apparatus	97	84.54%	97.56%	¥50,170.56
27. Tobacco and Smokers' Supplies	3	100.00%	100.00%	¥30,000.00
28. Pharmaceutical and Cosmetic Products, Toilet Articles and Apparatus	9	88.89%	100.00%	¥41,000.00
31. Machines and Appliances for Preparing Food or Drink, not Elsewhere Specified	7	100.00%	100.00%	¥49,674.00

It is difficult to distinguish general patterns from the above table. Design patents in patent infringement lawsuits covered 25 of the 32 LOC classes,[106]

106. The LOC classes with no categorized cases are the following: Class 1—Foodstuffs; Class 17—Musical instruments; Class 18—Printing and office machinery; Class 22—Arms, pyrotechnic articles, articles for hunting, fishing, and pest killing; Class 29—Devices and

indicating that the Chinese IP system has been very good at protecting a diverse array of subject matters. Since the number of cases categorized into each LOC class is relatively small, no robust conclusion should be drawn from the above data regarding the relationship between different subject matter areas and the final case outcomes. Therefore, no hypotheses are tested in this Section because the results would be unreliable.

F. INDEPENDENT/EXPLANATORY FACTOR III—FOREIGN VS. DOMESTIC PLAINTIFFS

The Chinese judicial system has gained international notoriety for its local protectionism and lack of impartiality. Many in the West believe that the patent system established in China serves primarily to facilitate domestic industry at the expense of foreign companies. For example, a European patent attorney, Andreas Bieberbach, wrote that Chinese patent law was continuously adjusted to benefit Chinese companies since its establishment in 1984. [107] PricewaterhouseCoopers, in its report, *China Strategy: Refining yours could open new doors*, also pointed out that actions taken by the Chinese government to bring in intellectual property as a new incentive scheme to promote the development of certain industries and regions "have inevitably heightened Western concern about Chinese protectionism, regulatory discrimination, and continued infringement of IP rights."[108]

In an effort to evaluate this widely held belief, this Article produces statistics to test the following two assumptions: (1) foreign patent holders are less likely to litigate in China than domestic patent holders; (2) foreign patent holders often receive worse results during such litigation. This Article breaks down 1,663 decisions in the data set into two categories, "foreign" and "domestic," based on the residency of the plaintiff.[109] If a case contains more than one plaintiff, it is labeled as "foreign" as long as one of the plaintiffs resides outside mainland China. Table 20 below indicates how many patents are litigated by residency of the plaintiff.

---

equipment against fire hazards, for accident prevention and for rescue; Class 30—Articles for the care and handling of animals; and Class 32—Graphic symbols and logos, surface patterns, ornamentation. *See supra* note 60.

107. *See* Andreas Bieberbach, *IP Strategies in Business Operations with China*, 9 J. BUS. CHEMISTRY 161, 161 (2012).

108. PRICEWATERHOUSECOOPERS, CHINA STRATEGY: REFINING YOURS COULD OPEN NEW DOORS 6 (2011), http://www.pwc.com/us/en/private-company -services/publications/ assets/gyb-63-china-strategies.pdf [https://perma.cc/KY6D-69YZ].

109. Plaintiffs residing in Hong Kong, Macao and Taiwan are categorized as "foreign" due to different jurisdictions.

Table 20: Residency of Plaintiff

	No. Domestic P.	Percentage	No. Foreign P.	Percentage
Total	1,548	93.08%	115	6.92%
1st Instance	990	93.84%	65	6.16%
2nd Instance	558	91.78%	50	8.22%

Not surprisingly, the overwhelming majority of patent infringement cases in China (1,548, or 93.08%) were litigated by domestic patent owners or licensees. Foreign plaintiffs accounted for only 115 (6.92%) of 1,663 decisions included in the population.[110] This percentage—although seems low—represents the ratio of patents granted by SIPO to international patent applicants. According to statistics released by SIPO, 93,285 patents were issued to foreign individuals and entities in 2014, making up approximately 7.16% of all 1,302,687 patents granted by SIPO that year.[111] This consistency indicates that foreign patent holders are as likely to enforce their patents in the Chinese courts as domestic patent owners, clearly rejecting the first assumption stated to above.

For the sake of interest, this study also examined how frequently foreign and domestic patent owners litigate different types of patents. It was found that foreign patent holders litigated far more frequently in cases involving invention patents than in cases involving utility models and design patents. Approximately 28.44% of invention patent cases in the data set were brought by foreign owners, while the figures for utility models and design patents were only slightly above 3%. This discrepancy may be attributed to the fact that foreign inventors often overlook utility models and design patents when seeking patent protection in China.[112] However, these two types of patents,

110. The percentage could be even higher when taking into consideration the possibility that some foreign patentees might disguise their foreign identity by introducing their lawsuit under the name of their Chinese subsidiaries. *See* Tansa Tugong Hecheng Cailiao (Zhongguo) Youxian Gongsi Su Sanmingshi Shuili Shuidian Gongcheng Youxian Gongsi (坦萨土工合成材料（中国）有限公司诉三明市水利水电工程有限公司) [Tansa Tugong Hecheng Material (China) Ltd. v. Sanming Water Conservancy and Water Power Engineering Ltd.] CHINA JUDGMENT ONLINE (Fuzhou Interm. People's Ct., Apr. 30, 2014). The plaintiff, Tansa Tugong Hecheng Material (China) Limited Company, a company located in China, is owned by a British company, Tensar Group Limited.

111. *See supra* note 95. This percentage is much lower than the percentage of patents in force held by foreigners. According to SIPO's data, 610,144 (13.14%) patents were held by foreigners among all 4,642,506 patents in force by the end of 2014. But this inconsistency may be caused by the lag that part of these valid patents may be litigated in the future.

112. The percentage of invention patents granted to international applicants is much

especially utility models, offer excellent opportunities for potential patentees to gain faster patent protection[113] and to reduce filing costs.[114] Foreign inventors should give more attention to these types of patents when building their Chinese patent strategies.

Table 21: Patent Type, by Residency of Plaintiff

	No. Domestic P.	Percentage	No. Foreign P.	Percentage
Total	1,545	93.07%[115]	115	6.93%[116]
Invention Patents	156	71.56%	62	28.44%
Utility Models	406	96.67%	14	3.33%
Design Patents	983	96.18%	39	3.82%

Cases brought by domestic and foreign plaintiffs are also broken down into different subject matter areas. As illustrated in Table 22, cases litigated by foreign patentees constituted a higher percentage of leading-edge technologies, electrical and chemical patents, than cases litigated by their domestic

higher than the percentage of utility models and design patents granted, as illustrated below:

Annual Patent Issuance to Foreign Applicants, by Patent Type

Year	Invention Patents	Utility Models	Design Patents
1985-2009	330,276 (56.30%)	11,425 (0.83%)	96,981 (8.60%)
2010	55,343 (40.96%)	2,216 (0.64%)	16,646 (4.97%)
2011	59,766 (34.72%)	3,024 (0.74%)	13,862 (3.65%)
2012	73,258 (33.74%)	4,425 (0.77%)	14,229 (3.05%)
2013	64,153 (30.89%)	6,637 (0.96%)	13,797 (3.34%)
2014	70,548 (30.25%)	7,912 (1.12%)	14,825 (4.10%)

See supra note 92.

113. Utility models and design patents require preliminary examination only and are often granted much more rapidly than invention patents. *See* CHINA IPR SME HELPDESK, GUIDE TO PATENT PROTECTION IN CHINA (2013), http://www.china- iprhelpdesk.eu/sites/ all /docs/publications/China_IPR_Guide-Guide_to_Patent_Protection_in_China_EN -2013.pdf [https://perma.cc/TZ8F-WATR].

114. Patent applicants must pay both an application fee (￥900, or US$146.58) and an examination fee (￥2,500, or US$407.17) for invention patent applications. However, for utility model and design patent applications, applicants pay only an application fee (￥500, or US$81.43). *Schedule of Fees*, STATE INTELLECTUAL PROP. OFF. (Dec. 30, 2005), http://english.sipo.gov.cn/application/howtopct/200804/t20080416_380500.html [https://perma.cc/Z4VF-TQEW].

115. The percentage of cases whose plaintiffs reside in China in Table 20 is slightly different from the figure listed in the above Table 21 because only 1,660 cases are counted in this part. *See supra* note 92.

116. *See id.*

counterparts.

Table 22: Subject Matter, by Residency of Plaintiff

	Total	Mechanical Patents	Electrical Patents	Chemical Patents
Total	638	540 (84.64%)	88 (13.79%)	10 (1.57%)
Domestic P.[117]	562	480 (85.41%)	75 (13.35%)	7 (1.25%)
Foreign P.[118]	76	60 (78.95%)	13 (17.11%)	3 (3.95%)

To test the second assumption referred to above—that foreign patent holders often receive worse results due to the local protectionism prevalent in the Chinese judicial system—data were collected on the outcomes of litigation brought by foreign and domestic plaintiffs.

Table 23: Case Results, by Residency of Plaintiff

	Decisions	Infringed	Injunction	Avg. Damages
Total	1,663 (100%)	1,333 (80.16%)	1,203 (90.25%)	¥75,942.39 ($12,368.47)[119]
Foreign P.	115 (6.92%)	97 (84.35%)	90 (92.78%)	¥201,620.45 ($32,837.21)
Domestic P.	1,548 (93.08%)	1,236 (79.84%)	1,113 (90.05%)	¥66,217.93 ($10,784.68)[120]

The comparison between the case outcomes generally received by foreign and domestic plaintiffs was illuminating. Contrary to widely held beliefs, foreign plaintiffs were more likely to have infringement found and injunctions granted than their Chinese counterparts in patent infringement cases brought in China. Moreover, damages awarded to foreign patent owners (¥201,620.45, or US$32,837.21) were almost three times higher than those awarded to the Chinese patent owners (¥66,217.93, or US$10,784.68). These striking results provided a credible explanation as to why foreign patentees did not fear enforcing their patent rights in China—the conventional wisdom notwithstanding. The important implication here is that the Chinese courts, while not preferring foreign parties to domestic ones, certainly did not protect

117. These percentages add to 100.01% due to rounding.
118. *See id.*
119. *See supra* note 80 & 81.
120. *Id.*

the local economy at the expense of foreign companies in practice.[121]

The predictive significance of the above data for the superpopulation was uneven. When conducting hypothesis testing, there was no statistically significant difference between the likelihood of having infringement found (G-square p-value = .2836) and injunctions granted (G-square p-value = .4725) for domestic and foreign plaintiffs. Therefore, the following two hypotheses could not be rejected.

Hypothesis III-A: There is no difference between the likelihood that infringement will be found by a Chinese court in a patent infringement case brought by a domestic patentee or licensee, and a patent infringement case brought by a foreign patentee or licensee. (Not Rejected)

Hypothesis III-B: There is no difference between the likelihood that injunctions will be granted after infringement is found by a Chinese court in a patent infringement case brought by a domestic patentee or licensee, and a patent infringement case brought by a foreign patentee or licensee. (Not Rejected)

However, for damages awarded to domestic and foreign plaintiffs, the following hypothesis was rejected with great confidence (G-square p-value = .0000):

Hypothesis III-C: There is no difference between the damages awarded to a domestic patentee or licensee and the damages awarded to a foreign patentee or licensee by a court in a patent infringement case in China. (Rejected)

G. INDEPENDENT/EXPLANATORY FACTOR IV—ELAPSED TIME

In this Section, the extent to which time elapsed between the patent application and the final judgment influences patent infringement cases in the Chinese courts is tested. The measures tested include "prosecution length," "patent age from date of issuance," and "patent age from date of application." "Prosecution length" is defined as the time elapsed from the filing of a patent application to the date of issuance. "Patent age from date of issuance" and "patent age from date of filing," as the terms suggest, are defined as the time

121. Another possible reason for the better results obtained by foreign patentees might be that foreign patentees were very cautious about litigating in China. They litigated only when there was a rather high probability of their winning. It is also possible that there is some protection of the local economy where the SIPO holds international patents to a higher standard.

elapsed from the date of issuance and filing respectively to the date when the court made a decision.[122] "Patent age from date of filing" is simply the sum of "prosecution time" and "patent age from date of issuance." Table 24 below presents the mean and median of these three measures for cases involving different types of patents.

Table 24: Prosecution Length (in Years), by Patent Types

	Mean	Median
Invention Patents	3.50	3.105[123]
Utility Models	0.91	0.90
Design Patents	0.66	0.60

122. A more precise definition of "patent age from date of issuance" would be the total time elapsed between the date a patent was issued and the date a patent infringement lawsuit was filed. However, since the filing details are missing for a significant number of decisions, it is not practical to apply this definition. Instead, I use the date of decision, which is always explicitly written in the judgments, as the last day to calculate patent age.

123. The value here and several values below are rounded to three decimal points because when there is an even number of results, the median is calculated by determining the mean of the two central numbers.

Table 25: Patent Age from Date of Issuance (in Years), by Patent Types[124]

	Mean	Median
Invention Patents	6.13	4.975
Utility Models	5.65	5.30
Design Patents	3.89	3.52

124. Fourteen cases are excluded when calculating patent age due to the lack of exact decision date: Zhushihuishe Bailida, Guangzhoushi Junyu Jiayong Dianzi Hengqi Youxian Gongsi (株式会社百利达诉广州市君宇家用电子衡器有限公司) [Tanita Co. v. Guangzhou Junyu Home Scale Co.] CHINA JUDGMENT ONLINE (Guangzhou Interm. People's Ct. June __, 2014), Chen Chujia, Guangdong Aodi Dongman Wanju Youxian Gongsi (陈楚佳诉广东奥迪动漫玩具有限公司) [Chen v. Guangdong Aodi Toys Co.] CHINA JUDGMENT ONLINE (Guangdong Higher People's Ct. Jan. __, 2014), Luo Yonglan v. Guo Guibo (罗永兰诉郭贵伯) CHINA JUDGMENT ONLINE (Guangdong Higher People's Ct. 2014), Jiangmenshi Xinhuiqu Daze Baiqing Wujin Guijiao Zhipinchang, Qiu Zhiwen (江门市新会区大泽柏庆五金硅胶制品厂诉周庆兵) [Jiangmenshi Xinhuiqu Hardware Silicon Gel Mfg. v. Zhou] CHINA JUDGMENT ONLINE (Guangdong Higher People's Ct. 2014), Dongguanshi Jingneng Zhengche Jixie Youxian Gongsi, Qixiang Zhenche (Shanghai) Youxian Gongsi (东莞市精能针车机械有限公司诉启翔针车（上海）有限公司) [Dongguan Jingneng Sewing Mach. Co. v. Qixiang Sewing Mach. (Shanghai) Co.] CHINA JUDGMENT ONLINE (Guangdong Higher People's Ct. 2014), He Qiansheng v. Hubei Quanyuan Dianli Gongcheng Youxian Gongsi (何乾生诉湖北泉源电力工程有限公司) [He v. Hubei Quanyuan Elec. Eng'g Co.] CHINA JUDGMENT ONLINE (Wuhan Interm. People's Ct. Aug. __, 2014), Dongguanshi Zhigao Wenju Youxian Gongsi, Xu Zhelin (东莞市智高文具有限公司诉徐哲琳) [Dongguan Zhigao Stationary Co. v. Xu] CHINA JUDGMENT ONLINE (Jiangxi Higher People's Ct. Apr. __, 2014), Xiamen Minghe Weiyu Shebei Youxian Gongsi, Zhang Zhijie (厦门明合卫浴设备有限公司诉张智杰) [Xiamen Bright Showers Co. v. Zhang] CHINA JUDGMENT ONLINE (Quanzhou Interm. People's Ct. Mar. __, 2014), Guangzhou Ailite Guangdian Keji Youxian Gongsi, Guangzhou Liangmeiji Dengshi Youxian Gongsi (广州艾丽特光电科技有限公司诉广州亮美集灯饰有限公司) [Guangzhou Ailite Optoelectronic Co. v. Guangzhou Liangmeiji Lighting Ltd.] CHINA JUDGMENT ONLINE (Guangdong Higher People's Ct. Mar. __, 2014), Guangzhou Liangmeiji Dengshi Youxian Gongsi, Guangzhou Ailite Guangdian Keji Youxian Gongsi (广州亮美集灯饰有限公司诉广州艾丽特光电科技有限公司) [Guangzhou Liangmeiji Lighting Ltd. v. Guangzhou Ailite Optoelectronic Co.] CHINA JUDGMENT ONLINE (Guangdong Higher People's Ct. Mar. __, 2014), Gan Ruifeng v. Su Zhaohong (范锐丰诉苏钊洪) CHINA JUDGMENT ONLINE (Guangdong Higher People's Ct. Apr. __, 2014), Foshanshi Nanhaijia Kemei Huayuan Yongpin Youxian Gongsi, Cheng Bin (佛山市南海家可美花园用品有限公司诉程兵) [Foshan Nanhai Kemei Garden Supplies Co. v. Cheng] CHINA JUDGMENT ONLINE (Guangdong Higher People's Ct. 2014), Liu Xiaotao, Jieyangshi Zhidi Chaju Youxian Gongsi (刘晓涛诉揭阳市值的茶具有限公司) [Liu v. Jieyang Zhidi Tea Supplies Co.] CHINA JUDGMENT ONLINE (Shantou Interm. People's Ct. Dec. __, 2014).

Table 26: Patent Age from Date of Application (in Years), by Patent Types[125]

	Mean	Median
Invention Patents	9.63	8.855
Utility Models	6.56	6.155
Design Patents	4.55	4.11

The average prosecution length for invention patents was 3.50 years. Due to mandatory substantive examination,[126] it was much longer than the average prosecution time for utility models (0.91 years) and design patents (0.66 years). Meanwhile, though both utility models and design patents are required to pass preliminary examination only, the average prosecution length for the former was approximately 37.88% longer than for the latter.

The average patent age between issuance and adjudication for invention patents, utility models, and design patents was 6.13 years, 5.65 years, and 3.89 years respectively. Together with the time spent in prosecution, patent owners had, on average, waited for approximately half of the protection term of their patents (48.15% for invention patents, 65.60% for utility models, and 45.50% for design patents) before enforcement. More surprisingly, utility models—which have been regarded as an effective tool to obtain faster patent protection in China—were enforced relatively later than both invention and design patents.[127]

These statistics imply that, for some reason, patent owners often did not litigate in the early years of the patent protection term. One possible explanation is that companies might obtain patents with no immediate intention of enforcement. Instead, they plan to use patents to scare competitors and exercise market power. Another explanation might be that patent enforcement in China was relatively weak, and many patent owners would therefore rather wait until the system reaches a certain level of maturity before enforcing their patents.[128]

To evaluate how the above measures of elapsed time influence the final

125. *Id.*

126. According to Chinese patent law, utility models and design patents only receive preliminary examination with no substantive prior art search, while invention patents receive both preliminary and substantive examination, which is more detailed and takes much longer.

127. I compare the ratios of the average ages from date of application of litigated invention patents, utility models, and design patents to their own patent protection terms here, instead of the pure figures relating to the average patent ages.

128. Further research is needed to test this hypothesis. If the average age of litigated patents drops when the patent age trend is monitored for several years in a row, it is more likely that weak enforcement is the reason for the rather old technology reported in this Article.

outcome of patent infringement cases in China, the quantitative time information was recoded into several intervals; that is, each piece of time information is arranged into one of two time intervals—"short" or "long"—based on whether it is shorter than the average time of its own category. The processed results are set out in Tables 27–29 below.

Table 27: Case Results, by Prosecution Length

	Decisions	Infringed	Injunction	Avg. Damages
Total	1,660 (100%)	1,330 (80.12%)	1,202 (90.38%)	¥76,078.01 ($12,390.56)
Short	924 (55.66%)	725 (78.46%)	668 (92.14%)	¥72,451.92 ($11,799.99)
Long	736 (44.34%)	605 (82.20%)	534 (88.26%)	¥80,539.43 ($13,117.17)

Table 28: Case Results, by Patent Age from Date of Issuance

	Decisions	Infringed	Injunction	Avg. Damages
Total	1,646 (100%)[129]	1,317 (80.01%)	1,191 (90.43%)	¥76,116.29 ($12,396.79)
Short	923 (56.08%)	710 (76.92%)	671 (94.51%)	¥80,810.11 ($13,161.26)
Long	723 (43.92%)	607 (83.96%)	520 (85.67%)	¥70,529.18 ($11,486.84)

Table 29: Case Results, by Patent Age from Date of Application

	Decisions	Infringed	Injunction	Avg. Damages
Total	1,646	1,317 (80.01%)	1,191 (90.43%)	¥76,116.29 ($12,396.79)
Short	906	690 (76.16%)	653 (94.64%)	¥71,620.84 ($11,664.63)
Long	740	627 (84.73%)	538 (85.81%)	¥81,137.96 ($13,214.65)

129. Fourteen cases are excluded when calculating delay time due to the lack of exact decision date. *See supra* note 124.

It is difficult to discern patterns from the above figures. However, some interesting findings arise from the predictive significance of the above. This Section tests nine hypotheses regarding the relationship between elapsed time—prosecution time, patent age from date of issuance, or patent age from date of application—and case outcomes—infringement, injunction, or damages. In five scenarios the time elapsed resulted in a statistically significant change in likelihood of success.

Hypothesis IV-B-1: There is no difference between the likelihood that infringement will be found by a Chinese court in a patent infringement case brought shortly after issuance and a patent infringement case brought a relatively long time after issuance. (Rejected)

Hypothesis IV-C-1: There is no difference between the likelihood that infringement will be found by a Chinese court in a patent infringement case brought early during its protection term and a patent infringement case brought late during its protection term. (Rejected)

The G-square p-values were .0005 and .0000 respectively, indicating that the above hypotheses can be rejected with great confidence. The relationship between patent age from date of issuance/application and infringement rate may result from the participation of NPEs. Professor Love found in his article "An Empirical Study of Patent Litigation Timing: Could a Patent Term Reduction Decimate Trolls without Harming Innovators" that practicing companies usually litigate soon after issuance and complete in the middle of their patent term, while NPEs start relatively late and would not end enforcement until their patent expired.[130] If that was also applicable to what happened in China, the lower infringement rate of cases with short patent age than cases with long patent age might lead to the conclusion that practicing entities were not as successful as NPEs in the Chinese courts.

The following two hypotheses can also be rejected with great confidence (G-square p-value = .0000).

Hypothesis IV-B-2: There is no difference between the likelihood that a patent infringement case brought shortly after issuance and a patent infringement case brought a relatively long time after issuance will be granted injunctions by a Chinese court. (Rejected)

Hypothesis IV-C-2: There is no difference between the likelihood that a patent infringement case brought early during its protection term and a patent

130. Professor Love's finding might not apply to Chinese infringement cases, and further research is required to test this hypothesis. *See* Love et al., *supra* note 29.

infringement case brought late during its protection term will be granted injunctions by a Chinese court. (Rejected)

The reason that cases brought shortly after issuance/early during the protection term enjoy a higher possibility of getting injunctions is quite obvious, because litigations brought relatively late sometimes end after the litigated patent has expired, thus making injunctions no longer necessary. Of the 87 cases with a long patent age from date of issuance in which no injunctions were granted, 32 were due to patent expiration.

The following hypothesis can also be rejected with a fair degree of confidence (G-square p-value = .0222).

Hypothesis IV-A-2: There is no difference between the likelihood that an infringement case involving a patent with a short prosecution time and a patent infringement case involving a patent with a long prosecution time will be granted injunctions by a Chinese court. (Rejected)

H. INDEPENDENT/EXPLANATORY FACTOR V—JURISDICTIONS

In terms of Article 28 of the Civil Procedure Law of the People's Republic of China (amended in 2012), litigants can have their patent infringement cases heard in courts located either at the place where one of the defendants resides, or where the infringing activities occurred.[131] The table below provides a breakdown of the jurisdiction in which each of the 1,663 cases was heard.

131. *See* Minshi Susong Fa (民事诉讼法) [Law on Civil Procedure] (promulgated by the Standing Comm. Nat'l People's Cong., April 9, 1991), art. 28 ("An action instituted for a tort shall be under the jurisdiction of the people's court at the place where the tort occurs or at the place of domicile of the defendant.").

Table 30: Case Counts by Jurisdictions

Rank	Jurisdiction	No. Cases	Percentage
1	Guangdong	530	31.87%
2	Zhejiang	280	16.84%
3	Shandong	96	5.77%
4	Beijing	82	4.93%
5	Jiangsu	80	4.81%
6	Fujian	79	4.75%
7	Henan	66	3.97%
8	Hebei	61	3.67%
9	Shanghai	55	3.31%
10	Yunnan	52	3.13%
11	Hunan	50	3.01%
12	Sichuan	35	2.10%
13	Hubei	32	1.92%
14	Anhui	27	1.62%
15	Guizhou	26	1.56%
16	Jilin	25	1.50%
17	Liaoning	20	1.20%
18	Chongqing	16	0.96%
19	Shaanxi	14	0.84%
20	Xinjiang	9	0.54%
21	Jiangxi	7	0.42%
22	Guangxi	5	0.30%
23	Heilongjiang	4	0.24%
23	Ningxia	4	0.24%
25	Gansu	3	0.18%
25	Tianjin	3	0.18%
27	Inner Mongolia	2	0.12%

Of the 31 provincial-level administrative divisions in mainland China ("provinces" unless otherwise specified),[132] 27 were selected at least once by patent holders as the jurisdiction in which to bring patent infringement

132. Hong Kong and Macau are excluded here because their legal systems are independent of the legal system in mainland China.

lawsuits.[133] However, the number of cases litigated in each province varied greatly. Provinces with better economic development heard significantly more cases than less economically developed provinces. For example, Guangdong, a province located in southern China, and with the highest GDP nationwide, heard over 30% of all patent infringement lawsuits in 2014 and approximately 50% of the lawsuits together with Zhejiang, a province located on east coast, with the fourth highest GDP.[134] The correlation between the level of economic development and the number of litigated cases makes a lot of sense. Economically developed provinces in China generally have more developed manufacturing industries, and more activities are likely to result in both litigation and infringement.

The National Bureau of Statistics of China divides mainland China's 31 provinces into 4 economic regions, based on their location and level of economic development.[135] Table 31 below lists the number and percentages of patent infringement cases heard within these various economic regions.

Table 31: Case Counts by Economic Regions

Rank	Economic Region	No. Cases (Percentage)	No. Provinces	No. Cases Per Province
1	East Coast[136]	1,266 (76.13%)	10	126.60
2	Central China[137]	182 (10.94%)	6	30.33
3	Western China[138]	166 (9.98%)	12	13.83
4	Northeast China[139]	49 (2.95%)	3	16.33

133. The fact that no patent infringement suits were litigated in the other four provinces in 2014 might be due to the incompleteness of CJO's data.

134. *See National Data*, NAT'L BUREAU OF STATISTICS OF CHINA, http://data.stats.gov.cn/english/easyquery.htm?cn=E0103 [https://perma.cc/G9HB-2JN5] (last visited Aug. 15, 2018).

135. *See Division of Economic Regions*, NAT'L BUREAU OF STATISTICS OF CHINA, http://www.stats.gov.cn/ztjc/zthd/sjtjr/dejtjkfr/tjkp/201106/t20110613_71947.htm [https://perma.cc/FYN8-SLYU] (last visited Oct. 4, 2017).

136. This includes ten provinces: Beijing, Tianjin, Hebei, Shanghai, Jiangsu, Zhejiang, Fujian, Shandong, Guangdong, and Hainan.

137. This includes six provinces: Shanxi, Anhui, Jiangxi, Henan, Hubei, and Hunan.

138. This includes twelve provinces: Inner Mongolia, Guangxi, Chongqing, Sichuan, Guizhou, Yunnan, Tibet, Shaanxi, Gansu, Qinghai, Ningxia, and Xinjiang.

139. This includes 3 provinces: Heilongjiang, Jilin, and Liaoning.

On the basis of these data, patent infringement cases were highly concentrated in the East Coast region—the most economically developed part of China. The nine provinces from this region, including Beijing, Tianjin, Hebei, Shanghai, Jiangsu, Zhejiang, Fujian, Shandong, and Guangdong, heard more than three quarters of all patent infringement lawsuits in 2014. Eight of them were among the ten provinces with the most litigated cases. However, the other 22 provinces from the other three economic regions heard only approximately a quarter of all litigated cases.

Case outcomes measured by economic regions are set out in Table 32 below.

Table 32: Case Results by Economic Regions

	No. Cases	No. Infringed	No. Injunctions	Avg. Damages
Total	1,663	1,333 (80.16%)	1,203 (90.25%)	¥75,942.39 ($12,368.47)
East Coast	1,266	1,016 (80.25%)	952 (93.70%)	¥84,136.61 ($13,703.03)
Central China	182	141 (77.47%)	127 (90.07%)	¥38,947.60 ($6,343.25)
Western China	166	136 (81.93%)	105 (77.21%)	¥61,491.49 ($10,014.90)
Northeast China	49	40 (81.63%)	19 (47.50%)	¥35,193.68 ($5,731.87)

The win rates across economic regions were remarkably consistent. Plaintiffs tended to obtain a verdict of infringement in approximately 80% of cases, no matter where the case was litigated. Injunction rates, however, were different in each region. Contrasting with injunction rates of higher than 90% in East Coast (93.70%) and Central China (90.07%), courts in Western China and Northeast China granted injunctions only in 77.21% and 47.50% of cases respectively. However, based on these figures, the conclusion that plaintiffs were more likely to receive injunctions in East Coast and Central China should not be drawn, because injunction rates in this Article are calculated by dividing the number of cases in which injunctions were granted by the number of cases in which infringement was found. The variance in injunction rates would be much smaller if the number of cases in which injunctions were requested and

necessary[140] was taken as the denominator.

The average damages awarded in the four economic regions were not consistent. On average, plaintiffs who litigated in the East Coast region received the highest amount in damages (￥84,136.61, or US$13,703.03), while plaintiffs who litigated in the Northeast region received the lowest (￥35,193.68, or US$5,731.87). One explanation for the higher rate of damages in the East Coast may be that sophisticated parties holding patents of higher value elected to litigate in that region.

The results of hypothesis testing support what is observed from the above descriptive statistics. Hypothesis V-A, testing the relationship between win rates and economic regions cannot be rejected (G-square p-value: .7508). In contrast, the relationship between injunction rates (G-square p-value: .0000) and damages (G-square p-value: .0288), and economic regions can be rejected with a different degree of confidence.

Hypothesis V-A: There is no difference between the likelihood that a court in the East Coast, a court in Central China, a court in Western China, and a court in Northeast China will find infringement in a patent infringement lawsuit. (Not Rejected)

Hypothesis V-B: There is no difference between the likelihood that a court in the East Coast, a court in Central China, a court in Western China, and a court in Northeast China will grant injunctions in a patent infringement lawsuit after infringement is found. (Rejected)

Hypothesis V-C: There is no difference between the damages awarded to a patentee or licensee in a patent infringement case by a court in the East Coast, a court in Central China, a court in Western China, and a court in Northeast China. (Rejected)

The Section below highlights several interesting characteristics of the patent infringement cases heard in different economic regions, for the sake of interest.

First, fewer invention patents and more utility models and design patents were litigated in Western and Northeast China than in East Coast and Central China (Table 33), indicating that the patents litigated in less developed regions were of lower quality than their counterparts litigated in more developed regions.

140. Injunctions are not necessary if the patent at issue expires at the time of adjudication, or an injunction has already been issued in a prior proceeding.

Table 33: Litigated Patent Types, by Economic Region

	Total	Invention Patents	Utility Models	Design Patents
East Coast	1,265	171 (13.52%)	280 (22.13%)	814 (64.35%)
Central China	182	25 (13.74%)	38 (20.88%)	119 (65.38%)
Western China	164	17 (10.37%)	85 (51.83%)	62 (37.80%)
Northeast China	49	5 (10.20%)	17 (34.69%)	27 (55.10%)

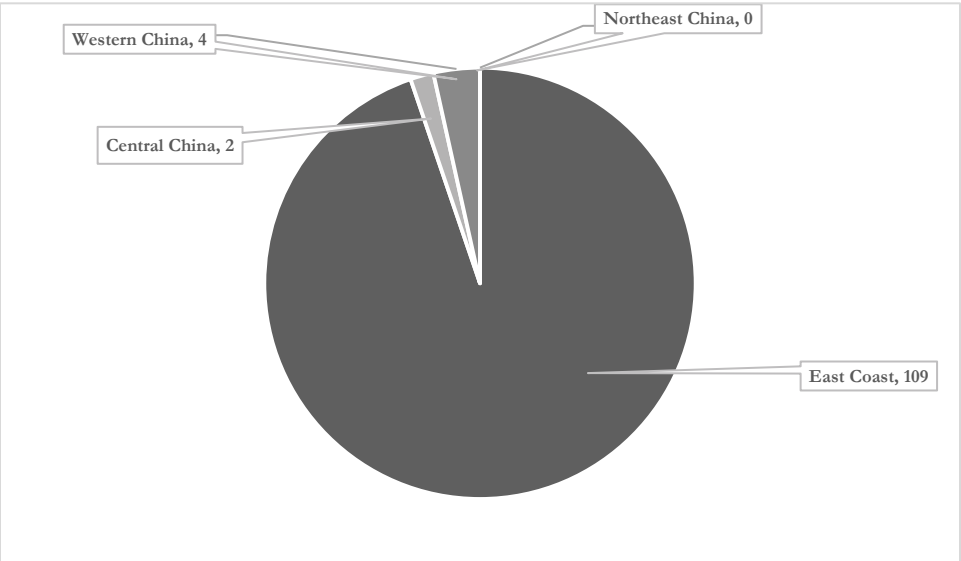
Second, fewer electrical and chemical patents were litigated in Western and Northeast China than in East Coast and Central China (Table 34), indicating that Western and Northeast China have a different industrial structure from the East Coast and Central China—focused primarily on run-of-the-mill mechanical inventions.

Table 34: Subject Matters, by Economic Region

	Total	Mechanical	Electrical	Chemical
East Coast	1,265	379 (84.04%)	64 (14.19%)	8 (1.77%)
Central China	182	48 (76.19%)	14 (22.22%)	1 (1.59%)
Western China	164	92 (90.20%)	9 (8.82%)	1 (0.98%)
Northeast China	49	21 (95.45%)	1 (4.55%)	0 (0.00%)

Third, an overwhelming majority of cases brought by foreign patentees or licensees were litigated in the East Coast (109, or 94.78%). Few such cases were litigated in the other three regions.

Figure 4: Foreign Plaintiffs



I. INDEPENDENT/EXPLANATORY FACTOR VI—APPEALS

The last explanatory factor tested in this study is the success of appeals. Of the 1,663 final judgments in the population, approximately 40% (608 out of 1,663) are second instance (appellate) opinions. The high percentage of appellate decisions might, on one hand, be the result of the inclusion of final judgments only. For cases that have second instance opinions, their first instance opinions were excluded to avoid overrepresentation/inaccuracies.[141] On the other hand, upper level courts that adjudicate second instance cases may have uploaded a larger number of judicial opinions to CJO than lower level courts.

Table 35: Second Instance Judgments, Affirmance, and Reversal

	No. of Decisions	Percentage
Second Instance Judgments	608	36.56%
Affirmed	517	85.03%
Reversed	91	14.97%

141. Due to this limitation, this Section will not provide the details of what types of cases are generally appealed.

Table 35 above also summarizes affirmance and reversal data for second instance decisions in the population. In a significant portion (85.03%) of second instance cases, the appellate courts affirmed lower courts' verdicts. It might therefore be reasonable to conclude that the decision to include final judgments only will not result in significant bias in this research, granted that part of the decisions was missing.

To test how appeals might affect case outcomes of patent infringement litigations in China, Table 36 below presents the case outcome data by instance of trial.

Table 36: Case Results, by Instance of Trial

	Decisions	Infringed	Injunctions	Avg. Damages
1st Instance	1,055	856 (81.14%)	766 (89.49%)	¥52,596.07 ($8,566.14)
2nd Instance	608	477 (78.45%)	437 (91.61%)	¥117,329.04 ($19,108.96)

The data in Table 36 suggest that the win rates on infringement and the injunction rates were relatively steady across different instances of trial, while the average damages awarded to first and second instance cases showed notable difference. The damages awarded by second instance courts were more than twice as high as those awarded by first instance courts. The hypothesis testing results bear out these observations.

Hypothesis VI-A: There is no difference between the likelihood that a first instance court and a second instance court will find infringement in a patent infringement lawsuit. (Not Rejected)

Hypothesis VI-B: There is no difference between the likelihood that a first instance court and a second instance court will grant injunctions in a patent infringement lawsuit after infringement is found. (Not Rejected)

Hypothesis VI-C: There is no difference between the damages awarded by a first instance court and a second instance court in a patent infringement lawsuit in China. (Rejected)

The G-square p-values for Hypothesis VI-A and Hypothesis VI-B were .2104 and .2419 respectively, meaning that neither of these hypotheses can be rejected with a fair degree of confidence. However, the G-square p-value for Hypothesis VI-C was .0000, indicating that patent holders tend to receive more damages on appeal. This discrepancy could be explained on the basis of common sense—that patentees holding valuable patents have stronger

incentive to appeal than those with less valuable patents.

V. CONCLUSION

Some of the findings in this Article disprove the long-standing beliefs about patent enforcement in China. One prominent example is that although damages awarded by the Chinese courts were frustratingly low (US$4,885.99 in median), patent protection in China is stronger than commonly thought. Plaintiffs were much more successful in China, with an 80.16% win rate, than in many major countries like Germany (approximately 66% win rate) and the United States (approximately 60% win rate).[142] Moreover, permanent injunctions were automatically granted in most cases (93.76%) based on a finding of infringement in China, which partially offsets the low damages awarded.

Another example is that foreign patent holders were as likely to litigate as domestic patent holders and received noticeably better results. Foreign patentees and assignees were more likely to win and get injunctions than Chinese patent owners. Meanwhile, damages awarded to foreign patent holders (￥201,620.45, or US$32,837.21) were almost three times higher than those awarded to their Chinese counterparts (￥66,217.93, or US$10,784.68). This might indicate that the Chinese courts, while not preferring foreign parties to domestic ones, certainly did not protect the local economy at the expense of foreign companies in practice. It might also be possible that foreign patentees were very cautious about litigating in China and only litigated when there was a high probability of winning.

Other observations are unrelated to the conventional wisdom, but are still valuable because they provide detailed data on several aspects of patent infringement litigation in China, and in some cases turn sheer conjecture relating to the Chinese patent system into concrete statements. For example, the overwhelming majority of patent infringement lawsuits in China involved mechanical patents (84.64%) instead of electrical (13.79%) and chemical (1.57%) patents; patent owners, on average, waited for approximately half of the protection term of their patents (48.15% for invention patents, 65.60% for utility models, and 45.50% for design patents) before enforcement; patent infringement cases were highly concentrated in the East Coast region—the most economically developed part of China; and etc.

These findings that patent protection in China is likely stronger than ever may seem striking and somewhat suspicious. However, China is currently adopting a bifurcated patent litigation system, which means that claims of

142. *See supra* note 64.

patent infringement and validity are usually brought and decided in separate proceedings at different courts instead of in a single proceeding at the same court. Therefore, the data on patent infringement cases provided in this Article only tell half of the patent litigation story in China, and they should be viewed jointly with information on patent validity cases in subsequent research.

In addition to these descriptive statistics, this Article also tested several hypotheses in an effort to identify variables that can predict the outcome of patent infringement cases in China. The results were uneven. Patent types and patent age were the only variables that might influence the finding of infringement. The granting of injunctions was related not only to patent types and patent age, but also to prosecution length and jurisdictions. Patent type, plaintiff's residency, jurisdiction, and appeals were the factors that influenced the amount of damages awarded by a Chinese court.

The predictions made here were based on several important but controversial assumptions mentioned in Section III.D Limitations. Despite these assumptions, this Article may nevertheless serve as a statistical report on patent infringement cases decided in 2014 and currently available on CJO. All the descriptive statistics produced are still valid, and of great value for those who are trying to get a deeper understanding of patent litigation in China.

APPENDIX A

Hypothesis I-A:

Total Cases: 1,660

Patent Type	Category	# Infringed	# Not Infringed
1	Invention Patents	157	61
2	Utility Models	325	95
3	Design Patents	848	174

Test of Independence:

Statistic	p-value
G-Square	0.0004
Chi-Square	0.0003

Hypothesis I-B:

Total Cases: 1,330

Patent Type	Category	# Injunctions	# Denied Injunctions
1	Invention Patents	148	9
2	Utility Models	275	50
3	Design Patents	779	69

Test of Independence:

Statistic	p-value
G-Square	0.0003
Chi-Square	0.0002

Hypothesis I-C:

Total Cases: 1,278

Patent Type	Category	Mean	Standard Deviation
1	Invention Patents	￥259,154.64	480622.69
2	Utility Models	￥83,620.94	105410.75
3	Design Patents	￥39,167.20	56940.93

Test of Independence:

Statistic	p-value
Damage Value	0.0000

Hypothesis II-A:

Total Cases: 638

Subject Matter	# Infringed	# Not Infringed
Mechanical	408	132
Electrical	69	19
Chemical	5	5

Test of Independence:

Statistic	p-value
G-Square	0.1803
Chi-Square	0.1406

Hypothesis II-B:

Total Cases: 482

Subject Matter	# Injunctions	# Denied Injunctions
Mechanical	357	51
Electrical	62	7
Chemical	4	1

Test of Independence:

Statistic	p-value
G-Square	0.7542
Chi-Square	0.7453

Hypothesis II-C:

Total Cases: 457

Subject Matter	Mean	Standard Deviation
Mechanical	¥137,338.00	310,548.39
Electrical	¥165,457.56	237,745.44
Chemical	¥239,000.00	382,000.00

Test of Independence:

Statistic	p-value
Damage Value	0.6114

Hypothesis III-A:

Total: 1,663

Residence of Plaintiff	# Infringed	# Not Infringed
Domestic	1236	312
Foreign	97	18

Test of Independence:

Statistic	p-value
G-Square	0.2836
Chi-Square	0.2951

Hypothesis III-B:

Total: 1,333

Residence of Plaintiff	# Injunctions	# Denied Injunctions
Domestic	1113	123
Foreign	90	7

Test of Independence:

Statistic	p-value
G-Square	0.4725
Chi-Square	0.4861

Hypothesis III-C:

Total: 1,281

Residence of Plaintiff	Mean	Standard Deviation
Domestic	￥66,217.93	133,629.77
Foreign	￥201,620.45	519,830.16

Test of Independence:

Statistic	p-value
Damage Value	0.0000

Hypothesis IV-A-1:

Total: 1,660

Prosecution Length	# Infringed	# Not Infringed
Short	725	199
Long	605	131

Test of Independence:

Statistic	p-value
G-Square	0.0658
Chi-Square	0.0667

Hypothesis IV-A-2:

Total: 1,330

Prosecution Length	# Injunctions	# Denied Injunctions
Short	668	57
Long	534	71

Test of Independence:

Statistic	p-value
G-Square	0.0222
Chi-Square	0.0219

Hypothesis IV-A-3:

Total: 1,278

Prosecution Length	Mean	Standard Deviation
Short	¥72,451.92	119,224.56
Long	¥80,539.43	256,178.61

Test of Independence:

Statistic	p-value
Damage Value	0.4569

Hypothesis IV-B-1:

Total: 1,646

Delay Time	# Infringed	# Not Infringed
Short	710	213
Long	607	116

Test of Independence:

Statistic	p-value
G-Square	0.0005
Chi-Square	0.0005

Hypothesis IV-B-2:

Total: 1,317

Delay Time	# Injunctions	# Denied Injunctions
Short	671	39
Long	520	87

Test of Independence:

Statistic	p-value
G-Square	0.0000
Chi-Square	0.0000

Hypothesis IV-B-3:

Total: 1,266

Delay Time	Mean	Standard Deviation
Short	¥80,810.11	225,999.56
Long	¥70,529.18	146,522.10

Test of Independence:

Statistic	p-value
Damage Value	0.3477

Hypothesis IV-C-1:

Total: 1,646

Patent Age	# Infringed	# Not Infringed
Short	690	216
Long	627	113

Test of Independence:

Statistic	p-value
G-Square	0.0000
Chi-Square	0.0000

Hypothesis IV-C-2:

Total: 1,317

Patent Age	# Injunctions	# Denied Injunctions
Short	653	37
Long	538	89

Test of Independence:

Statistic	p-value
G-Square	0.0000
Chi-Square	0.0000

Hypothesis IV-C-3:

Total: 1,266

Patent Age	Mean	Standard Deviation
Short	￥71,620.84	129,577.07
Long	￥81,137.96	246,506.80

Test of Independence:

Statistic	p-value
Damage Value	0.3836

Hypothesis V-1:

Total: 1,663

Economic Region	# Infringed	# Not Infringed
East Coast	1,016	250
Central China	141	41
Western China	136	30
Northeast China	40	9

Test of Independence:

Statistic	p-value
G-Square	0.7508
Chi-Square	0.7467

Hypothesis V-2:

Total: 1,333

Economic Region	# Injunctions	# Denied Injunctions
East Coast	952	64
Central China	127	14
Western China	105	31
Northeast China	19	21

Test of Independence:

Statistic	p-value
G-Square	0.0000
Chi-Square	0.0000

Hypothesis V-3:

Total: 1,281

Economic Region	Mean	Standard Deviation
East Coast	¥84,136.61	209,694.93
Central China	¥38,947.60	83,844.17
Western China	¥61,491.49	148,069.89
Northeast China	¥35,193.68	59,723.84

Test of Independence:

Statistic	p-value
Damage Value	0.0288

Hypothesis VI-1:

Total: 1,663

Instance	# Infringed	# Not Infringed
1st Instance	856	199
2nd Instance	477	131

Test of Independence:

Statistic	p-value
G-Square	0.2104
Chi-Square	0.2085

Hypothesis VI-2:

Total: 1,333

Instance	# Injunctions	# Denied Injunctions
1st Instance	766	90
2nd Instance	437	40

Test of Independence:

Statistic	p-value
G-Square	0.2419
Chi-Square	0.2464

Hypothesis VI-3:

Total: 1,281

Instance	Mean	Standard Deviation
1st Instance	52596.07	184422.862
2nd Instance	117329.0433	200457.3029

Test of Independence:

Statistic	p-value
Damage Value	0.0000

APPENDIX B

Hypothesis Testing Results			
	Infringement	Injunctions	Damages
Patent Types	Rejected	Rejected	Rejected
Subject Matters (Invention Patents & Utility Models)	Not Rejected	Not Rejected	Not Rejected
Plaintiff's Residency	Not Rejected	Not Rejected	Rejected
Elapsed Time—Prosecution Length	Not Rejected	Rejected	Not Rejected
Elapsed Time—Patent Age from Date of Issuance	Rejected	Rejected	Not Rejected
Elapsed Time—Patent Age from Date of Application	Rejected	Rejected	Not Rejected
Jurisdictions/Economic Regions	Not Rejected	Rejected	Rejected
Appeals	Not Rejected	Not Rejected	Rejected

TRUST, BUT VERIFY: WHY THE BLOCKCHAIN NEEDS THE LAW

Kevin Werbach†

ABSTRACT

The blockchain could be the most consequential development in information technology since the Internet. Created to support the Bitcoin digital currency, the blockchain is actually something deeper: a novel solution to the age-old human problem of trust. Its potential is extraordinary. Yet, this approach may not promote trust at all without effective governance. Wholly divorced from legal enforcement, blockchain-based systems may be counterproductive or even dangerous. And they are less insulated from the law's reach than it seems. The central question is not how to regulate blockchains but how blockchains regulate. They may supplement, complement, or substitute for legal enforcement. Excessive or premature application of rigid legal obligations will stymie innovation and forego opportunities to leverage technology to achieve public policy objectives. Blockchain developers and legal institutions can work together. Each must recognize the unique affordances of the other system.

DOI: https://doi.org/10.15779/Z38H41JM9N

† Associate Professor of Legal Studies and Business Ethics, The Wharton School, University of Pennsylvania. Email: werbach@wharton.upenn.edu. Thanks to Dan Hunter for collaborating to develop the ideas that gave rise to this Article, and to Sarah Light, Patrick Murck, and participants in the 2017 Lastowka Cyberlaw Colloquium and 2016 TPRC Conference for comments on earlier drafts.

TABLE OF CONTENTS

I. INTRODUCTION: CODE'S REVENGE

The blockchain[1] has been called "[t]he technology most likely to change the next decade of business."[2] It has also been described as a haven for criminal activity,[3] a Ponzi scheme,[4] and a road both to anarchy[5] and to authoritarianism.[6] The root of this confusion is the blockchain's uncertain relationship to law. Proponents of blockchain technology describe it as a democratizing escape from the failings of territorial legal systems. Critics see it as a clever trick to avoid legal accountability. Neither is entirely correct…or entirely wrong. Both perspectives focus excessively on regulation of blockchains and not enough on how blockchains regulate. To achieve their monumental potential and avoid catastrophic failures, blockchain-based systems will need to integrate with the operations and institutions of the law.

From its roots in the Bitcoin cryptocurrency,[7] launched in 2009 by the pseudonymous Satoshi Nakamoto, the blockchain has rapidly taken hold around the world. The price of bitcoin jumped twenty-fold between late 2016 and the end of 2017, and other cryptocurrencies experienced similar appreciation.[8] Venture capitalists poured over $1 billion into blockchain-based

1. There is not yet agreement on terminology. Technically, a blockchain (sometimes written as "block chain") is a data storage system using sequentially signed blocks, as described in Part II. "The blockchain" may describe the universe of blockchains (similar to "the Internet"), the subset of public blockchains, or just the public ledger for Bitcoin.
Adding further confusion, some "blockchain" platforms use neither chains of blocks nor Bitcoin-like digital currencies. The more accurate term for this class of systems is distributed ledger technology (DLT).

2. *See* Don Tapscott & Alex Tapscott, *The Impact of the Blockchain Goes Beyond Financial Services*, HARV. BUS. REV. (May 10, 2016), https://hbr.org/2016/05/the-impact-of-the-blockchain-goes-beyond-financial-services [https://perma.cc/7M3G-XUQY].

3. *See* Kim Zetter, *FBI Fears Bitcoin's Popularity with Criminals*, WIRED (May 9, 2012), https://www.wired.com/2012/05/fbi-fears-bitcoin/ [https://perma.cc/2LCF-XPQK].

4. *See* Matt O'Brien, *Bitcoin Isn't the Future of Money—It's Either a Ponzi Scheme or a Pyramid Scheme*, WASH. POST: WONKBLOG (June 8, 2015), http://www.washingtonpost.com/blogs/wonkblog/wp/2015/06/08/bitcoin-isnt-the-future-of-money-its-either-a-ponzi-scheme-or-a-pyramid-scheme/ [https://perma.cc/6MDJ-U6PY].

5. *See* Matthew Sparkes, *The Coming Digital Anarchy*, TELEGRAPH (June 9, 2014), http://www.telegraph.co.uk/technology/news/10881213/The-coming-digital-anarchy.html [https://perma.cc/T4LT-BXRK].

6. *See* Ian Bogost, *Cryptocurrency Might Be a Path to Authoritarianism*, ATLANTIC (May 30, 2017), https://www.theatlantic.com/technology/archive/2017/05/blockchain-of-command/528543/ [https://perma.cc/UU6F-7MFW].

7. A cryptocurrency is a form of digital money secured not through the backing of a state or financial institution, but through cryptography. *See infra* Section II.A. In this Article, the term Bitcoin is capitalized when describing the system as a whole, and lower case when referring to the unit of currency.

8. *See* Nathaniel Popper, *Bitcoin's Price Has Soared. What Comes Next?*, N.Y. TIMES (Dec.

startups between 2013 and 2016.[9] Blockchain projects themselves topped that in 2017, raising over $5 billion[10] selling digital tokens directly to users and investors.

The wave of blockchain adoption is not limited to entrepreneurial ventures. Technology giants such as IBM, Microsoft, and Intel are making major blockchain commitments,[11] as are leading professional services firms such as PwC and KPMG.[12] Directly or through consortia, virtually all the world's largest financial institutions are implementing distributed ledger technology based on similar principles.[13] Governments are getting into the act as well. Several are experimenting with distributed ledger platforms, and the world's central banks, from the Bank of England to the People's Bank of China, are studying the potential of issuing their own cryptocurrencies.[14] Even relatively sober observers such as Goldman Sachs see tens of billions of dollars in annual benefits just from low-hanging fruit opportunities.[15] While the near-

---

7, 2017), https://www.nytimes.com/2017/12/07/technology/bitcoin-price-rise.html [https://perma.cc/XW86-8AMW].

9. *See* Garrick Hileman, *State of Blockchain Q1 2016: Blockchain Funding Overtakes Bitcoin*, COINDESK (May 11, 2016), http://www.coindesk.com/state-of-blockchain-q1-2016/ [https://perma.cc/LC42-4Z7Y].

10. *See* Oscar Williams-Grut, *Only 48% of ICOs Were Successful Last Year—but Startups Still Managed to Raise $5.6 Billion*, BUS. INSIDER (Jan. 31, 2018), http://www.businessinsider.com/how-much-raised-icos-2017-tokendata-2017-2018-1 [https://perma.cc/LP6N-U7H5].

11. *See* Anna Irrera, *Microsoft Unveils Technology to Speed Up Blockchain and Its Adoption*, REUTERS (Aug. 10, 2017), https://www.reuters.com/article/us-microsoft-blockchain-idUSKBN1AQ1KD [https://perma.cc/PV7M-SMB7]; Jeff John Roberts, *Can IBM Really Make a Business Out of Blockchain?*, FORTUNE (June 28, 2016), http://fortune.com/2016/06/28/ibm-blockchain/ [https://perma.cc/T6GH-VP6B].

12. *See Blockchain Services*, PRICEWATERHOUSECOOPERS, https://www.pwc.com/us/en/financial-services/fintech/blockchain.html [https://perma.cc/ND35-7P5T] (last visited Apr. 10, 2018); *Digital Ledger Services at KPMG: Seize the Potential of Blockchain Today*, KPMG, https://home.kpmg.com/xx/en/home/insights/2017/02/digital-ledger-services-at-kpmg-fs.html [https://perma.cc/8KLG-AUZM] (last visited Aug. 17, 2018).

13. *See* Nathaniel Popper, *Envisioning Bitcoin's Technology at the Heart of Global Finance*, N.Y. TIMES (Aug. 12, 2016), http://www.nytimes.com/2016/08/13/business/dealbook/bitcoin-blockchain-banking-finance.html [https://perma.cc/NT2P-P2CT] ("The report estimates that 80 percent of banks around the world could start distributed ledger projects by next year.").

14. *See* John Barrdear & Michael Kumhof, *The Macroeconomics of Central Bank Issued Digital Currencies* 3 (Bank of England, Staff Working Paper No. 605, 2016), http://www.bankofengland.co.uk/research/Documents/workingpapers/2016/swp605.pdf [https://perma.cc/QJV3-MNTT]; Chuan Tian, *China's Central Bank Opens New Digital Currency Research Institute*, COINDESK (June 30, 2017), https://www.coindesk.com/chinas-central-bank-opens-new-digital-currency-research-institute/ [https://perma.cc/3GRF-L7C3].

15. *See* James Schneider et al., *Blockchain: Putting Theory into Practice*, GOLDMAN SACHS EQUITY RES. 4 (May 24, 2016), https://www.scribd.com/doc/313839001/Profiles-in-Innovation-May-24-2016-1 [https://perma.cc/93FJ-EEDW].

term impacts of the blockchain may be overhyped, its long-term potential as a distributed foundation for the exchange of value is extraordinary.[16]

Blockchains use complex technology, but their basic function is simple: providing a distributed yet provably accurate record. Everyone can maintain a copy of a dynamically-updated ledger, but all those copies remain the same, even without a central administrator or master version.[17] This approach offers two basic benefits. First, one can have confidence in transactions without trusting the integrity of any individuals, intermediaries, or governments. Second, the single distributed ledger replaces many private ledgers that must be reconciled for consistency, thus reducing transaction costs. The software enabling this uses digital cryptography and game-theoretic incentives to make it difficult to cheat the system.

The initial interest in blockchains focused on Bitcoin as a private digital currency outside the control of territorial governments. Traditionally, currency transactions are heavily regulated to address concerns about fraud, money laundering, capital flight, currency manipulation, terrorist financing, and more.[18] Governments and powerful private interests have also prevailed on banks or payment processors to cut off services involved in gambling, distribution of copyrighted material, or dissemination of leaked government documents, even when such conduct was not clearly illegal in some jurisdictions. Bitcoin appears to operate as a store of value and a mechanism for transactions without any such constraints. It raises the tantalizing prospect (for some) of "censorship-proof" money.

On the other hand, unregulated currency can easily become a haven for lawlessness, consumer abuses, and financial speculation.[19] For some time, Bitcoin had a somewhat unsavory reputation. The early Bitcoin-based marketplace Silk Road, which was used primarily for drugs and other contraband, is the most spectacular example.[20] It was eventually shut down by

16. *See* Marco Iansiti & Karim R. Lakhani, *The Truth About Blockchain*, HARV. BUS. REV. (Jan./Feb. 2017), https://hbr.org/2017/01/the-truth-about-blockchain [https://perma.cc/XEH4-YUE2] (describing the vast potential of the blockchain as a foundational technology, which will nonetheless take time to be realized fully).

17. A detailed explanation of how the blockchain achieves this paradoxical result is provided in Part II.

18. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-14-496, VIRTUAL CURRENCIES: EMERGING REGULATORY, LAW ENFORCEMENT, AND CONSUMER PROTECTION CHALLENGES 19 (2014); JERRY BRITO & ANDREA CASTILLO, BITCOIN: A PRIMER FOR POLICYMAKERS 43–47 (2013).

19. *See* HOMELAND SEC. STUDIES & ANALYSIS INST., RISKS AND THREATS OF CRYPTOCURRENCIES 2–3 (2014), https://www.anser.org/docs/reports/RP14-01.03.03-02_Cryptocurrencies 508_31Dec2014.pdf [https://perma.cc/6MYY-DLX5].

20. *See* David Yermack, *Is Bitcoin a Real Currency?* 6 (Nat'l Bureau of Econ. Research, Working Paper No. 19747, 2013), http://www.nber.org/papers/w19747.pdf

the FBI in 2013, and its operator, Ross Ulbricht, was sentenced to life in prison. However, during its three years of operation, Silk Road processed sales worth 9.5 million Bitcoin, or roughly $1.2 billion at the time.[21] Although legitimate applications have multiplied since then, the question whether Bitcoin and its progeny are the world's greatest gift to criminals remains.

While it seemingly precludes traditional legal enforcement, a blockchain-based system's software enforces its own rules in a manner analogous to the legal system. It thus illustrates the foundational insight of cyberlaw scholar Lawrence Lessig's 1999 book, *Code and Other Laws of Cyberspace*: code is law.[22] As in the 1990s, when peer-to-peer file sharing seemed on the verge of transforming copyright and free speech online seemed immune from government repression, those who seek to overturn existing power dynamics are invigorated. Legal scholars Aaron Wright and Primavera de Filippi, for example, argue that the blockchain "could make it easier for citizens to create custom legal systems, where people are free to choose and to implement their own rules within their own techno-legal frameworks."[23] Cyber-libertarianism remains a beautiful dream. But the idea that all online communities will successfully enforce their own rules, without regard for governments, will fare as poorly as it did the first time. It already has.

Over a few weeks in mid-2016, some 11,000 individuals worldwide committed Ether cryptocurrency worth roughly $150 million to a blockchain-based virtual company with no employees, no management, and no legal existence.[24] The DAO, short for "distributed autonomous organization," was

[https://perma.cc/Z53K-SG9T]; Joshuah Bearman, *The Rise and Fall of Silk Road: Part II*, WIRED (May 2015), http://www.wired.com/2015/05/silk-road-2 [https://perma.cc/L3G2-BUAG]; Joshuah Bearman, *The Rise and Fall of Silk Road: Part I*, WIRED (Apr. 2015), http://www.wired.com/2015/04/silk-road-1 [https://perma.cc/5V47-EB6S].

21. Sealed Complaint at 15, United States v. Ulbricht, 31 F. Supp. 3d 540 (S.D.N.Y. 2014) (No. 14-cr-68), https://www.documentcloud.org/documents/801103-172770276-ulbricht-criminal-complaint.html [https://perma.cc/2FNK-F37V]. At that point, the total supply of Bitcoin was only about twelve million.

22. *See generally* LAWRENCE LESSIG, CODE, AND OTHER LAWS OF CYBERSPACE (1999). Lessig published an updated version of the book in 2006, to incorporate new developments such as social media. *See generally* LAWRENCE LESSIG, CODE VERSION 2.0 (2006) [hereinafter CODE VERSION 2.0].

23. *See* Aaron Wright & Primavera De Filippi, Decentralized Blockchain Technology and the Rise of Lex Cryptographia 40 (unpublished manuscript) (Mar. 12, 2015), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2580664 [https://perma.cc/3YUP-PNM4].

24. *See* Nathaniel Popper, *A Venture Fund With Plenty of Virtual Capital, but No Capitalis*t, N.Y. TIMES (May 21, 2016), https://www.nytimes.com/2016/05/22/business/dealbook/crypto-ether-bitcoin-currency.html [https://perma.cc/4DWV-VETX]; Joon Ian Wong, *The Price of Ether, a Bitcoin Rival, Is Soaring Because of a Radical, $150 Million Experiment*, QUARTZ (May 20, 2016), https://qz.com/688194/the-price-of-ether-a-bitcoin-rival-is-soaring-because-of-a

an online crowdfunding system built entirely out of self-executing software known as smart contracts.[25] It was hailed as "[a] new paradigm of economic cooperation . . . a digital democratization of business."[26] Autonomous code, running on a distributed platform with no central authority, took the place of law, intermediaries, and personal relationships as the instrument of trust. And then someone stole a third of the money overnight.[27]

That is when things got interesting.[28] According to The DAO's software, the siphoning off of funds was entirely legitimate. The blockchain had no way to distinguish between a thief and a customer.[29] More seriously, the immutability of blockchain records meant that no one had the power to stop or reverse the theft.[30] Eventually, the entire blockchain platform The DAO operated on had to be split in half in order to restore the funds.[31] A renegade group disagreed with this decision, so it began operating a duplicate currency where the thief kept the stolen funds.[32] The story sounds bizarre, but it is a

-radical-150-million-experiment/ [https://perma.cc/UYM2-PVUX].

25. *See generally* Christoph Jentzsch, Decentralized Autonomous Organization to Automate Governance (unpublished manuscript) https://download.slock.it/public/DAO/WhitePaper.pdf [https://perma.cc/4B6L-BW68] (last visited Aug. 18, 2018) (describing the structure and functions of The DAO). For a more detailed discussion of smart contracts, see generally Max Raskin, *The Law and Legality of Smart Contracts*, 1 GEO. L. TECH. REV. 305 (2017); Jeremy M. Sklaroff, *Smart Contracts and the Cost of Inflexibility*, 166 U. PA. L. REV. 263 (2017); Kevin Werbach & Nicolas Cornell, *Contracts Ex Machina*, 67 DUKE L.J. 313 (2017).

26. Seth Bannon, *The Tao of "The DAO" or: How the Autonomous Corporation Is Already Here*, TECHCRUNCH (May 16, 2016), https://techcrunch.com/2016/05/16/the-tao-of-the-dao-or-how-the-autonomous-corporation-is-already-here/ [https://perma.cc/V5Z3-B6JC].

27. *See* Klint Finley, *A $50 Million Hack Just Showed that the DAO Was All Too Human*, WIRED (June 18, 2016), https://www.wired.com/2016/06/50-million-hack-just-showed-dao-human/ [https://perma.cc/4V66-8ARF]; Nathaniel Popper, *A Hacking of More Than $50 Million Dashes Hopes in the World of Virtual Currency*, N.Y. TIMES (June 17, 2016), http://www.nytimes.com/2016/06/18/business/dealbook/hacker-may-have-removed-more-than-50-million-from-experimental-cybercurrency-project.html [https://perma.cc/QFQ5-B528].

28. One account described the subsequent events as "arguably the most philosophically interesting event to take place in your lifetime or mine." E.J. Spode, *The Great Cryptocurrency Heist*, AEON (Feb. 14, 2017), https://aeon.co/essays/trust-the-inside-story-of-the-rise-and-fall-of-ethereum [https://perma.cc/9HGW-9SEA].

29. *See* Vitalik Buterin, *Thinking About Smart Contract Security*, ETHEREUM BLOG (June 19, 2016), https://blog.ethereum.org/2016/06/19/thinking-smart-contract-security/ [https://perma.cc/TP5M-SBPN] ("All instances of smart contract theft or loss—in fact, *the very definition* of smart contract theft or loss, is fundamentally about differences between implementation and intent.").

30. *See* Finley, *supra* note 27 ("If people can simply reverse transactions they didn't mean to make, it proves that people, not mathematics are really in charge of the system . . . .").

31. Michael del Castillo, *Ethereum Executes Blockchain Hard Fork to Return DAO Funds*, COINDESK (July 20, 2016), http://www.coindesk.com/ethereum-executes-blockchain-hard-fork-return-dao-investor-funds/ [https://perma.cc/EK4R-XTAU].

32. Paul Vigna, *The Great Digital-Currency Debate: 'New' Ethereum Vs. Ethereum 'Classic'*,

harbinger of things to come. The DAO's software worked exactly as designed to replace legal enforcement and third-party intermediaries. Yet that created its own problems. There was verification, but a breakdown in trust. Users only got their money back because the supposedly immutable, unstoppable blockchain actually was not.

The DAO incident is emblematic of deeper issues. The reason the blockchain needs law is that both the blockchain and the law are, at their core, mechanisms of trust. Distributed ledger technology allows participants to trust the outcome of a system without trusting any individual participant. Yet trust implies uncertainty or vulnerability.[33] That is why President Reagan's favorite Russian proverb,[34] the title of this Article, is often criticized as meaningless: "If you trust, you won't insist on verifying, whereas if you insist on verifying, clearly you don't trust."[35] The blockchain is an ingenious solution for verification but to promote trust requires something more. That is where the legal system comes in play.

Even if the math works perfectly, blockchains are systems designed, implemented, and used by humans. Subjective intent remains relevant even when expressed through objective code. Blockchains are vulnerable to selfish behavior, attacks, and manipulation.[36] By 2016, there were already at least fifteen incidents in which cryptocurrency worth at least $1 million was stolen, with a total value exceeding $600 million.[37] And the scope of theft only increased after that, as cryptocurrency prices skyrocketed in 2017.[38] The scope

---

WALL ST. J. (Aug. 1, 2016), http://blogs.wsj.com/moneybeat/2016/08/01/the-great-digital-currency-debate-new-ethereum-vs-ethereum-classic/ [https://perma.cc/D5CZ-DYUU].

33. *See* Roger C. Mayer et al., *An Integrative Model of Organizational Trust*, 20 ACAD. MGMT. REV. 709, 712–14, (1995); Helen Nissenbaum, *Will Security Enhance Trust Online, or Supplant It*, *in* TRUST AND DISTRUST IN ORGANIZATIONS: DILEMMAS AND APPROACHES 155, 173 (Roderick M. Kramer & Karen S. Cook eds., 2004); Denise M. Rousseau et al., *Not So Different After All: A Cross-Discipline View of Trust*, 23 ACAD. MGMT. REV. 393, 394–95 (1998).

34. Reagan famously used this aphorism at the signing ceremony for the Intermediate-Range Nuclear Forces treaty with the Soviet Union in 1987. Soviet leader Mikhail Gorbachev remarked with exasperation, "You repeat that at every meeting." *See* DAVID E. HOFFMAN, THE DEAD HAND: THE UNTOLD STORY OF THE COLD WAR ARMS RACE AND ITS DANGEROUS LEGACY 295 (2009). The aphorism works better in the original Russian, because the two verbs rhyme and derive from the same root.

35. Barton Swaim, *'Trust, but Verify': An Untrustworthy Political Phrase*, WASH. POST (Mar. 11, 2016), https://www.washingtonpost.com/opinions/trust-but-verify-an-untrustworthy-political-phrase/2016/03/11/da32fb08-db3b-11e5-891a-4ed04f4213e8_story.html [https://perma.cc/QR8E-ZFMU].

36. *See infra* Section III.A (describing various attacks on blockchain systems or uses of the technology to commit fraud).

37. *See* Michael Matthews, *List of Bitcoin Hacks (2012-2016)*, STEEMIT (Aug. 20, 2016), https://steemit.com/bitcoin/@michaelmatthews/list-of-bitcoin-hacks-2012-2016 [https://perma.cc/LK3V-8MJ5].

38. *See* Anna Irrera, *More Than 10 Percent of $3.7 Billion Raised in ICOs Has Been Stolen: Ernst*

of legitimate practices for blockchain-based systems is fundamentally a governance question, not a computer science one. Without realizing it, blockchain developers have wandered into territories that legal scholars have fought over for centuries.

The challenge, therefore, is what happens when ledgers meet law? Legal structures such as contracts, property, corporations, and judicial enforcement replace interpersonal trust with more structured rights, expectations, and remedies. Yet there are places the legal system cannot go, and sometimes the very formalization that law imposes is an impediment to trust. The blockchain offers a tantalizing solution. Realizing its potential, however, will require a careful mapping of the respective roles of the "dry code" of cryptography and the "wet code" of law.[39] And surprisingly, developers of blockchain-based systems will often need to incorporate both. Even at this early stage, several hybrid solutions are under development, including regulatory mechanisms, technical approaches, and new dispute resolution techniques.[40] Some make legal institutions operate more like software code; others make the blockchain's code more consistent with law.

It is a mistake, therefore, to see law and the blockchain as necessarily enemies. Legal actors can make mistakes, but so can software designers. There have been many serious failures already in the blockchain's short history; The DAO is just one example. Developing the rules, norms, incentives, and technical architectures[41] for a well-functioning community is a very hard problem. There are points where law needs to adapt to recognize the potential of the blockchain, but the reverse is also true: the blockchain needs law. Its impact will depend on its developers' ability to connect Satoshi Nakamoto's cryptoeconomic trust model with the formal structures and institutions of legal enforcement.

This Article defends the contrarian claim that law is the blockchain's destiny, not its undoing. Much of the legal scholarship in this area concentrates

---

& Young, REUTERS (Jan. 22, 2018), https://www.reuters.com/article/us-ico-ernst-young/more-than-10-percent-of-3-7-billion-raised-in-icos-has-been-stolen-ernst-young-idUSKBN1FB1MZ [https://perma.cc/V3QG-D8CS]; Nathaniel Popper, *As Bitcoin Bubble Loses Air, Frauds and Flaws Rise to Surface*, N.Y. TIMES (Feb. 5, 2018), https://www.nytimes.com/2018/02/05/technology/virtual-currency-regulation.html [https://perma.cc/J4S4-PLKP].

39. The terms "wet code" and "dry code" come from smart contracts inventor Nick Szabo. *See* Nick Szabo, *Wet Code and Dry*, UNENUMERATED (Aug. 24, 2008), http://unenumerated.blogspot.com/2006/11/wet-code-and-dry.html [https://perma.cc/B8QB-YRMC].

40. *See infra* Sections IV.A, IV.B.

41. These represent the four "things that regulate" in Lessig's model. *See* CODE VERSION 2.0, *supra* note 22.

on regulation of cryptocurrencies.[42] While there are many challenges to resolve about the legal treatment of Bitcoin and its progeny, the more fundamental question is whether they can displace traditional law entirely. They cannot. Part II of this Article describes the technical features of the blockchain architecture and explains why it is seeing such rapid adoption. Part III shows how blockchain-based systems go wrong when they stray too far from legal enforcement. Part IV describes the emerging governance hybrids that connect cryptocurrency code with law. Part V concludes. The blockchain could indeed become a transformative technology for business, government, and society on the scale of the Internet, but only if it reaches accommodations with law.

II. HERE COMES THE BLOCKCHAIN

In just a few years, Bitcoin and the blockchain have sparked extraordinary excitement and activity in the technology world.[43] Leading figures equate them

42. *See generally* Jerry Brito et al., *Bitcoin Financial Regulation: Securities*, *Derivatives*, *Prediction Markets, and Gambling*, 16 COLUM. SCI. & TECH. L. REV. 144 (2015); Danton Bryans, *Bitcoin and Money Laundering: Mining for an Effective Solution*, 89 IND. L.J. 441 (2014); Joshua J. Doguet, *The Nature of the Form: Legal and Regulatory Issues Surrounding the Bitcoin Digital Currency System*, 73 LA. L. REV. 1119 (2013); Paul H. Farmer, Jr., *Speculative Tech: The Bitcoin Legal Quagmire & the Need for Legal Innovation*, 9 J. BUS. & TECH. L. 85 (2014); Andres Guadamuz & Chris Marsden, *Blockchains and Bitcoin: Regulatory Responses to Cryptocurrencies*, 20 FIRST MONDAY (2015), http://firstmonday.org/ojs/index.php/fm/article/view/6198/5163 [https://perma.cc/QXC8-E5NU]; Nikolei M. Kaplanov, *Nerdy Money: Bitcoin*, *the Private Digital Currency*, *and the Case Against Its Regulation*, 25 LOY. CONSUMER L. REV. 111 (2012); Trevor I. Kiviat, *Beyond Bitcoin: Issues in Regulating Blockchain Transactions*, 65 DUKE L.J. 569 (2015); Stephen T. Middlebrook & Sarah Jane Hughes, *Regulating Cryptocurrencies in the United States: Current Issues and Future Directions*, 40 WM. MITCHELL L. REV. 813 (2014); Carla L. Reyes, *Moving Beyond Bitcoin to an Endogenous Theory of Decentralized Ledger Technology Regulation: An Initial Proposal*, 61 VILL. L. REV. 191 (2016); Kevin V. Tu & Michael W. Meredith, *Rethinking Virtual Currency Regulation in the Bitcoin Age*, 90 WASH. L. REV. 271 (2015); Wright & De Filippi, *supra* note 23; Ruoke Yang, *When Is Bitcoin a Security Under U.S. Securities Law?*, 18 J.L. TECH. & POL'Y 99 (2013).

43. *See, e.g.*, Marc Andreessen, *Why Bitcoin Matters*, N.Y. TIMES (Jan. 21, 2014), http://dealbook.nytimes.com/2014/01/21/why-bitcoin-matters [https://perma.cc/RK6A-M5J4]; Amy Cortese, *Blockchain Technology Ushers in the "Internet of Value"*, CISCO (Feb. 10, 2016), https://newsroom.cisco.com/feature-content?type=webcontent&articleId=1741667 [https://perma.cc/KX8X-P4V8]; Jerry Cuomo, *How Businesses and Governments Can Capitalize on Blockchain*, FORBES (Mar. 17, 2016), http://www.forbes.com/sites/ibm/2016/03/17/how-businesses-and-governments-can-capitalize-on-blockchain/ [http://archive.is/HYwR7] (calling the blockchain a "revolutionary technology"); Reid Hoffman, *Reid Hoffman: Why the Blockchain Matters*, WIRED (May 15, 2015), https://www.wired.co.uk/article/bitcoin-reid-hoffman [https://perma.cc/VU4U-LV5M]; MARK WALPORT, U.K. GOV'T OFFICE FOR SCI., DISTRIBUTED LEDGER TECHNOLOGY: BEYOND BLOCK CHAIN 4 (2016), https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/492972/gs-16-1-distributed-ledger-technology.pdf [https://perma.cc/X4C3-HQPV] ("In distributed ledger technology, we may be witnessing one of those potential explosions of creative potential that catalyse exceptional levels of innovation."); UBS, BUILDING THE TRUST ENGINE 5

with nothing less than a new Internet: a radically powerful, open, and distributed platform that will enable a vast economy of new and enhanced digital services.[44] Some say they could prevent future financial crises[45] or even "transform business, government, and society."[46] Others suggest the blockchain heralds a new form of private law, which may supersede government-based institutions.[47] For libertarians, these technologies represent economic activity outside the bounds of sovereign state control. For progressives, they promise to undermine entrenched private power. For others, they are simply a huge opportunity to make money or solve problems.

The magic of distributed ledgers is to make certain activities trustworthy without the need to trust anyone in particular.[48] Billionaire entrepreneur and

(2016), https://www.ubs.com/microsites/blockchain-report/en/home/ [https://perma.cc/H66V-Q8DH] ("Like many of our peers, we at UBS believe the blockchain is a potentially transformative technology . . . ."); ARVIND NARAYANAN ET AL., BITCOIN AND CRYPTOCURRENCY TECHNOLOGIES 2 (2016) ("Optimists claim that Bitcoin will fundamentally alter payments, economics, and even politics around the world."); DON TAPSCOTT & ALEX TAPSCOTT, BLOCKCHAIN REVOLUTION: HOW THE TECHNOLOGY BEHIND BITCOIN IS CHANGING MONEY, BUSINESS, AND THE WORLD 8–9 (2016); Popper, *supra* note 13 ("A new report from the World Economic Forum predicts that the underlying technology introduced by the virtual currency Bitcoin will come to occupy a central place in the global financial system.").

44. *See* Cadie Thompson, *Bitcoin Transformative as the Web*, *Venture Capitalist Says*, CNBC (Jan. 28, 2014), http://www.cnbc.com/2014/01/28/bitcoin-transformative-as-the-web-venture-capitalist-says.html [https://perma.cc/K5D7-ET6W]; Scott Rosenberg, *How Bitcoin's Blockchain Could Power an Alternate Internet*, WIRED (Jan. 13, 2015), https://www.wired.com/2015/01/how-bitcoins-blockchain-could-power-an-alternate-internet/ [https://perma.cc/29VW-KCPD]; Peter Spence, *Bitcoin Revolution Could Be the Next Internet, Says Bank of England*, TELEGRAPH (Feb. 25, 2015), http://www.telegraph.co.uk/finance/currency/11434904/Bitcoin-revolution-could-be-the-next-Internet-says-Bank-of-England.html [https://perma.cc/WX5U-38EM]; Daniel Folkinshteyn, Mark Lennon & Tim Reilly, *A Tale of Twin Tech: Bitcoin and the WWW*, 10 J. STRATEGIC & INT'L STUD. 82 (2015).

45. *See Bring on the Blockchain Future*, BLOOMBERG (June 6, 2016), http://www.bloomberg.com/view/articles/2016-06-06/bring-on-the-blockchain-future [https://perma.cc/5D6X-JFDP] ("The blockchain really could change the world . . . .").

46. Tapscott & Tapscott, *supra* note 2. Going even further, Skype co-founder Jaan Tallinn believes the blockchain can be used to overcome the tragedy of the commons and solve some of humanity's greatest challenges. *See* Rebecca Burn-Callander, *Skype Inventor Jaan Tallinn Wants to Use Bitcoin Technology to Save the World*, TELEGRAPH (June 20, 2016), http://www.telegraph.co.uk/business/2016/06/20/skype-inventor-jaan-tallinn-wants-to-use-bitcoin-technology-to-s/ [https://perma.cc/GNT3-4KWM].

47. *See* Wright & De Filippi, *supra* note 23, at 40–41; Michael Abramowicz, *Cryptocurrency-Based Law*, 58 ARIZ. L. REV. 359, 404 (2016).

48. *See* Joshua A.T. Fairfield, *BitProperty*, 88 S. CAL. L. REV. 805, 814 (2015) ("Bitcoin creates a manipulation-resistant solution to the problem of trust—a way of providing verification without centralization and its attendant risks and costs.").

venture capitalist Reid Hoffman calls this "trustless trust."[49] Blockchain proponents argue that costly mechanisms of intermediation and legal enforcement can be dispensed with. Instead of trusting banks and courts and governments, proponents suggest that we can trust math and computation, in the form of open-source cryptographic protocols.

A. HOW THE BLOCKCHAIN WORKS

The blockchain was first described in a paper distributed online in late 2008 by someone (or some group) using the pseudonym Satoshi Nakamoto.[50] Many of the concepts in Nakamoto's paper were familiar to cryptographers, but the system was implemented in a novel and elegant way to create a private, decentralized form of digital cash, called bitcoin. The Bitcoin network was implemented in open source software in 2009 and has been operating ever since. Exchanges around the world sprung up to trade bitcoin for fiat currencies such as dollars or euros. A collection of developers works to improve the Bitcoin software—Nakamoto was last heard from in 2011—and "miners" around the world provide computing power to secure the network. One bitcoin now costs thousands of dollars to purchase on an exchange.[51]

Bitcoin was the first production of the blockchain system. In subsequent years, many others were created, differing from the Bitcoin network in various ways. Some of them, like Ripple, which facilitates cross-border currency exchange between financial services providers, are optimized for specific purposes.[52] Others, like Ethereum, are designed as general-purpose platforms.[53] These other blockchains still have a native cryptocurrency token that can be traded, but it is a means to an end. The primary purpose of their currencies is to incentivize activity. Another class of systems, called permissioned ledgers, have no cryptocurrency because they are designed for private groups of firms to share information or transactions. The leading two examples are Hyperledger—an open source project under the auspices of the

49. *See* Hoffman, *supra* note 43.

50. *See generally* Satoshi Nakamoto, Bitcoin: A Peer-To-Peer Electronic Cash System (unpublished manuscript), https://bitcoin.org/bitcoin.pdf [https://perma.cc/QGW4-W934] (last visited Aug. 18, 2018). Nakamoto's identity has never been conclusively identified.

51. *Bitcoin (USD) Price*, COINDESK, https://www.coindesk.com/price/ [https://perma.cc/X2FK-F47J] (last visited Sept. 3, 2018).

52. *See* Nathaniel Popper, *The Rush to Coin Virtual Money with Real Value*, N.Y. TIMES (Nov. 11, 2013), https://dealbook.nytimes.com/2013/11/11/the-rush-to-coin-virtual-money-with-real-value [https://perma.cc/5LMD-QNXC].

53. *See* Nathaniel Popper, *Move Over, Bitcoin. Ether Is the Digital Currency of the Moment*, N.Y. TIMES (June 19, 2017), https://www.nytimes.com/2017/06/19/business/dealbook/ethereum-bitcoin-digital-currency.html [https://perma.cc/26SC-PH9P].

Linux Foundation[54]—and the R3 financial services consortium.[55]

All the platforms use slightly different technical approaches. They make design tradeoffs to optimize for factors such as performance, decentralization, regulatory compliance, anonymity, security, and functionality. In the future, there may be only one blockchain of consequence, or there may be dozens of significant platforms and thousands of minor ones. Bitcoin today remains the biggest platform in terms of market capitalization of tokens, but its dominance appears to be waning. In twenty years, it could be worth several trillion dollars, or zero. However the market develops, the blockchain architecture that Bitcoin pioneered is now well-established. All systems of this type incorporate three primary features: distributed ledgers, consensus, and smart contracts.

1. Ledgers

A ledger is a record of accounts. Perhaps the most familiar ledgers are those used for double-entry bookkeeping, the foundation of accounting. However, ledgers are not limited to recording debits and credits for corporate balance sheets.[56] Real estate markets could not exist without land title registries. Democracy requires ledgers tallying votes. Copyright depends on both public and private records tracking the registration and assignment of rights. The modern firm depends on ledgers not just for its financials but for the relationships among its internal agents and external partners, as well as its supply chain, back-office, and customer-facing activities. Sociologists such as Max Weber and Werner Sombart argue that double-entry bookkeeping was the foundation of modern capitalism.[57]

---

54. *See* Cade Metz, *Tech and Banking Giants Ditch Bitcoin for Their Own Blockchain*, WIRED (Dec. 17, 2015), https://www.hyperledger.org/news/2015/12/17/wired-tech-and-banking-giants-ditch-bitcoin-for-their-own-blockchain [https://perma.cc/KP2E-Z4BN].

55. *See* Paul Vigna, *Blockchain Firm R3 CEV Raises $107 Million*, WALL ST. J. (May 23, 2017, 6:37 PM), https://www.wsj.com/articles/blockchain-firm-r3-raises-107-million-1495548641 [https://perma.cc/G2CR-AXJP].

56. *See* Dominic Frisby, *In Proof We Trust*, AEON (Apr. 21, 2016), https://aeon.co/essays/how-blockchain-will-revolutionise-far-more-than-money [https://perma.cc/S6NH-YELA] (explaining the broader potential of distributed ledgers for all kinds of record-keeping).

57. *See* MAX WEBER, GENERAL ECONOMIC HISTORY 276 (Frank H. Knight trans., 1927) ("[T]he most general presupposition for the existence of . . . present-day capitalism is that of rational capital accounting . . . ."); WERNER SOMBART, DER MODERNE KAPITALISMUS 23 (1916) ("[C]apitalism and double entry bookkeeping are absolutely indissociable; their relationship to each other is that of form to content"); *see also* Quinn DuPont & Bill Maurer, *Ledgers and Law in the Blockchain*, KING'S REV. (June 23, 2016), http://kingsreview.co.uk/articles/ledgers-and-law-in-the-blockchain/ [https://perma.cc/VA6B-W34B] (detailing the significance of ledgers and the implications for the blockchain). Going back even further, many of the earliest surviving written documents from antiquity, in Mesopotamian cuneiform, are ledgers of commercial transactions. *See* HANS

A blockchain is a kind of distributed ledger.[58] It is "distributed" in that there is no master copy. Any participant in the network can maintain an instantiation of the ledger, yet be confident it matches all the others. Venture capitalist Albert Wenger calls blockchains logically centralized (there is only one ledger), but organizationally decentralized (many entities maintain copies of that ledger).[59] Computers directly participating in a blockchain network, often called full nodes, are in constant communication to remain synchronized. Maintaining that synchronization, called consensus, is the hard part, because there is no canonical master copy.

Centralized ledgers have their own difficulties. If one entity keeps the master ledger, it becomes a single point of failure for the system. If, on the other hand, each organization or computer keeps its own ledger (as with most corporate financial records), every transaction is recorded independently at least twice. Whenever, for example, a company pays a vendor or a bank cashes a check from another bank's customer, their ledgers must be synchronized after the fact through a process of reconciliation. This introduces complexity, delay, and possibilities for error. Until the blockchain came along, these difficulties were thought to be necessary evils.[60]

2. Consensus

At the heart of the Bitcoin architecture is a set of software protocols often called Nakamoto Consensus.[61] Consensus means that participants in a network

---

J. NISSEN, PETER DAMEROW & ROBERT K. ENGLUND, ARCHAIC BOOKKEEPING: EARLY WRITING AND TECHNIQUES OF ECONOMIC ADMINISTRATION IN THE ANCIENT NEAR EAST (Paul Larsen trans., 1993).

58. *See* WALPORT, *supra* note 43; PAUL VIGNA & MICHAEL J. CASEY, THE AGE OF CRYPTOCURRENCY: HOW BITCOIN AND DIGITAL MONEY ARE CHALLENGING THE GLOBAL ECONOMIC ORDER 124 (2015). Not all distributed ledgers are structured as blockchains. For example, the Corda system for financial agreements between regulated banks uses a different data structure. *See* Richard Gendal Brown, *Introducing R3 Corda(TM): A Distributed Ledger Designed for Financial Services*, GENDAL.ME (Apr. 5, 2016), https://gendal.me/2016/04/05/introducing-r3-corda-a-distributed-ledger-designed-for-financial-services/ [https://perma.cc/ES9K-8J9A]. Blockchains are the most common approach, especially for public ("permissionless") systems, so that is the term used here.

59. Albert Wenger, *Bitcoin: Clarifying the Foundational Innovation of the Blockchain*, CONTINUATIONS (Dec. 15, 2014), http://continuations.com/post/105272022635/bitcoin-clarifying-the-foundational-innovation-of [https://perma.cc/8JXA-WRGN].

60. There has been extensive research and significant deployment of distributed database systems for many years. However, these systems generally assume all nodes will be controlled by a single company. They focus on the danger nodes that will fail, whereas blockchain systems protect against untrustworthy nodes that attack the system. *See* Rajesh Nair, *Why Aren't Distributed Systems Engineers Working on Blockchain Technology?*, PAXOS ENGINEERING BLOG (Aug. 1, 2017), https://eng.paxos.com/why-arent-distributed-systems-engineers-working-on-blockchain-technology [https://perma.cc/JG64-NRDC].

61. *See* Joseph Bonneau et al., *SoK: Research Perspectives and Challenges for Bitcoin and*

have confidence that their ledgers are both accurate and consistent.[62] Without a robust means of ensuring consensus, any Bitcoin participant could, for example, spend the same bitcoin multiple times (known as the double-spend problem), or claim it had more currency than it really did. The trouble with most approaches to consensus on digital systems is that it is easy to create multiple fake accounts. This is known as the "Sybil attack."[63] Even if most real users are honest, an attacker can dominate the network and impose its own false consensus on the system.

Nakamoto's response to Sybil attacks cleverly combined cryptographic[64] techniques with insights from game theory.[65] As a baseline, all Bitcoin transactions are cryptographically signed. It can be proven mathematically that only the possessor of the relevant private key (a secret string of letters and numbers) could have sent the relevant message. Next, Bitcoin and other consensus-based systems replace trust in individual actors with trust in networks of actors. Those actors—called "miners" in Bitcoin—are responsible for verifying transactions.[66] Anyone can be a miner. Even if some of them are untrustworthy, the system holds so long as the majority is honest.[67] In

Cryptocurrencies, *in* PROCEEDINGS OF THE 36TH IEEE SYMPOSIUM ON SECURITY AND PRIVACY 104, 106–07 (2015); Nick Szabo, *The Dawn of Trustworthy Computing*, UNENUMERATED (Dec. 11, 2014), http://unenumerated.blogspot.com/2014/12/the-dawn-of-trustworthy-computing.html [https://perma.cc/Z7YL-F5XB].

62. For a more detailed discussion of the importance of consensus, see Casey Kuhlman, *What Are Ecosystem Applications*, MONAX (June 5, 2016), https://monax.io/2016/06/05/ecosystem-applications/ [https://perma.cc/MQ93-SKVU] ("The problem that blockchain technology solves is not electronic P2P cash, nor is it settlement latency, it is the problem of attribution and ordering of inbound events . . . .").

63. *See generally* John R. Douceur, *The Sybil Attack*, *in* PEER-TO-PEER SYSTEMS 251 (2002).

64. Cryptography is the use of mathematical techniques for secure communications. Encryption is a subset of cryptography used to make information unreadable without possession of a key. Bitcoin's core protocols use no encryption. Transactions are public but secure.

65. Others described similar approaches in the same time frame, although none achieved consensus in as robust a way. For example, cryptographer Nick Szabo propounded a system called Bit Gold. *See generally* Nick Szabo, *Liar-Resistant Government*, UNENUMERATED (May 7, 2009), http://unenumerated.blogspot.com/2009/05/liar-resistant-government.html [https://perma.cc/5BEZ-LM7T].

66. This approach is analogous to the republican form of government epitomized by the United States. Instead of empowering a king, power is decentralized to the people, who express it through voting. To mediate the potential for factionalism and mob rule, voters exercise power indirectly, by electing representatives. *See Introduction to Hyperledger Business Blockchain Design Philosophy and Consensus*, 1 HYPERLEDGER ARCHITECTURE 4 (2017) [hereinafter HYPERLEDGER], https://www.hyperledger.org/wp-content/uploads/2017/08/HyperLedger_Arch_WG_Paper_1_Consensus.pdf [https://perma.cc/Y97U-8XGP] (describing the advantages of voting-based systems for verifying transactions).

67. Security researchers have identified scenarios in which dishonest miners that control more than one-third of the computing power in the network could attack the system

Nakamoto's version, miners compete to validate groups of Bitcoin transactions, called "blocks."[68] The winner for each block earns a reward.

Sybil attacks are the major concern for such a system: if it is easy and rewarding to be untrustworthy, someone probably will be. Hence the second cryptographic technique in Bitcoin: proof of work.[69] Bitcoin's system requires miners who wish to earn the reward to solve cryptographic puzzles involving one-way functions known as "hashes."[70] Solutions require massive and growing computing power, which is sufficiently expensive to deter Sybil attacks.[71] The benefits of cheating are less than the costs. Other consensus systems include proof of stake, in which validators risk losing their existing currency if they attempt to cheat, and a variety of voting and lottery algorithms such as the Ripple Consensus Protocol, which do not require such "skin in the game."[72]

---

successfully. *See* Ittay Eyal & Emin Gün Sirer, *Majority Is Not Enough: Bitcoin Mining Is Vulnerable*, *in* FINANCIAL CRYPTOGRAPHY & DATA SECURITY 436, 438 (2014).

68. *The Magic of Mining*, ECONOMIST (Jan. 10, 2015), https://www.economist.com/business/2015/01/08/the-magic-of-mining [https://perma.cc/9EQB-MA2W]; ANDREAS M. ANTONOPOULOS, MASTERING BITCOIN: UNLOCKING DIGITAL CRYPTOCURRENCIES (2014); *see also* Kevin Werbach, *Bitcoin Is Gamification*, MEDIUM (Aug. 5, 2014), https://medium.com/@kwerb/bitcoin-is-gamification-e85c6a6eea22 [https://perma.cc/VX6X-2B8Z] (explaining the significance of the motivational system to Bitcoin).

69. *See* NARAYANAN ET AL., *supra* note 43, at 61. Not every blockchain implements proof of work in the same manner as Bitcoin. For example, Ethereum uses a modified algorithm so that miners do not gain an advantage from using custom chips known as ASICs. Other distributed ledger platforms such as Ripple and Tendermint do not employ proof of work at all, but instead implement alternate mechanisms to achieve the same goal. *See* Bonneau et al., *supra* note 61. It remains to be seen whether these other consensus protocols are as successful as Bitcoin's proof of work. *See id.*

70. A hash function takes some input string (such as a document file) and turns it into an output string—the hash—with a specified length. Although in theory multiple input strings could map to the same hash, cryptographic hash spaces are sufficiently large that such "collisions" are infinitesimally rare. It is easy to compute the hash function of any file. An input string will produce the same output string every time. However, there is no known way to go from a hash back to the input string other than trial and error. *See* NARAYANAN ET AL., *supra* note 43, at 23–24. Miners must attempt truly vast numbers of hashes to find the one that produced the specified output. *See id.* at 61–68.

71. The level of difficulty automatically adjusts as more computing power is added to the network. The Bitcoin network today is thousands of times more powerful than the world's 500 most powerful supercomputers combined. *See* Laura Shin, *Bitcoin Production Will Drop by Half in July, How Will that Affect the Price?*, FORBES (May 24, 2016), http://www.forbes.com/sites/laurashin/2016/05/24/bitcoin-production-will-drop-by-half-in-july-how-will-that-affect-the-price/ [https://perma.cc/XU65-KANQ]. The computing power involved is so vast that it raises concerns about the environmental impacts of the electricity required to power and cool the data centers involved. *See* TAPSCOTT & TAPSCOTT, *supra* note 43, at 259–63.

72. *See* HYPERLEDGER, *supra* note 66. There are various tradeoffs in the choice of consensus algorithm. For example, "permissioned" systems such as Ripple and Hyperledger

Consensus affirms the integrity both of each individual transaction and of the ledger as a whole. It does so by aggregating transactions together into blocks.[73] The proof of work system is tuned dynamically to generate a valid solution to the hashing puzzle for a block roughly once every ten minutes.[74] Each block thus validated is cryptographically signed with the hash of the prior block, creating an immutable chain of sequential blocks. The longest chain represents the consensus state of the system.[75] Only an attacker with a majority of total computing power in the entire network (known as a 51-percent attack) can "fork" the longest chain with a fraudulent block.[76] Doing so becomes increasingly difficult for blocks earlier in the chain.

A public blockchain, such as Bitcoin's, records all transactions on the network and is totally transparent to all participants.[77] Not only are the contents of the Bitcoin blockchain available to all, but the software involved is open source and freely available.[78] Bitcoin is also designed to be censorship- and tamper-resistant. There is no central control point or network that a government could manipulate or block. And once a transaction is recorded, it cannot easily be changed, a property known as immutability. For example, user A could send some bitcoin to user B, and then user B could send some or all of it back, but there is no way for user A, the miners, or anyone else to reverse the initial transfer.[79]

Fabric only allow approved nodes to join the network. This largely prevents Sybil Attacks and improves transaction throughput but limits the scope of decentralization and the game -theoretic security guarantees of the Bitcoin approach. The security and performance of most consensus algorithms at scale are still open research questions. One approach might come to dominate, although it is more likely that different consensus systems will be used based on the category of application.

73. *See* NARAYANAN ET AL., *supra* note 43, at 88–90.

74. *See id.* at 65.

75. *See id.* at 59. More precisely, it is the chain with the most proof of work.

76. Although as noted above, some research suggests an attacker with over one-third of the mining power could disrupt the network. *See supra* note 67.

77. Users are identified on the blockchain through digital signatures, so the real-world identity of the parties to a transaction may be impossible to determine. For those desiring further anonymity, there are ways to break up transactions in order to obscure large transfers.

78. Alec Liu, *Who's Building Bitcoin? An Inside Look at Bitcoin's Open Source Development*, MOTHERBOARD (May 7, 2013), https://motherboard.vice.com/en_us/article/9aa4ae/whos-building-bitcoin-an-inside-look-at-bitcoins-open-source-development [https://perma.cc/2A7U-N9KS].

79. The Bitcoin system records transactions, not asset holdings, using a mechanism called Unspent Transaction Output (UTXO). This makes it difficult to "walk back" account balances even if a majority of miners change their Bitcoin software to unwind the validation of a particular block. Some other cryptocurrency platforms are easier to "hard fork" so as to revert prior transactions, because they operate on accounts rather than UTXO. The Ethereum community did so in July 2016 to address the theft of currency from a crowdfunding platform called The DAO. *See infra* notes 135–141. Such steps are controversial, because they call into

These features suggest an inherent openness and decentralization more like the early Internet than today's more-controlled online environment.[80] They seem to fulfill the dreams of some Internet pioneers for a technology space that was not, in Lawrence Lessig's terminology, regulable.[81]

The final key piece of Nakamoto Consensus is the game-theoretic or psychological dimension: Why will miners bother? Proof of work is expensive, literally. It requires specialized computing hardware and large quantities of electricity. Miners will not be incentivized sufficiently out of altruism. Nakamoto's solution was supremely elegant. The miner who successfully validates a block receives a reward in a valuable currency: Bitcoin. This solves several problems, including how currency enters the money supply without a central bank. New bitcoin is only created through the reward mechanism, at a rate that declines over time.[82] Miners thus act purely out of self-interest, but in doing so, they fulfill a socially beneficial role.

Bitcoin is thus both the output and input of the system. One could equally well describe it as a trust infrastructure designed to support a digital currency, or a digital currency designed to support a trust infrastructure.

3. *Smart Contracts*

Distributed ledgers are active, not passive. In other words, they do not simply record information passed to them. They are part of a consensus system, so they must ensure that recorded transactions are actually completed to match the consensus.[83] For Bitcoin, that means the system self-enforces financial transfers.[84] Someone cannot initiate a transaction promising to send bitcoin to another and then renege; the synchronization that reconciles and

question the censorship resistance and immutability of public blockchains.

80. *See* Andreessen, *supra* note 43; Morgen E. Peck, *The Future of the Web Looks a Lot Like the Bitcoin Blockchain*, IEEE SPECTRUM (July 1, 2015), http://spectrum.ieee.org/computing/networks/the-future-of-the-web-looks-a-lot-like-bitcoin [https://perma.cc/Y2VT-D8V7].

81. Lawrence Lessig, *Deja Vú All Over Again: Thinking Through Law & Code*, *Again*, VIMEO (Dec. 11, 2015), https://vimeo.com/148665401 [https://perma.cc/C7DM-66XY].

82. Hence the analogy to mining for previous resources in the physical world. Eventually the block rewards will drop to zero. At that point, the number of Bitcoins in circulation will be fixed at twenty-one million. Nakamoto envisioned that voluntary transaction fees paid to miners by those seeking validation would gradually replace the rewards as adoption of the Bitcoin system grew. This remains to be seen.

83. Bitcoin actually uses a scripting language for transactions, meaning that every transfer is actually running software code on the blockchain. *See* NARAYANAN ET AL., *supra* note 43, at 79–88 (describing the Bitcoin scripting language and some applications beyond basic cash transfers).

84. To be precise, the blockchain records challenges and responses that either create or destroy Bitcoins, rather than transfers of discrete tokens as such. *See* NARAYANAN ET AL., *supra* note 43, at 75–76.

completes the transfer is part of the process. This mechanism is known as a "smart contract."[85] Both the specification of rights and obligations, and the execution of that contractual agreement, occur through the platform.

The idea of smart contracts was introduced independently from blockchains, and well before Bitcoin was developed.[86] Its practical relevance was limited, however, until Nakamoto's synthesis. Bitcoin takes advantage of smart contracts to execute transactions, and smart contracts take advantage of Bitcoin's distributed ledger to operate with autonomy. Smart contracts are essentially autonomous software agents.[87] With smart contracts, a distributed ledger becomes functionally a distributed computer. The same consensus algorithms that allow each node to have an identical copy of the ledger allow it to perform identical computations in the identical order. While Bitcoin operates based on smart contracts, it strictly limits their capabilities to basic fund transfers for security.

The most prominent platform for smart contracts today is Ethereum, which launched in 2015.[88] Ethereum offers a Turing-complete programming language, meaning that in theory, any application that runs on a conventional computer can be executed on the distributed computer of its consensus network.[89] Ethereum makes it easy for developers to code new kinds of

85. *See* TIM SWANSON, GREAT CHAIN OF NUMBERS: A GUIDE TO SMART CONTRACTS, SMART PROPERTY AND TRUSTLESS ASSET MANAGEMENT 15–30 (2014). *See generally* Nick Szabo, *Formalizing and Securing Relationships on Public Networks*, 2 FIRST MONDAY (1997) [hereinafter Szabo, *Public Networks*], http://ojphi.org/ojs/index.php/fm/article/view/548/469 [https://perma.cc/U2L2-B34P]; Nick Szabo, *The Idea of Smart Contracts*, *in* NICK SZABO'S ESSAYS, PAPERS, AND CONCISE TUTORIALS (1997) [hereinafter Szabo, *Smart Contracts*], http://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html [https://perma.cc/YED2-ACVP]; Werbach & Cornell, *supra* note 25.

86. *See* Szabo, *Smart Contracts*, *supra* note 85.

87. *See generally* Vitalik Buterin, *A Next-Generation Smart Contract and Decentralized Application Platform*, GITHUB (Aug. 20, 2018), https://github.com/ethereum/wiki/wiki/White-Paper [https://perma.cc/5DTZ-NEZ2].

88. *See generally id.*; Popper, *supra* note 53; D.J. Pangburn, *The Humans Who Dream of Companies that Won't Need Us*, FAST COMPANY (June 19, 2015), http://www.fastcompany.com/3047462/the-humans-who-dream-of-companies-that-wont-need-them [https://perma.cc/9GRQ-SPKS]; Jim Epstein, *Here Comes Ethereum, an Information Technology Dreamed Up By a Wunderkind 19-Year-Old That Could One Day Transform Law, Finance, and Civil Society*, REASON (Mar. 19, 2015), http://reason.com/blog/2015/03/19/here-comes-ethereum-an-information-techn [https://perma.cc/FH6S-4ZSS]; Tina Amirtha, *Meet Ether, the Bitcoin-Like Cryptocurrency That Could Power the Internet of Things*, FAST COMPANY (May 21, 2015), http://www.fastcompany.com/3046385/meet-ether-the-bitcoin-like-cryptocurrency-that-could-power-the-Internet-of-things [https://perma.cc/NY3K-SBBY].

89. The overhead of distributed consensus means that such applications may run far slower than on a single computer or a cloud computing platform such as Amazon Web Services.

applications on top, just as the web and various infrastructure tools such as application servers were the foundation for Google, Amazon, and eBay. Ether, Ethereum's cryptocurrency, is now easily the second most valuable after bitcoin.[90]

Generalized smart contracts platforms are the foundation for decentralized applications, or "DApps."[91] As with the financial uses of the blockchain, many decentralized applications mimic existing centralized applications. IPFS and Storj provide decentralized cloud storage, comparable to Dropbox or Apple's iCloud;[92] Steemit provides an open discussion platform, similar to Reddit;[93] Commuterz supports decentralized ridesharing, comparable to Uber or Lyft.[94]

Other DApps are more novel. For example, Goldman Sachs suggests that the blockchain might facilitate distributed markets for electricity.[95] Users could sell excess power generated through rooftop solar cells to local utilities. Such transactions are limited today due to the overhead of managing the volume of potential transactions among large numbers of individual customers and electric utilities.[96] A distributed ledger could track those transactions without the overhead of a central system. Goldman Sachs estimates a two and one-half to seven-billion-dollar annual opportunity in the U.S. electricity industry by enabling distributed markets.[97]

A distributed autonomous organization, or "DAO," is an ambitious

90. *See* Nathaniel Popper, *Ethereum, a Virtual Currency, Enables Transactions That Rival Bitcoin's*, N.Y. TIMES (Mar. 27, 2016), http://www.nytimes.com/2016/03/28/business/dealbook/ethereum-a-virtual-currency-enables-transactions-that-rival-bitcoins.html?_r=1 [https://perma.cc/28VK-BQKQ].

91. One site lists nearly two thousand decentralized application projects at various stages of development as of August 2018. *See* STATE OF THE DAPPS, http://dapps.ethercasts.com/ [https://perma.cc/6N9A-LWME] (last visited Sept. 3, 2018).

92. *See* Gautham, *Storj, the New Decentralized Cloud Storage Platform Goes Live*, NEWSBTC (Apr. 10, 2016), http://www.newsbtc.com/2016/04/10/storj-new-decentralized-cloud-storage-platform-goes-live/ [https://perma.cc/DA2K-SDMP]; Ian Allison, *How IPFS Is Reimagining the Internet*, NEWSWEEK (Oct. 21, 2016), http://www.newsweek.com/how-ipfs-reimagining-Internet-512566 [https://perma.cc/6XGR-L54T].

93. *See* Andrew McMillen, *The Social Network Doling Out Millions in Ephemeral Money*, WIRED (Oct. 4, 2017), https://www.wired.com/story/the-social-network-doling-out-millions-in-ephemeral-money/ [https://perma.cc/R9CX-AWQ3].

94. COMMUTERZ, http://commuterz.io [https://perma.cc/E3HY-GSAE] (last visited Sept. 3, 2018).

95. *See* Schneider et al., *supra* note 15, at 4.

96. A trial program of this sort is underway in Brooklyn, New York. *See* Aviva Rutkin, *Blockchain-Based Microgrid Gives Power to Consumers in New Nork*, NEW SCIENTIST (March 9, 2016), https://www.newscientist.com/article/2079845-blockchain-based-microgrid-gives-power-to-consumers-in-new-york/ [https://perma.cc/H9M6-D2DU].

97. *See* Schneider et al., *supra* note 15, at 4.

category of decentralized applications.[98] In a DAO, the standard corporate arrangements of equity, debt, and corporate governance could be encoded as a series of smart contracts.[99] Investors could contribute funds in the form of a cryptocurrency, and the distributed application would handle payment of salaries, dividends, proxy votes, and so forth. "The DAO," the crowdfunding system that was catastrophically hacked, was styled as the first implementation of the concept.[100]

B. REASONS FOR ADOPTION

If distributed ledgers did not solve real-world problems, they would be of interest only to cryptographers or philosophers. Some adoption is driven by ideological desire to circumvent state control. For the most part, however, the entrepreneurs, established corporations, major financial institutions, and governments investigating the blockchain today are pursuing tangible benefits. The blockchain's two primary value propositions are avoiding dependence on central actors and creating universal truth among untrusting parties.

1. Avoiding Problems with Central Authority

In 2016, authorities in Buenos Aires, Argentina forbade credit card companies from processing transactions for the ride-hailing company Uber, which was violating local regulations. Xapo, which offers a bitcoin-based debit card, was able to circumvent the ban[101] because it did not require a local connection to a traditional payment processor. Uber could continue operating

98. *See* Vitalik Buterin, *Bootstrapping A Decentralized Autonomous Corporation: Part I*, BITCOIN MAG. (Sept. 19, 2013), https://bitcoinmagazine.com/7050/bootstrapping-a-decentralized-autonomous-corporation-part-i/ [https://perma.cc/DZQ5-EUL5]; MELANIE SWAN, BLOCKCHAIN: BLUEPRINT FOR A NEW ECONOMY (2015); Wright & De Filippi, *supra* note 23, at 17, 31–32.

99. The legal status of such virtual corporations as well as that of their investors, developers, and beneficiaries, is an open question. *See* Shawn Bayern, *Of Bitcoins, Independently Wealthy Software, and the Zero-Member LLC*, 108 NW. U.L. REV. 1483, 1496–97 (2014); Tanaya Macheel, *The DAO Might Be Groundbreaking, But Is It Legal?*, AM. BANKER (May 19, 2016), http://www.americanbanker.com/news/bank-technology/the-dao-might-be-groundbreaking-but-is-it-legal-1081084-1.html [https://perma.cc/MND9-KMS2]; Peter Van Valkenburgh, *DAOs: the Internet Is Weird Again, and These Are the Regulatory Issues*, COIN CENTER (Jun. 2, 2016), https://coincenter.org/entry/daos-the-Internet-is-weird-again-and-these-are-the-regulatory-issues [https://perma.cc/JQ47-52JZ].

100. *See supra* notes 24–32 and accompanying text.

101. *See* Jamie Redman, *Uber Thriving in Argentina Once Again Thanks to Bitcoin*, BITCOIN NEWS (July 9, 2016), https://news.bitcoin.com/uber-thriving-argentina-bitcoin/ [https://perma.cc/8AL3-M6AS]; Joel Valenzuela, *Uber Switches to Bitcoin in Argentina After Govt Blocks Uber Credit Cards*, COINTELEGRAPH (July 6, 2016), http://cointelegraph.com/news/uber-switches-to-bitcoin-in-argentina-after-govt-blocks-uber-credit-cards [https://perma.cc/88VX-MVU6].

despite the regulatory objections.

Whether routing around authority in this way is desirable or not depends on one's perspective. In at least some cases, however, avoiding dependence on central actors is clearly a valuable thing. This is the reason, for example, that Latin American countries have seen some of the most aggressive adoption of bitcoin for payments.[102] Citizens there are skeptical of the government and the financial system, after calamitous experiences with hyperinflation and currency devaluation. Bitcoin, perceived as immune from the vicissitudes of politics and the demands of international lenders, seems like a safer option. One of Bitcoin's value propositions is to serve as a residual store of value in many ways superior to gold, which today is a $7 trillion asset class.[103]

The same dynamic applies when central private actors are involved. Trust imposes risk. There is always the danger that the one you trust turns out to be untrustworthy. Investors in Bernie Madoff's Ponzi scheme lost their money because they trusted the wrong investment manager.[104] Law, regulation, and insurance are all mechanisms to limit such risks. The Madoff scenario is the exception rather than the rule, at least in the United States. For those at the mercy of loan sharks, payday lenders, or extortionate money transfer agents, however, the blockchain offers an appealing alternative.

Even when trusted authorities are not fundamentally untrustworthy, they are single points of failure that can be exploited. For example, access to websites is secured through cryptographic certificates that verify the user is connected to the correct site, with no interference in the middle. Those certificates are issued by central certificate authorities. In 2011, DigiNotar, a Dutch certificate authority, was hacked.[105] Fraudulent certificates were issued which allowed attackers to intercept and redirect traffic between users and Google's Gmail service. The damage was limited because Google and web browser vendors acted quickly to invalidate the fraudulent certificates, but the incident shows the risk of centralized systems.[106] Projects such as Namecoin,

---

102. *See* Sonny Singh & Alberto Vega, *Why Latin American Economies Are Turning to Bitcoin*, TECHCRUNCH (Mar. 16, 2016), https://techcrunch.com/2016/03/16/why-latin-american-economies-are-turning-to-bitcoin/ [https://perma.cc/6H9C-MB29].

103. *See* Nathan Lewis, *Gold or Bitcoin? Gold and Bitcoin*, FORBES (June 30, 2017), https://www.forbes.com/sites/nathanlewis/2017/06/30/gold-or-bitcoin-gold-and-bitcoin/#3a6f0fe33e4b [http://perma.cc/GGT9-FDMQ].

104. A leading biography of Madoff is subtitled, "Bernie Madoff and the Death of Trust." DIANA B. HENRIQUES, THE WIZARD OF LIES (2011).

105. *See* Kim Zetter, *DigiNotar Files for Bankruptcy in Wake of Devastating Hack*, WIRED (Sept. 20, 2011), https://www.wired.com/2011/09/diginotar-bankruptcy/ [https://perma.cc/EG8W-XE99].

106. *See* Josephine Wolff, *How a 2011 Hack You've Never Heard of Changed the Internet's Infrastructure*, SLATE (Dec. 21, 2016), http://www.slate.com/articles/technology/future_tense/2016/12/how_the_2011_hack_of

Ethernet Name Service, and Blockstack are creating security frameworks for access to online resources that use blockchains to avoid this problem.[107]

Moreover, all intermediaries impose costs. When an intermediary is a private company, it expects to generate revenue in return for the value it provides. Google charges advertisers for exposing them to large number of users and for precisely targeting advertisements. Google's advertising revenues, now in the tens of billions of dollars annually, represent a direct cost of intermediation.[108] If the search engine advertising marketplace could exist without Google at the center, it would not have to bear those costs. And as the number of intermediaries multiplies, so do the costs. Search engine optimization firms, for example, are intermediaries that piggyback on Google. Those providers charge for their services, and Google has to expend resources to prevent excessive gaming of its search results.[109]

Intermediaries also shape markets to serve their own interests. They may restrict conduct or fail to innovate if they do not see the benefits. In 2017, the European Union imposed a $2.7 billion fine on Google for manipulating online shopping search results to benefit its affiliates.[110] In essence, being the trusted heart of a community conveys a kind of monopoly power. For example, many websites use Facebook's "social login" service to verify credentials for their users. It is more convenient to hand off to Facebook the process of identity management because Facebook is such a powerful trusted intermediary for online social interactions. Social login, however, entrenches Facebook's control.[111] It gives Facebook access to data from outside its own boundaries and raises barriers to competition. Companies in Facebook's central position for long periods of time tend to, like any monopoly, raise prices and slow innovation. This monopoly is essentially cashing in on the

_diginotar_changed_the_Internet_s_infrastructure.html [https://perma.cc/LA57-EP2P].

107. *See* Michael del Castillo, *Blockstack Releases Blockchain-Powered, Tokenized Internet Browser*, COINDESK (May 23, 2017), https://www.coindesk.com/blockstack-blockchain-decentralized-browser/ [https://perma.cc/3GEJ-98ZG].

108. *See* Rani Molla, *Google Leads the World in Digital and Mobile Ad Revenue*, RECODE (July 24, 2017), https://www.recode.net/2017/7/24/16020330/google-digital-mobile-ad-revenue-world-leader-facebook-growth [https://perma.cc/YRR4-ZKDM] (stating that Google was expected to make $73.8 billion in net digital ad sales in 2017).

109. *See* David Kesmodel, *Sites Get Dropped By Search Engines After Trying to 'Optimize' Rankings*, WALL ST. J. (Sept. 22, 2015), https://www.wsj.com/articles/SB11271416697874492 5 [https://perma.cc/XWF4-49KY].

110. *See* Mark Scott, *Google Fined Record $2.7 Billion in E.U. Antitrust Ruling*, N.Y. TIMES (June 27, 2017), https://www.nytimes.com/2017/06/27/technology/eu-google-fine.html [https://perma.cc/P574-QUA8].

111. *See generally* Julie E. Cohen, *Law for the Platform Economy*, 51 U.C. DAVIS L. REV. 133 (2017) (discussing how digital platforms have exploited the Internet environment to aggregate power).

gains it created. To the others in the network, however, the effect is a tax, and sometimes a significant one.

2. Shared Truth

The second appealing aspect of the blockchain model is its potential for speed and efficiency. At first glance, this sounds odd. Bitcoin validates a block roughly every ten minutes, and currently has a theoretical limit of seven transactions per second.[112] This is quite a small number: the Visa credit card network handles up to 10,000 transactions in the same period.[113] The overhead of synchronizing the distributed ledger is so great that, according to one estimate by cryptographer Nick Szabo, the process operates 10,000 times slower than a conventional computer.[114]

Yet there is a hidden advantage of removing the need to trust the specific actors with which you interact. Trust is not transitive. I may trust my bank, but that does not mean I trust yours. For me to cash your check, our banks must enter into their own trust relationship. With many thousands of financial institutions processing billions of transactions across hundreds of jurisdictions, this pairwise structure quickly bogs down. Or more accurately, it works only with huge inefficiencies and transaction costs. Much of the time, transaction costs become further value-extraction opportunities for the trusted actors. Hence the massive revenues for providers of remittances and credit cards.[115] The complexity of reconciling transactions between many interconnected trusted parties adds delay to the process. Stock trades, for example, typically settle after two days (a standard known as T+2).[116] This ties up capital that could otherwise be deployed more efficiently.

In the traditional system, every actor is individually responsible for keeping its ledger in sync with the virtual consensus. Yet it only has visibility (limited at that) into its direct partners. With the blockchain, every new block reconciles

112. *See* NARAYANAN ET AL., *supra* note 43, at 134 (validation every ten minutes), 95 (seven transactions per second limit).

113. *See* Timothy B. Lee, *Bitcoin Needs to Scale By a Factor of 1000 to Compete with Visa. Here's How to Do It*, WASH. POST (Nov. 12, 2013), https://www.washingtonpost.com/news/the-switch/wp/2013/11/12/bitcoin-needs-to-scale-by-a-factor-of-1000-to-compete-with-visa-heres-how-to-do-it/ [https://perma.cc/QXZ7-HJWC]. New technologies may greatly increase the speed of the Bitcoin transaction network. *See* Romain Dillet, *Blockchain Open Sources Thunder Network, Paving the Way for Instant Bitcoin Transactions*, TECHCRUNCH (May 16, 2016), https://techcrunch.com/2016/05/16/blockchain-open-sources-thunder-network-paving-the-way-for-instant-bitcoin-transactions/ [https://perma.cc/M4FX-DSRV].

114. *See* Szabo, *supra* note 61.

115. The remittance market generates $38 billion in annual fees worldwide. *See* TAPSCOTT & TAPSCOTT, *supra* note 43, at 183.

116. *See* SEC, *SEC Adopts T+2 Settlement Cycle for Securities Transaction*, (Mar. 22, 2017), https://www.sec.gov/news/press-release/2017-68-0 [https://perma.cc/7DAW-Y7YH].

its transactions across the entire system. Each participant knows that its copy of the ledger is identical to every other. The truth—or what computer scientists call the network's "state"—is shared among them. Thus, while it may take much longer to record each transaction, the network as a whole updates more rapidly. Because this occurs through one synchronized process, rather than a potentially large number of separate transactions, costs may be significantly lower.[117] Goldman Sachs estimates that the blockchain could save $11–$12 billion annually in settlement and reconciliation fees, just for securities transactions.[118]

Bitcoin and other blockchain-based systems do face significant scaling challenges. The Bitcoin development community is engaged in debates about mechanisms such as increasing the size of each block to improve performance.[119] By contrast, the existing financial system has been optimized over an extended period for robust operation at massive scale. Predictions that the blockchain will soon sweep away the banking system as we know it are thus exaggerated. However, the potential for faster and more efficient reconciliation is a key reason major financial institutions are actively exploring permissioned blockchains.

Finally, there are different ways to structure a distributed ledger.[120] On public blockchains, such as Bitcoin and Ethereum, anyone can operate a mining node and maintain a copy of the shared ledger. Because there is no way to verify the integrity of network participants, elaborate protocols such as Nakamoto Consensus and high-overhead distribution of all transaction information are necessary. Permissioned ledgers can do away with those limitations and operate more efficiently, but at the cost of reintroducing elements of central control.[121] Different use cases will call for different solutions.

As far as the world of distributed ledgers has come since the launch of Bitcoin in 2009, these are still early days. Vlad Zamfir, one of the core developers of Ethereum, created a stir when he tweeted in March 2017, "Ethereum isn't safe or scalable. It is immature experimental tech. Don't rely

117. *See* BUILDING THE TRUST ENGINE, *supra* note 43, at 9, 18.

118. *See* Schneider et al., *supra* note 15, at 5.

119. *See* NARAYANAN ET AL., *supra* note 43, at 98.

120. *See* Nolan Bauerle, *What Is the Difference Between Public and Permissioned Blockchains?*, COINDESK, https://www.coindesk.com/information/what-is-the-difference-between-open-and-permissioned-blockchains/ [https://perma.cc/A8E4-EE4N] (last visited Sept. 3, 2018); *see generally*, Swanson, *supra* note 85 at 4–5.

121. *See* Richard Gendal Brown, *Towards Deeper Collaboration in Distributed Ledgers: Thoughts on Digital Asset's Global Synchronisation Log*, GENDAL.ME (Jan. 24, 2017), https://gendal.me/2017/01/24/towards-deeper-collaboration-in-distributed-ledgers-thoughts-on-digital-assets-global-synchronisation-log/ [https://perma.cc/Q9BP-V8K2].

on it for mission critical apps unless absolutely necessary!"[122] He is correct. And not just for Ethereum. There are so many well-founded efforts underway, so many significant use cases, so much support from major enterprises, and so much capital flowing in that the blockchain is clearly more than a fad. Exactly how it will develop, though, remains uncertain. The blockchain offers tremendous potential benefits. It also poses very serious risks and public policy challenges.

III. LEDGERS MEET LAW

Distributed ledger technology gives users confidence that they can store and exchange valuable assets. However, that is not the same thing as finding a person or institution trustworthy.[123] If the blockchain entirely replaces reliance on people, companies, and governments with reliance on software code and cryptography, it will produce distrust. And this dissonance has real consequences. When the beautiful math of Satoshi Nakamoto meets the messy reality of real-world implementation, it turns out to be not so perfect. The limitations of the blockchain create problems when it is positioned as the sole guarantor of enforcement. Fortunately, there is a mechanism that can work alongside the technical trust architecture of the blockchain. That mechanism is the law.

A. WHAT COULD POSSIBLY GO WRONG?

The Bitcoin consensus ledger has not been successfully hacked since its very early days. Sophisticated attackers have tried. Given that bitcoin is literally money, the ledger represented a bank vault storing over $300 billion at the 2017 peak. The best evidence that blockchain technology works is that this massive target remained secure. However, as successful as Bitcoin and other major blockchain systems have been in avoiding major security failures, the security of the cryptocurrencies is not a foregone conclusion. And as

122. Vlad Zamfir (@VladZamfir), TWITTER (Mar. 4, 2017, 4:40 AM), https://twitter.com/vladzamfir/status/838006311598030848?lang=en [https://perma.cc/Z94J-VNDB]. Zamfir felt the need to explain himself the next day in a longer post. *See* Vlad Zamfir, *About My Tweet from Yesterday.*., MEDIUM (Mar. 5, 2017), https://medium.com/@Vlad_Zamfir/about-my-tweet-from-yesterday-dcc61915b572 [https://perma.cc/P6BL-ECND].

123. Agreement does not necessarily presume trust. An insight of game theory is that even non-communicating parties may converge on common points by independently choosing the most likely or familiar option. *See* THOMAS C. SCHELLING, THE STRATEGY OF CONFLICT 54–55 (1960). The creators of both smart contracts and Ethereum make reference to these Schelling Points. *See* Szabo, *Public Networks*, *supra* note 85; Vitalik Buterin, *SchellingCoin: A Minimal-Trust Universal Data Feed*, ETHEREUM BLOG (Mar. 28, 2014), https://blog.ethereum.org/2014/03/28/schellingcoin-a-minimal-trust-universal-data-feed/ [https://perma.cc/ZHA6-WSH9].

circumstances change, there is no guarantee it will continue. According to a group of leading researchers in 2015, "[w]e do not yet have sufficient understanding to conclude with confidence that Bitcoin will continue to work well in practice . . . ."[124]

Think of a blockchain network as a series of concentric circles. In the middle is the ledger, secured through robust decentralized consensus. At the next layer are the smart contracts, the software code that direct transactions on the network. Outside that are edge service providers like exchanges and wallet services, which interface between cryptocurrencies and the traditional world. Finally, there are coins that DApps and others sell directly to users. Each has weaknesses, but they are different weaknesses.

1. Trusting Ledgers

Blockchain-based systems are vulnerable. At the most general level, they depend on modern cryptographic techniques. Basic vulnerabilities in these mechanisms cannot be ruled out, especially with advances in computing power. Quantum computers, for example, might be able to break encryption methods that the most powerful conventional computers cannot crack.[125] If such flaws exist, however, they will apply at least as strongly to the existing online transactional systems, which rely on the same cryptography. And the blockchain world has attracted some of the world's foremost experts in cryptography, who are working actively to prevent such failures. A more likely danger is flawed implementation of cryptographic techniques, such as reliance on random number generators that are not actually random. Blockchain technology, like any system built on computer code, is not perfect. There have been significant bugs discovered in the open source Bitcoin code, although they were addressed prior to any lasting damage.

More serious vulnerabilities relate to the mining or proof of work process. Nakamoto's solution for consensus is remarkably robust, but it can be overcome by a 51% attack.[126] If someone controls more than half of the mining power in the network, they can validate blocks of their choosing, even if they involve double-spending. Bitcoin relies on the difficulty of amalgamating such enormous processing power. Today, that would be equivalent to several hundred of the world's fastest supercomputers, running

124. Bonneau et al., *supra* note 61, at 104.

125. *See First Quantum-Secured Blockchain Technology Tested in Moscow*, MIT TECH. REV. (June 6, 2017), https://www.technologyreview.com/s/608041/first-quantum-secured-blockchain-technology-tested-in-moscow/ [https://perma.cc/B554-SYE8].

126. While the 51% attack is the most widely-discussed scenario, security researchers have identified several other potential attack vectors against Bitcoin. *See* Bonneau et al., *supra* note 61, at 110–12.

non-stop.[127]

Nonetheless, because most mining is now handled through pools in which many participants aggregate their activity, it is not inconceivable that a pool could cross the threshold.[128] The danger of a 51% attack increases when mining network power decreases.[129] That tends to occur when the price of bitcoin falls, reducing the incentives for miners, or at the "halving" points when the algorithm automatically reduces the award to slow the flow of new currency into the system.[130] Other blockchain platforms such as Ripple use consensus approaches that do not involve mining rewards, and Ethereum plans to migrate to an alternate approach called "proof-of-stake."[131] However, these techniques have their own limitations and have survived less real-world exposure than Bitcoin.[132] And while permissioned blockchains, which have an additional layer of centralized trust over the participants in the network, may not need to worry about 51% of the attacks, they face more of the traditional information security concerns of centralized systems.

Different levels of security and robustness will be needed depending on the context. A bank will be more concerned about certain risks than a merchant engaged in a small-value consumer transaction. Medical records on the blockchain will have different risk profiles than supply chain records for diamonds. Such variation is not unique to the blockchain; it is part of trust and security with existing centralized systems. Given the novelty of distributed

127. *See* Reuven Cohen, *Global Bitcoin Computing Power Now 256 Times Faster Than Top 500 Supercomputers, Combined!*, FORBES (Nov. 28, 2013), https://www.forbes.com/sites/reuvencohen/2013/11/28/global-bitcoin-computing-power-now-256-times-faster-than-top-500-supercomputers-combined/ [https://perma.cc/7SYQ-E6YH].

128. *See* Jon Matonis, *The Bitcoin Mining Arms Race: GHash.io and the 51% Issue*, COINDESK (July 17, 2014), http://www.coindesk.com/bitcoin-mining-detente-ghash-io-51-issue/ [https://perma.cc/VK55-XRCQ] ("A forum for discussing these issues is critical to maintaining the integrity of the bitcoin network, as its overall health depends on smooth mining operations with a minimum amount of . . . players capable of executing a 51% attack.").

129. More generally, public blockchains must maintain sufficient scale and network effects to remain viable. *See* Fairfield, *supra* note 48, at 823–25.

130. *See* Fredrick Reese, *As Bitcoin Halving Approaches, 51% Attack Question Resurfaces*, COINDESK (July 6, 2016), http://www.coindesk.com/ahead-bitcoin-halving-51-attack-risks-reappear/ [https://perma.cc/UNV5-4YZU] (describing concerns about a 51% attack after the halving in July 2016). Adjusting to the expected scarcity, the price of Bitcoin tends to increase around these halving points, but equilibrium is not guaranteed. Other blockchains do not necessarily use the halving mechanism, but all those employing proof of work face the concern about incentives when the price of the cryptocurrency falls.

131. *See* Vlad Zamfir, *Introducing Casper "the Friendly Ghost"*, ETHEREUM BLOG (Aug. 1, 2015), https://blog.ethereum.org/2015/08/01/introducing-casper-friendly-ghost/ [https://perma.cc/6YH9-3JJA].

132. *See generally* Bonneau et al., *supra* note 61 (describing open research questions for cryptocurrencies).

ledgers, though, it will take some time to sort out the appropriate security models.

2. Trusting Smart Contracts

The next layer beyond the blockchain itself is the smart contract code that implements transactions.[133] A smart contract can have errors and security flaws, like any other software code. And indeed, vulnerabilities have already been identified in high-profile Ethereum smart contracts.[134] Errors or security exploits in smart contracts are particularly dangerous because the blockchain directly carries value or rights to assets. There are significant practical limitations in replacing human enforcement of agreements with software running on the blockchain. Things simply do not always go according to plan.

The collapse of The DAO, noted in the introduction, illustrated this vulnerability.[135] The transactions siphoning off funds were valid smart contracts according to the rules of The DAO, so they were subject to the same immutable execution as any others. Ethereum had to employ a "hard fork" to return the stolen Ether.[136] A hard fork creates two incompatible chains.[137] Although most miners adopted the new software without incident, the move was not without controversy.[138] It meant that Ethereum transactions were not truly immutable, or immune from centralized interference. It also raised concerns about what might happen when governments or other central authorities became concerned about records stored on distributed ledgers.[139]

133. *See* Ari Juels, et al., *The Ring of Gyges: Investigating the Future of Criminal Smart Contracts*, *in* PROCEEDINGS OF THE 2016 ACM SIGSAC CONFERENCE ON COMPUTER AND COMMUNICATIONS SECURITY 283, 285–87 (2016).

134. *See* Zikai Alex Wen & Andrew Miller, *Scanning Live Ethereum Contracts for the "Unchecked-Send" Bug*, HACKING, DISTRIBUTED (June 16, 2016), http://hackingdistributed.com/2016/06/16/scanning-live-ethereum-contracts-for-bugs/ [https://perma.cc/35M6-AGKL].

135. *See supra* notes 25–31 and accompanying text; *see generally* Jentzsch, *supra* note 25, at 1 (describing "the first implementation of Decentralized Autonomous Organization (DAO) code to automate organizational governance and decision-making.").

136. *See* Paul Vigna, *Ethereum Gets Its Hard Fork*, *and the 'Truth' Gets Tested*, WALL ST. J. (July 20, 2016), http://blogs.wsj.com/moneybeat/2016/07/20/ethereum-gets-its-hard-fork-and-the-truth-gets-tested/ [https://perma.cc/56WJ-8ANL].

137. Miners of one chain do not recognize the validity of blocks mined by the other clients, and vice versa, even though they may otherwise use exactly the same protocols. *See* Bonneau et al., *supra* note 61, at 112.

138. *See* Stan Higgins, *Will Ethereum Fork? DAO Attack Prompts Heated Debate*, COINDESK (June 17, 2016), http://www.coindesk.com/will-ethereum-hard-fork/ [https://perma.cc/8VD3-LUD2]; Michael del Castillo, *Specter of Ethereum Hard Fork Worries Australian Banking Group*, COINDESK (June 29, 2016), http://www.coindesk.com/spectre-ethereum-hardfork-worries-anz-banking-group/ [https://perma.cc/8GTJ-Y23U].

139. Ethereum is a public blockchain, like Bitcoin. Permissioned blockchains do not provide the same assurance of non-interference because access is limited to identified parties.

The assumption was that the pre-fork blockchain would wither away. That did not happen. A small but growing group of miners kept running the old software,[140] evidently dissatisfied with the Ethereum Foundation's willingness to break the ledger's immutability. A group of developers agreed to manage the software going forward, under the name "Ethereum Classic" (ETC). Ethereum core developer Peter Szilagyi summarized the experience with profound understatement: "The DAO has shown us that it takes much more effort to write smart contracts than we originally anticipated . . . ."[141]

The fallout of The DAO hack is still being felt. In May 2017, QuadrigaCX, the largest cryptocurrency exchange in Canada, announced it had lost Ether worth over $14 million.[142] There was no foul play involved. And the Ether did not disappear. It was permanently inaccessible because of an erroneous smart contract. The cause, it turned out, was a bug in code that was added to split Ethereum and Ethereum Classic balances after the hard fork.[143] Cryptographic immutability is a powerful thing. That power makes blockchain-based systems trustworthy, but it also leads to problems that code itself cannot solve.

3. Trusting Edge Services

Even when value is stored in decentralized systems, it is often accessed through centralized edge services. In theory, anyone can operate a full node with a complete copy of the blockchain on a public network such as Bitcoin or Ethereum. In practice, the technical and hardware requirements are prohibitive for ordinary users. Virtually all consumers use wallet services such as Coinbase or Xapo. Users must trust the wallet services in the same manner as a bank. A wallet provider stores the private cryptographic keys for its customers, which allows them to access their cryptocurrency through a standard username and password. However, if the wallet provider is hacked, the keys are vulnerable. And given the novelty of cryptocurrencies, many are inexperienced or unsophisticated. As Nick Szabo tweeted, "Bitcoin is the most secure financial network on the planet. But its centralized peripheral companies are among the most insecure."[144]

140. *See* Vigna, *supra* note 32.

141. Peter Szilagyi, *DAO Wars: Your Voice on the Soft-Fork Dilemma*, ETHEREUM BLOG (June 24, 2016), https://blog.ethereum.org/2016/06/24/dao-wars-youre-voice-soft-fork-dilemma/ [https://perma.cc/CSZ7-2WVY].

142. *See* Stan Higgins, *Ethereum Client Update Issue Costs Cryptocurrency Exchange $14 Million*, COINDESK (June 2, 2017), https://www.coindesk.com/ethereum-client-exchange-14-million/ [https://perma.cc/PJ2M-ER4W].

143. *See id.*

144. Nick Szabo (@NickSzabo4), TWITTER (June 17, 2017, 6:05 PM), https://twitter.com/NickSzabo4/status/876244539211735041 [https://perma.cc/6ZE9-XYDR].

A particular point of vulnerability lies in exchanges that trade cryptocurrencies for dollars or other government-backed fiat money. In proof of work systems like Bitcoin, the only two ways to obtain cryptocurrency are through mining or by exchanging with someone else. Most users are not miners, so at some point they have to buy their bitcoin. Exchanges make markets among various cryptocurrencies and dollars or other fiat currencies. Unfortunately, the exchanges sometimes prove insufficient to the task.

In 2014, the most prominent Bitcoin exchange, Mt. Gox, collapsed after hackers stole a significant amount of currency, then worth over $400 million.[145] Another major exchange, Bitfinex, was hacked in 2016, losing cryptocurrency valued at nearly $70 million.[146] And in early 2018, a Japanese exchange reported a theft of half a billion dollars of cryptocurrency.[147] Although there has been some effort to require licensing of cryptocurrency exchanges, the global nature of the market means many exchanges are effectively unregulated.[148]

Edge providers can also decide whether to police transactions. A Bitcoin transaction for drugs, gambling, or a contract killing will be processed on the ledger in the same way as one for a pizza. There is no bank or payment processor that governments can pressure to block the transaction. If, however, a user operates through an edge provider, it can be subjected to legal enforcement. That might be difficult depending on where the service is located and whether it hides identities of its management. It is not impossible, as the Silk Road takedown and similar law enforcement actions illustrated.[149]

145. *See* Robin Sidel, Eleanor Warnock & Takashi Mochizuki, *Almost Half a Billion Worth of Bitcoins Vanish*, WALL ST. J. (Feb. 28, 2014) https://www.wsj.com/articles/mt-gox-to-hold-news-conference-1393579356 [https://perma.cc/C8E5-AG7A]; Robert McMillan, *The Inside Story of Mt. Gox, Bitcoin's $460 Million Disaster*, WIRED (Mar. 3, 2014), http://www.wired.com/2014/03/bitcoin-exchange/ [https://perma.cc/6T7N-XD2H].

146. Josh Horwitz, *The $65 Million Bitfinex Hack Shows That It Is Impossible to Tell a Good Bitcoin Company From a Bad One*, QUARTZ (Aug. 9, 2016), https://qz.com/753958/the-65-million-bitfinex-hack-shows-that-it-is-impossible-to-tell-a-good-bitcoin-company-from-a-bad-one/ [https://perma.cc/XE5K-EYUP].

147. Evelyn Cheng, *Japanese Cryptocurrency Exchange Loses More Than $500 Million to Hackers*, CNBC (Jan. 26, 2018), https://www.cnbc.com/2018/01/26/japanese-cryptocurrency-exchange-loses-more-than-500-million-to-hackers.html [https://perma.cc/DTA3-J2W3].

148. This may be changing. Bitfinex, one of the largest exchanges, announced in August 2017 that it would stop serving U.S. customers after the SEC suggested that it might be liable for trading tokens that are incorrectly failed to register as securities upon issuance. *See* Wolfie Zhao, *Bitfinex to Bar US Customers from Exchange Trading*, COINDESK (Aug. 11, 2017), https://www.coindesk.com/bitfinex-suspends-sale-select-ico-tokens-citing-sec-concerns/ [https://perma.cc/GE9L-GS2S].

149. *See supra* note 20 and accompanying text.

4. *Trusting Coin Issuers*

A final source of vulnerability involves the services built on top of blockchains. If these are centralized systems, they have the same issues as exchanges and other edge services. If they are decentralized, they operate based on vulnerable smart contracts. Many of them add an additional element, however, by offering their own cryptocurrency coins directly to users. These token sales create a further level of risk.

Just as a company can sell stock to the public to finance its operations, a distributed ledger network or DApp can sell cryptocurrency tokens. By analogy to an initial public offering (IPO) of stock, these token sales are often called initial coin offerings (ICOs). What rights the tokens grant depends on the associated smart contracts.[150] The first ICO was Mastercoin, a system for creating new application-specific "colored" coins on top of the Bitcoin network. Its 2013 ICO generated $5 million in bitcoin. Ethereum followed in 2014, raising approximately $18 million in bitcoin a year before it mined its first block of Ether. As the price of bitcoin surged in 2017, there was a flurry of ICOs raising over $5 billion.[151] The encrypted messaging application Telegram launched an ICO in early 2018 designed to raise $2 billion by itself, which is more than Google raised in its initial public offering.[152]

Token sales could offer a new means of funding innovative technologies that circumvents the limitations of the traditional venture capital model. They also offer an almost perfect way to cheat people out of their money.[153] Token purchasers today are generally contributing money to blockchain-based projects with virtually no way to guarantee they get anything in return, and very limited information about risks. The projects may be scams. The teams involved may try, but fail to build the application they described. The offering may be structured with unfair terms toward ordinary purchasers relative to the development team or their associates. The application may fail to attract activity, depressing the value of the token.

Such risks overlap very significantly with those that produced the 1933 Securities Act and 1934 Securities Exchange Act.[154] Securities and Exchange

150. Something they generally do not offer are the equity ownership rights in a corporate entity associated with stocks. Token holders own a share of the value of the network, but not a formal claim on any assets.

151. *See supra* note 10.

152. *See* Mike Orcutt, *Telegram's ICO: Give Us $2 Billion and We'll Solve All of Blockchain's Problems*, MIT TECH. REV. (Jan. 25, 2018), https://www.technologyreview.com/s/610055/telegrams-ico-give-us-2-billion-and-well-solve-all-of-blockchains-problems/ [https://perma.cc/U68E-32WR].

153. *See* Popper, *supra* note 38.

154. *See* Securities Act of 1933, Pub. L. No. 73-22, 48 Stat. 74 (1933) (codified as amended at 15 U.S.C. §§ 77a et seq. (1982 & Supp. IV 1986)); *see also* SEC, *Registration Under the Securities*

Commission (SEC) rules require all securities offerings to be registered—triggering detailed disclosure and antifraud requirements—or subject to a specific exemption. Yet to this point, virtually no ICOs have attempted to register.[155]

The foundational principle of securities regulation is disclosure. Investment involves risks, and no one is entitled to legal protection against a bad decision. However, without regulation, there is a strong information asymmetry between investors, especially retail investors, and investment promoters. Token sales represent a sudden, grand experiment in *caveat emptor* securities offerings, targeting retail investors all around the world.[156] Given all the uncertainties and technical complexities of blockchain technology, most investors are unlikely to understand what they are getting into, even with extensive financial disclosure. Without disclosure, they are at the mercy of the offerors and investment promoters. A system that invites abuse on this scale will inevitably lead to scams.[157]

The potential abuses of ICOs do not mean that the entire enterprise should be banned or that all such offerings must be fit into the strictures of U.S. securities laws. Not all token offerings are necessarily securities, for one thing. An SEC investigation concluded that The DAO tokens should have been classified as securities and therefore subject to the SEC's rules for public

Act of 1933, https://www.sec.gov/fast-answers/answersregis33htm.html (last visited Sept. 3, 2018) [https://perma.cc/4G4W-X7Q5]; Securities Exchange Act of 1934, Pub. L. No. 73-291, § 78(b), 48 Stat. 881 (1934) (codified as amended at 15 U.S.C. §§ 78a–qq (1982 & Supp. IV 1986)).

155. A number of ICOs limit their offerings to wealthy "accredited" investors, which qualifies them for one of the registration exemptions under SEC rules. These are often structured using a framework called the Simple Agreement for Future Tokens (SAFT), under which purchasers hope to re-sell their tokens to the public once the application becomes operational. *See* Juan Batiz-Benet et al., *The SAFT Project: Toward a Compliant Token Sale Framework*, PROTOCOL LABS COOLEY (Oct. 2. 2017), https://saftproject.com/static/SAFT-Project-Whitepaper.pdf [https://perma.cc/AAX3-PE64]. The SEC has not passed judgment on the legality of this arrangement.

156. U.S. securities laws only apply when securities are marketed or sold to U.S. citizens. However, most other major jurisdictions have similar disclosure obligations. As the SEC affirmed in its investigative report on The DAO token offering, a foreign entity or even a virtual organization selling tokens to Americans is still subject to its rules. *See* SEC, REPORT OF INVESTIGATION PURSUANT TO SECTION 21(A) OF THE SECURITIES EXCHANGE ACT OF 1934: THE DAO 1–2 (2017) [hereinafter SEC DAO INVESTIGATION] https://www.sec.gov/litigation/investreport/34-81207.pdf [https://perma.cc/9X5T-DB44].

157. *See* David Z. Morris, *The Rise of Cryptocurrency Ponzi Schemes*, ATLANTIC (May 31, 2017), https://www.theatlantic.com/technology/archive/2017/05/cryptocurrency-ponzi-schemes/528624/ [https://perma.cc/4JH4-23AH].

offerings.[158] However, it stopped short of declaring that all tokens would be.[159] Regulators around the world need to consider how to draw lines around token offerings that protect investors without chilling innovation. Without such efforts, investors will be hurt. And failures of ICOs could undermine confidence in the market as a whole. Blockchain effectively implements a decentralized security model, but this does not obviate the need for legal and regulatory involvement.

B. CODE VS. LAW

1. "No Sovereignty Where We Gather"

In the late 1990s, it was fashionable to see the Internet as a technology that undermined regulation through decentralization. Electronic Frontier Foundation co-founder John Perry Barlow's 1996 Declaration of the Independence of Cyberspace thundered that governments "have no sovereignty where we gather" and do not "possess any methods of enforcement we have true reason to fear."[160] This view captured the spirit of a cyber-libertarian movement that included not just traditional skeptics of state power, but also innovation-focused developers and legal experts. Scholars wrote of online communities freed from the strictures of territorial sovereigns.[161] Some cyber-activists went so far as to claim an abandoned British naval platform in international waters as the independent territory of Sealand, believing they could operate Internet servers completely outside of legal restrictions.[162]

158. *See* SEC DAO INVESTIGATION, *supra* note 156. The SEC concluded The DAO was an unauthorized, unregistered securities offering, but chose not to impose sanctions, "based on the conduct and activities known to the Commission at this time." *Id.* at 1. This apparently referred to the fact that, thanks to the hard fork, all investors received their money back, and The DAO subsequently shut down.

159. In February 2018 testimony before the Senate Banking Committee, SEC Chairman Jay Clayton stated that, "I believe every ICO I've seen is a security." However, he acknowledged that a token offering could conceivably be structured to avoid that classification. Jordan Pearson, *The SEC Is Mad About All These ICOs, Wants the Government to Regulate Cryptocurrency Trading*, MOTHERBOARD (Feb. 6, 2018), https://motherboard.vice.com/en_us/article/mb5anx/sec-regulate-cryptocurrency-icos-cftc-senate-hearing [https://perma.cc/59A7-LHJ3].

160. John Perry Barlow, *A Declaration of the Independence of Cyberspace*, ELECTRONIC FRONTIER FOUND. https://www.eff.org/cyberspace-independence [https://perma.cc/SF3L-Y7PX].

161. *See* David R. Johnson & David G. Post, *Law and Borders: The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1367 (1996) (discussing the need for new laws and legal institutions in Cyberspace that differ from those of the geographically-bound "real world").

162. *See* JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD 65 (Oxford Univ. Press, Inc., 2006), http://cryptome.org/2013/01/aaron-swartz/Who-Controls-Net.pdf

These visions of an unregulable cyberspace met the cold hard limits of reality. As Jack Goldsmith and Tim Wu explained in their 2006 book, *Who Controls the Internet*, governments around the world were able to impose their will on online activity.[163] Utopian initiatives like Sealand collapsed amid internal squab

bling, with little or no adoption.[164] China built a *Great Firewall* that allowed it to censor Internet traffic in and out of the country.[165] Geo-location technology allowed courts to impose sanctions on activity touching citizens of their jurisdictions.[166] Efforts to circumvent legal regimes, whether through peer-to-peer technology to hobble copyright enforcement or online gambling services located in island jurisdictions where the conduct was legal, were repeatedly shut down.[167] Authoritarian regimes discovered they could use the Internet as a tool for monitoring and repression.[168]

The Internet did represent something big and new. But the legal system was able to incorporate it, as it has incorporated every technology since at least the printing press. It turns out that while cyberspace is nowhere, the people and companies and systems that deliver Internet services are very much somewhere. There are any number of control points, from the Internet service and hosting providers that manage the flow of bits to the financial services firms that control the flow of money, which regulators can target to control online activity.[169] The Internet is a regulated space,[170] which is not to say, of course, that it is regulated the same way everywhere, or that online transactions are regulated identically to their offline analogues. Working through the practicalities of Internet regulation has been a twenty-year global process, with no end in sight. Yet a key point is incontestable: Internet regulation is not an oxymoron.

The blockchain rekindled the cyber-libertarian flame. There are two ways to frame a discussion about blockchain and law: *Can* these technologies be subject to legal and administrative oversight? And *should* they be? Many

---

[https://perma.cc/QSB5-G732].

163. *See id.* at 66.

164. *See id.*

165. *See id.* at 87–92.

166. *See id.* at 79–81.

167. *See id.* at 73–77.

168. *See generally* EVGENY MOROZOV, THE NET DELUSION (2011) (discussing the Internet's failed promise to aid the fight against authoritarianism, the global mindsets that allowed for it to fail, and policies that may be more successful).

169. *See* Jonathan Zittrain, *Internet Points of Control*, 44 B.C. L. REV. 653, 655–73 (2002) (discussing four different control points: the source, the source ISP, the destination, and the destination ISP).

170. Careful readers of Lawrence Lessig's *Code* knew this already. *See* CODE VERSION 2.0, *supra* note 22.

blockchain developers and advocates, especially those who cut their teeth on Bitcoin in its earlier years, see the answer to the second question as obvious, and the first nearly so. Cryptocurrency, they argue, was created as a solution to the problem of government oversight of value-based transactions. Satoshi Nakamoto's breakthrough was to invent money that escaped the prison of regulation. On this view, the decentralized architecture of consensus computing is a firewall against government intervention. The blockchain is not just immutable; it is "censorship resistant." No higher authority can command a blockchain to do something any more than it can order around the Internet. There is no *there* to regulate. Regulation and the blockchain are antithetical.

Proponents of distributed ledgers are taking up this banner. Wright and De Filippi draw a direct connection between the blockchain's "Lex Cryptographia" and the "Lex Informatica" of software code described in a foundational 1997 article by Fordham law professor Joel Reidenberg.[171] Self-executing smart contracts and decentralized autonomous organizations could, they argue, implement private legal systems without regard to territorial states, much as Bitcoin created a private global currency.

The experience of the past twenty years suggests that governments and powerful private institutions will not so easily be disintermediated.[172] Where they had a strong desire to regulate online activity, they found ways to do so. A similar pattern seems likely for activity on the blockchain, where the stakes are high enough, governments will not simply defer their authority. Even when transactions are entirely digital, peer-to-peer, cross-border, and cryptographically secured, providers and users on the network can be identified and subject to territorial legal obligations.[173] Moreover, outside of

171. *See* Wright & De Filippi, *supra* note 23, at 48–51; Joel Reidenberg, *Lex Informatica: The Formulation of Information Policy Rules through Technology*, 76 TEX. L. REV. 553 (1997). Wright and De Filippi define Lex Cryptographia as "rules administered through self-executing smart contracts and decentralized (and potentially autonomous) organizations." Wright & De Filippi, *supra* note 23, at 48. Reidenberg's "Lex Informatica" and Lessig's "West Coast code" both involve regulations through computer processes rather than laws enacted by governments.

172. *See generally* Kevin Werbach, *The Song Remains the Same: What Cyberlaw Might Teach the Next Internet Economy*, 69 FLA. L. REV. 887 (2017) (detailing how the vision of unregulated digital spaces failed); GOLDSMITH & WU, *supra* note 163, at 73–77 (showing how governments successfully imposed controls on online activity).

173. *See* Sarah Meiklejohn et al., *A Fistful of Bitcoins: Characterizing Payments Among Men With No Names*, *in* PROCEEDINGS OF THE 2013 CONFERENCE ON INTERNET MEASUREMENT, 127 (2013) (showing how seemingly anonymous Bitcoin transactions can be tied to users through forensic analytics). For further validation, consider the fate of Grokster, Kazaa, and Streamcast, the decentralized file-sharing services that were shut down when the U.S. Supreme Court declared them liable for contributory copyright infringement. *See* MGM Studios, Inc. v. Grokster, Ltd., 545 U.S. 913 (2005). The courts cannot entirely prevent distribution or use of open-source peer-to-peer software, but they can impose liability on companies making money from that software. There is an important difference between fringe activities of bands of

activity that is illegal or in need of extreme security, the incentives are lacking for most users to adopt custom legal systems where the existing ones are functional.[174] And as the creators of The DAO discovered, taking the place of law is not as easy as it may seem.

Wright and De Filippi acknowledge this fact. Yet they remain optimistic that the blockchain will dramatically expand the scope of regulation by code relative to other regulatory modalities.[175] Although ledgers based on Nakamoto Consensus are new, smart contracts and digital currencies are not. Nick Szabo described the mechanism for private regulation by smart contract in the early 1990s. There has not, however, been widespread adoption of cryptographically-based private law.

One reason is that immutable consensus appears to broach no half-measures. As one of the creators of OpenBazaar, a distributed eBay-like online marketplace based on cryptocurrency, put it, "if we allowed people to be accountable towards traditional courts and law, we're opening up [P]andora's box in letting governments interfere by making their own laws about what's 'cheating in a transaction' and what isn't, which leaves room for censorship . . . ."[176]

Many would cheer the use of blockchain technology by activists in China or North Korea to publish illegal pro-democracy manifestos, but it would not stop there. In a truly decentralized network, there is no way to impose limits on money transfers to known terrorists, transactions selling children into modern slavery, or laundering of funds known to be stolen. Universal freedom, at the limit, is tantamount to anarchy: Thomas Hobbes' war of all against all.[177]

The Augur prediction market illustrates this conundrum.[178] A prediction

---

users, and substantial markets that can scale for the mainstream.

174. There are similar problems with Josh Fairfield's appealing argument that smart contracts could be used to negotiate terms of service with online sites, returning power to users. *See* Josh A.T. Fairfield, *Smart Contracts*, *Bitcoin Bots*, *and Consumer Protection*, 71 WASH. & LEE L. REV. ONLINE 35, 46–49 (2014), http://scholarlycommons.law.wlu.edu/wlulr-online/vol71/iss2/3 [https://perma.cc/YA7N-6XBT]. Service providers that benefit from the current system of clickwrap terms of service have no incentive to adopt an alternate legal regime.

175. *See* Wright & De Filippi, *supra* note 23, at 40–44.

176. Dionysis Zindros, *Trust Is Risk: A Decentralized Trust System*, OPENBAZAAR (Aug. 1, 2017), https://www.openbazaar.org/blog/trust-is-risk-a-decentralized-trust-system/ [https://perma.cc/Q9QW-3P2E].

177. THOMAS HOBBES, LEVIATHAN: OR, THE MATTER, FORME, & POWER OF A COMMON-WEALTH ECCLESIASTICALL AND CIVILL (1676). The "war of all against all" has been defined as "people living in a state of nature, without a common power over them to keep them in awe, are in a state of war of every person against every other." Gregory S. Kavka, *Hobbes's War of All Against All*, 93 ETHICS 291, 292 (Jan. 1983).

178. *See* Pete Rizzo, *Augur Bets on Bright Future for Blockchain Prediction Markets*, COINDESK (Mar. 1, 2015) http://www.coindesk.com/augur-future-blockchain-prediction-market/

market allows participants to bet real money on the outcome of future events by "buying" or "selling" predictions like stocks.[179] Don and Alex Tapscott, in their best-selling book *Blockchain Revolution*, are enthusiastic about Augur's potential. After observing that centralized prediction markets such as Intrade were shut down, partly over concerns about "assassination markets and terrorism futures," they state briskly that this will not be a problem for the blockchain-based version: "Augur resolves the issue of unethical contracts by having a zero-tolerance policy for crime."[180]

That entirely begs the question: what is a crime, when laws governing the contracting parties, the developers, and the other participants in the prediction market disagree? Deciding what counts as unethical and what zero-tolerance means is even more difficult. The Augur developers do not control what questions can be posted on the prediction market. On Facebook or Reddit, administrators have the ability to delete illegal, offensive, or harassing material that users post. Not so on a distributed platform such as Augur. If someone lists a criminal contract such as one promoting an assassination, who is to stop it? There seems to be an inherent conflict between the innovative scope of something like Augur and legitimate public policy considerations.

2. Regulatory Debates

Regulatory skirmishes over blockchain-based systems are already being fought. Broadly speaking, there are three major types of controversies: illegality, classification, and legal validity.

The first involves using cryptocurrencies to break the law, or theft of cryptocurrencies through hacking and similar means. The fact that bitcoin can be used to pay for drugs does not by itself raise legal problems for the cryptocurrency; Russian rubles or bars of gold can do the same. The challenge is that a private, decentralized currency that is pseudonymous or anonymous makes it easier to engage in such illegal activity without consequence. Contrary to fears, no major Western government attempted to ban cryptocurrencies on this basis, and most of the nations that did have since recognized the basic legitimacy of bitcoin and similar currencies. That does not mean they are necessarily accepted as valid within the regulated banking system or for other particular purposes. It only means that transacting with cryptocurrencies in not *per se* prohibited.

[https://perma.cc/AH4F-V7DA] (Augur could " 'become one of the definitive prediction markets,' provided it can be maintained by its decentralized community.").

179. Prediction markets can produce highly accurate forecasts by aggregating the *wisdom of the crowd* based on financial incentives. *See* Kenneth J. Arrow et al., *The Promise of Prediction Markets*, 320 SCIENCE 877 (2008).

180. TAPSCOTT & TAPSCOTT, *supra* note 43, at 84.

The open question is how to deal with code that makes it quite difficult to engage in censorship or tampering, which also makes it easier to engage in terrorist financing or ransomware. A related concern is that code, by creating decentralized digital bearer instruments, creates an attractive target for thieves, both external and internal. These two problems, typified in Silk Road and Mt. Gox respectively, were the most prominent legal questions during the early years of Bitcoin. They remain central today.

A second category involves activity that is basically legitimate but not structured according to the legal requirements for the non-blockchain equivalent. Is a cryptocurrency exchange or a miner considered a money transfer agent or bank under state and federal laws in the United States? Is an issuance of tokens a securities offering under SEC rules, and are those doing the issuing investment managers?[181] Is a cryptocurrency exchange a derivatives marketplace subject to regulatory requirements issued by the Commodity Futures Trading Commission (CFTC)? [182] Should cryptocurrency service providers be required to obtain verified information about their customers and the destination of their transactions, as regulated financial institutions are under Anti-Money Laundering/Know Your Customer (AML/KYC) rules? Are profits on appreciation in cryptocurrencies subject to income tax as assets, currencies, or neither? The list is long and growing.

Finally, there is the matter of how other legal structures recognize distributed ledgers. States are beginning to move toward treating blockchain-based information analogous to more traditional records. The State of Delaware adopted legislation authorizing distributed ledgers for both government records and regulatory functions such as tracking corporate shares

181. In testimony before the Senate Banking Committee in February 2018, SEC Chairman Jay Clayton argued that, "by and large, the structures of ICOs that I have seen involve the offer and sale of securities and directly implicate the securities registration requirements and other investor protection provisions of our federal securities laws." SEC, *Chairman's Testimony on Virtual Currencies: The Roles of the SEC and CFTC* (Feb. 6, 2018), https://www.sec.gov/news/testimony/testimony-virtual-currencies-oversight-role-us-securities-and-exchange-commission [https://perma.cc/JH4M-489Y]. However, he did acknowledge that, "there are cryptocurrencies that, at least as currently designed, promoted and used, do not appear to be securities," leaving open the question of how the SEC would distinguish close cases. *Id.*

182. CFTC Chairman Chris Giancarlo told the Senate Banking Committee in February 2018 that, "[i]n 2015, the CFTC determined that virtual currencies, such as Bitcoin, met the definition of 'commodity' under the [Commodity Exchange Act (CEA)]. Nevertheless, the CFTC does NOT have regulatory jurisdiction under the CEA over markets or platforms conducting cash or 'spot' transactions in virtual currencies . . . ." J. Christopher Giancarlo, Chairman, Commodity Futures Trading Comm'n, Written Testimony Before the Senate Banking Committee, Washington, D.C. (Feb. 6, 2018), https://www.cftc.gov/PressRoom/SpeechesTestimony/opagiancarlo37 [https://perma.cc/YQ7R-EJBZ].

and liens.[183] Arizona passed a law declaring blockchain-based digital signatures as legally enforceable.[184] Vermont made blockchain-based information admissible as evidence in court.[185] As with the classification issues, however, there are many specific questions to consider and many jurisdictions that must act.

3. Dumb Contracts

Smart contracts are another domain in which blockchain-based approaches cannot escape the law. Smart contracts seem to offer a superior alternative to the messy process of legal enforcement. When parties agree on contractual terms, why would they rely on slow, potentially inaccurate or biased, and jurisdictionally-limited courts, when a distributed network of machines can execute the agreement perfectly each time? This view is prevalent among blockchain promoters.[186] The flaw in this reasoning is the failure to distinguish contractual execution from enforcement. Carrying out the specified steps in an agreement is the easy part. It is not a particularly novel phenomenon. Billions of dollars of derivatives trades are executed each day with no human intervention. Computers are programmed with the contractual terms and perform the trades when specified circumstances occur.

The difference is that, with current "computable contracts" (to use a term from law professor and software engineer Harry Surden) execution of the

183. *See* Jeff John Roberts, *Companies Can Put Shareholders on a Blockchain Starting Today*, FORTUNE (Aug. 1, 2017), http://fortune.com/2017/08/01/blockchain-shareholders-law/ [https://perma.cc/D89K-MJMH].

184. *See* Stan Higgins, *Arizona Governor Signs Blockchain Bill into Law*, COINDESK (Mar. 31, 2017), https://www.coindesk.com/arizona-governor-signs-blockchain-bill-law/ [https://perma.cc/T2JJ-RMAJ].

185. *See Vermont State to Recognize Blockchain Data in the Court System*, ECONOTIMES (May 18, 2016), http://www.econotimes.com/Vermont-State-to-recognize-blockchain-data-in-the-court-system-209803 [https://perma.cc/VGE2-C33X].

186. *See, e.g.*, TAPSCOTT & TAPSCOTT, *supra* note 43, at 109 ("[T]hrough smart contracts . . . [c]ompanies can program relationships with radical transparency . . . . And overall, like it or not, they must conduct business in a way that is considerate of the interests of other parties. The platform demands it."); Jay Cassano, *What Are Smart Contracts? Cryptocurrency's Killer App*, FAST COMPANY (Sept. 17, 2014), http://www.fastcolabs.com/3035723/app-economy/smart-contracts-could-be-cryptocurrencys-killer-app [https://perma.cc/4CUK-5JTY] ("Someday, these programs may replace lawyers . . . ."). Andrew Keys, *Memo from Davos: We Have a Trust Problem. Personal Responsibility and Ethereum Are the Solutions*, CONSENSYS (Jan. 19, 2017), https://media.consensys.net/memo-from-davos-we-have-a-trust-problem-personal-responsibility-and-ethereum-are-the-solutions-19d1104946d8#.c46zvkcks [https://perma.cc/5KKN-SAYH] ("It is early days, and there will surely be the need of attorneys, auditors, and regulators to learn, educate and facilitate smart contracts, but the process will become much more automated, intermediaries will be removed and the **cost of trust will plummet**.")(emphasis in original).

agreement is automated but enforcement is not.[187] The parties involved can revise the agreement before performance, and a court can reverse it after. Smart contracts automate contractual enforcement by ceding all power to the decentralized network maintaining the ledger.[188] Everything beyond the code is just an explanation, or to quote The DAO's terms of service, it is "merely offered for educational purposes."[189]

Automating contractual enforcement is not as neat as automating execution. There are certainly large potential benefits to eliminating the legal system from the contractual process. An unstoppable contract does not operate at the whim of some confused judge, or corrupt local official, or greedy government, or deceitful counterparty. The potential efficiency and automation gains of taking lawyers out of the enforcement loop are great. Yet the same process allowed for the catastrophic failure of The DAO.

No matter how fast they calculate, there are some things computers cannot do as well as humans. The same is true for smart contracts.[190] There is no good way to represent terms such as "reasonable" or "best efforts" in code. And sometimes the meaning of the contract is best understood in terms of the intent of the parties rather than the precise meaning of the terms they used. The DAO was a perfect example. The only difference between the attacker who tried to steal the funds and the miners who took it back through the hard fork was their motivations.[191] That cannot be assessed by a computer.

Even when smart contracts fully execute agreements, parties aggrieved at the results will still resort to litigation.[192] Judges who believe an injustice or legally cognizable injury has occurred will not simply throw up their hands and defer to a distributed ledger. There may be practical difficulties in identifying pseudonymous or anonymous counterparties, as well as in bringing legal actions against actors in other countries. On the former, there is almost always some known entity to sue, whether the action succeeds or not. Had contributors to The DAO not received their money back through the Ethereum hard fork, some of them doubtless would have sued Slock.it (the developers of the DApp) and the Ethereum Foundation. On the latter concern, cross-border contractual disputes are a staple of modern business among multi-national firms. There are certainly some parties to smart contracts

187. Harry Surden, *Computable Contracts*, 46 U.C. DAVIS L. REV. 629 (2012).

188. *See* Werbach & Cornell, *supra* note 25, at 344–48.

189. The DAO's terms of service page is no longer available. For a contemporaneous quotation, see Joel Ditz, *DAOs, Hacks and the Law*, MEDIUM (June 17, 2016), https://web.archive.org/web/20160622212443/https://daohub.org/explainer.html [https://perma.cc/SL53-WKLA].

190. Werbach & Cornell, *supra* note 25, at 365–66.

191. *See id.* at 360–63.

192. *See id.*

who will refuse to appear in court but established firms are unlikely to do so. Issues of jurisdiction and choice of law are challenging but not insoluble.

C. REGULATION AND INNOVATION

1. Classifying Cryptoducks

Regulation is often posed as the antithesis of innovation. To many, it seems obvious that government involvement in the development of cryptocurrencies and blockchain-based systems will slow and corrupt the development of new systems. If government was only necessary because people could not trust each other without the fear of Thomas Hobbes' mythical Leviathan, then perhaps Satoshi Nakamoto solved that problem.

Here too, however, there is reason to question the old cyber-libertarian view. Regulation of the Internet was actually an important step in its widespread adoption.[193] Many things that "just worked" in the early days turned out to be consequences of a small, close-knit, homogeneous online community. As the Internet began to look more like society, it faced the same political and economic challenges as offline communities. For example, when Microsoft used its monopoly power in the late 1990s to threaten Internet-based startups, the U.S. Government intervened through antitrust enforcement to restrain it.[194] Moreover, the knowledge that governments were operating to police abusive practices helped promote trust in the new and unfamiliar word of virtual transactions. Internet advocates began to call for government intervention to enforce network neutrality rules and privacy protections.[195]

Something similar is likely to occur for distributed ledger technology. The notion that activity on a blockchain cannot be subject to legal enforcement died with the arrest of Ross Ulbricht, if not before. Alexander Vinnik, who allegedly masterminded the massive theft from Mt. Gox and hid his tracks through exchanges and mixer services that make it difficult to trace bitcoin transactions, was also eventually arrested.[196] Particularly with the rise of permissioned ledgers and enterprise-grade systems on top of public ledgers, regulation as a facilitator of blockchain development is gaining currency. Not that the path forward will be easy. The Internet offers a largely positive model of governments acting thoughtfully and nascent industries acting

193. *See* Werbach, *supra* note 172, at 888–89.

194. *See id.* at 909–11.

195. *See id.* at 914–16.

196. *See* Samuel Gibbs, *'Criminal Mastermind' of $4bn Bitcoin Laundering Scheme Arrested*, GUARDIAN (July 27, 2017), https://www.theguardian.com/technology/2017/jul/27/russian-criminal-mastermind-4bn-bitcoin-laundering-scheme-arrested-mt-gox-exchange-alexander-vinnik [https://perma.cc/2EKW-KAH5].

responsibly.[197] There are plenty of counter-examples, but there are enough cases of regulators and the regulated cooperating to allow growth and innovation. There is no guarantee the same will be true for the blockchain.

While Silk Road-like illicit cryptocurrency marketplaces still operate, as do non-blockchain "darknet" sites frequented by erstwhile criminal hackers, infringing content distributors, and identity thieves, such furtive activity is on a limited scale. Most people do not buy drugs online and pay to access streaming media services. The blockchain created a new challenge for law enforcement but so did the Internet. As did the development of strong encryption technology in the early 1990s and the spread of personal computers in the 1980s. The list goes on. The digital technology of the contemporary world is a double-edged sword, capable of good as well as evil. The blockchain adds a new chapter to this story, but does not fundamentally change the balance of power.

To be sure, there are important questions about where to draw lines around surveillance and permissible uses of technology. Criminals and terrorists will try to exploit the blockchain, just as they exploit other technologies whenever possible. Governments will overreact and propose rules with collateral damage to legitimate operations. The point is that these are not new questions. Nor should they be seen as evidence of some fundamental opposition between the blockchain and legality. The more interesting scenarios involve new services that do not set out to break the law. To what extent does the blockchain render superfluous existing legal regimes by interposing a powerful new mechanism for trust and compliance? And to what extent do those existing legal regimes necessarily impose excessive burdens on blockchain-based innovation?

As described in the previous section, much of regulation is a classification exercise. The rules establish status categories, and the regulators police who is subject to those categories. Sometimes the classification is obvious. Verizon and AT&T do not dispute that in completing conventional circuit-switched landline telephone calls, they are operating as "telecommunications carriers" under the Communications Act of 1934.[198] Sometimes, though, the classification is more difficult. Does Comcast—which historically did not offer telephone service and now does so over specialized packet-switched data networks using Internet technologies—fit in that box? Does Vonage, which owns no network facilities itself and provides voice calling as an application for broadband users? Does Amazon, which now supports voice messages on its Echo personal assistant devices?

197. *See* Werbach, *supra* note 172, at 916–17; Kevin Werbach, *The Federal Computer Commission*, 84 N.C. L. REV. 1, 63–65 (2005).

198. 47 U.S.C. § 153(51) (2018).

The simple answer is that services that look like ducks and quack like ducks should be regulated as ducks. The practical implications in the case of Internet telephony involved more than a decade of contentious debates.[199] That was not necessarily a bad thing. The FCC was sensitive to concerns about preemptive and over-expansive regulation dampening innovation.[200] There was no way the classification controversy could have been resolved quickly in the 1990s because the technology was too immature and its implementation too limited.

Regulators today face a similar challenge in classifying the flock of young "cryptoducks."[201] In 2015, FinCEN, the financial crimes enforcement office of the United States Treasury Department, announced a civil enforcement action against Ripple.[202] Ripple uses a blockchain to greatly reduce the cost of international money transfers, a multi-billion dollar annual market. The problem, in FinCEN's eyes, was that Ripple did so without registering as a regulated money services business.[203] There was nothing wrong with processing money transfers; the issue was doing so without the obligations of existing players in that industry. In particular, Ripple failed to follow the anti-money laundering and "know your customer" (AML/KYC) rules for its users. These are designed to prevent criminals and terrorists from using the banking system to support their activities. In response to the FinCEN action, Ripple agreed to a $950,000 fine and committed to establish an AML/KYC compliance regime.[204]

The Ripple sanctions were a turning point for the cryptocurrency industry. Unlike Bitcoin, which is a protocol implemented on a distributed network, Ripple is a for-profit company. Its business model depends on its ability to develop partnerships with financial institutions around the world. For Ripple, FinCEN sanctions are a big deal. The AML/KYC process, which typically requires financial services operators to verify physical identity documents such as passports and check against blacklists of individuals, can be onerous, especially for fast-moving and highly-computerized service providers.

---

199. *See* Kevin Werbach, *No Dialtone: The End of the Public Switched Telephone Network*, 66 FED. COMM. L.J. 203, 207 (2013).

200. *See id.* at 231.

201. *See* Camila Russo, *Ethereum Co-Founder Says Crypto Coin Market Is a Time-Bomb*, BLOOMBERG (July 18, 2017), https://www.bloomberg.com/news/articles/2017-07-18/ethereum-co-founder-says-crypto-coin-market-is-ticking-time-bomb [https://perma.cc/H3ZB-6CPC] (quoting Ripple CEO Brad Garlinghouse, stating that, "If it talks like a duck and walks like a duck, the SEC will say it's a duck.").

202. *See* Sarah Todd, *Fincen Fines Ripple Labs Over AML, Says Firm 'Enhancing' Protocol*, AM. BANKER (May 5, 2015), https://www.americanbanker.com/news/fincen-fines-ripple-labs-over-aml-says-firm-enhancing-protocol [https://perma.cc/Q5B6-QRAB].

203. *See id.*

204. *See id.*

Some companies saw the FinCEN action as a signal that the U.S. was not a hospitable jurisdiction for cryptocurrency companies. Xapo, a venture-backed Bitcoin wallet startup, relocated its headquarters from California to Switzerland ten days after the decision.[205] A few months later, the New York State Department of Financial Services began requiring virtual currency businesses operating in the state to obtain a "BitLicense" from the agency.[206]

The idea behind the BitLicense—that financial exchanges transacting in cryptocurrencies should be treated similarly to comparable exchanges transacting in traditional currencies—was sound. However, the implementation was lacking. The requirements for covered entities were onerous. The regulations were drafted in a way that seemed to cover many cryptocurrency businesses other than custodial exchanges, and the certification process was cumbersome. As of early 2017, only three BitLicenses had been granted, despite dozens of applications.[207] The recipients—Circle, Ripple, and Coinbase—were three of the best-funded startups in the space, reinforcing concerns that BitLicense would crowd out innovative small players. At least ten Bitcoin companies announced they were ceasing business in New York as a direct result of the BitLicense.[208]

2. Jurisdictional Competition

One difference between the regulatory debates in the dot-com and distributed ledger eras is that the United States is no longer the dominant source of activity. The Internet today is highly globalized, but in the 1990s, usage and startup creation were heavily centralized in the United States. In contrast, there are concentrations of distributed ledger activity around the world. London, Berlin, Switzerland, and Singapore are major hubs, with significant centers in mainland China, Canada, South Korea, Japan, Estonia, Argentina, and Hong Kong.[209] Vitalik Buterin, leader of the Ethereum project,

---

205. *See* Kia Kokalitcheva, *Switzerland is a Banking Capital. But a Bitcoin Capital?*, FORTUNE (May 15, 2015), http://fortune.com/2015/05/15/bitcoin-switzerland-privacy/ [https://perma.cc/JV4Q-B25N].

206. *See* Michael J. Casey, *NY Financial Regulator Lawsky Releases Final BitLicense Rules for Bitcoin Firms*, WALL ST. J. (June 3, 2015), https://www.wsj.com/articles/ny-financial-regulator-lawsky-releases-final-bitlicense-rules-for-bitcoin-firms-1433345396 [https://perma.cc/5AW4-DQZG].

207. *See* Michael del Castillo, *Bitcoin Exchange Coinbase Receives New York BitLicense*, COINDESK (Jan. 17, 2017), https://www.coindesk.com/bitcoin-exchange-coinbase-receives-bitlicense/ [https://perma.cc/TB5S-PBQM].

208. *See* Daniel Roberts, *Behind the "Exodus" of Bitcoin Startups from New York*, FORTUNE (Aug. 14, 2015), http://fortune.com/2015/08/14/bitcoin-startups-leave-new-york-bitlicense/ [https://perma.cc/RC8X-7UXX].

209. *See* Richard Kastelein, *Global Blockchain Innovation: U.S. Lags, Europe and China Lead*, VENTUREBEAT (Apr. 16, 2017), https://venturebeat.com/2017/04/16/global-blockchain

is a Russian who grew up in Canada, heads a foundation headquartered in Switzerland, and now lives in Singapore. If he had created an early Internet startup, he would have likely headed to Silicon Valley.

The global distribution of blockchain development activity encourages jurisdictional competition among regions. U.S. dominance of the early Internet industry produced major benefits, both economic and in terms of global soft power. Hoping to be the Silicon Valley of the crypto economy, countries ranging from tiny Gibraltar to Russia are creating new legal frameworks to attract blockchain startups, coin offerings, and other activity. The early leader is the canton of Zug, Switzerland, which combines a stable government, a central location in Europe, a welcoming environment for cryptocurrency companies, and very favorable tax policies.[210] It is bidding to be the cryptocurrency equivalent of Delaware for U.S. incorporation, although the real Delaware, among other locales, seems determined to compete.

The U.S. is still a very important driver of blockchain activity. A significant portion of core Bitcoin development occurs in the United States. New York is one of the primary centers for distributed ledger technology in financial services. Many of the most significant investors in blockchain startups are in the United States, including Digital Currency Group, Blockchain Capital, Andreessen Horowitz, and Union Square Ventures. U.S. technology and services firms such as IBM, Microsoft, and PwC are at the forefront of most large-scale enterprise implementations of distributed ledger applications. The technical talent and technology startup ecosystems in the United States remain unmatched.

It bears repeating that major Internet companies did not locate in Sealand or island tax havens; they went to where the developers and customers were. Organizations do not just seek the least regulation; they seek the best regulation, among a slate of other factors. A reliable and stable regulatory environment will be important for building trust in blockchain platforms that seek a large user base. Similarly, even jurisdictions keen to attract entrepreneurial businesses in fields such as cryptocurrency do not simply engage in a race to the bottom. Singapore is a hotbed of blockchain activity, due in part to its permissive regulatory attitude. However, the Monetary Authority of Singapore made clear in an August 2017 announcement that initial coin offerings there would be subject to money laundering and terrorist financing restrictions.[211] They would also be regulated as securities offerings

-innovation-u-s-lags-europe-and-china-lead/ [https://perma.cc/T6ST-QRLC].

210. *See* Kokalitcheva, *supra* note 205 (noting Switzerland's "regulatory stability, international neutrality and its deep-seated tradition in global finance").

211. Monetary Auth. of Sing., MAS Clarifies Regulatory Position on the Offer of Digital Tokens in Singapore (Aug. 1, 2017), http://www.mas.gov.sg/News-and-Publications/Media

when they "represent ownership or a security interest over an issuer's assets or property."[212]

Some small territories focused on generating revenues may take an "anything goes" attitude, but ICOs based there will eventually be less trusted—and therefore less successful in attracting capital. Moreover, the countries where that capital comes from will not be shy about exercising jurisdiction. These are the same reasons why all companies today do not domicile in offshore tax havens.

While the BitLicense may have given the United States a poor regulatory reputation in some cryptocurrency circles, more recent initiatives were more thoughtfully drawn. The Uniform Law Commission, which creates model codes that are widely adopted by state legislatures, adopted a model cryptocurrency law in 2017 that limits the scope of regulation.[213] The CFTC created a LabCFTC group to study cryptocurrencies and engage with the nascent industry.[214] The SEC's investigative report on initial coin offerings and The DAO was widely praised as measured and technically knowledgeable.[215]

There is no certainty that the United States, or any jurisdiction, will strike the appropriate balance between flexibility and protection in its regulatory approaches to blockchain-based systems. The debates have just begun. Overall, though, regulators who do nothing will be a greater threat to the development of the market than those who engage in thoughtful and evolving efforts to address public policy considerations.

-Releases/2017/MAS-clarifies-regulatory-position-on-the-offer-of-digital-tokens-in -Singapore.aspx [https://perma.cc/5RD2-T865].

212. *Id.*

213. Peter Van Valkenburgh, *The ULC's Model Act for Digital Currency Businesses Has Passed. Here's Why It's Good for Bitcoin*, COIN CENTER (July 19, 2017), https://coincenter.org/entry/the-ulc-s-model-act-for-digital-currency-businesses-has -passed-here-s-why-it-s-good-for-bitcoin?mc_cid=c93d4ad9d7&mc_eid=7845af7088 [https://perma.cc/D3E3-RMGA].

214. *See* J. Christopher Giancarlo, Acting Chairman, Commodity Futures Trading Comm'n, Address before the New York FinTech Innovation Lab: *LabCFTC: Engaging Innovators in Digital Financial Markets*, (May 17, 2017), http://www.cftc.gov/PressRoom/SpeechesTestimony/opagiancarlo-23 [https://perma.cc/HF8W-NW8W].

215. *See, e.g.*, Kyle E. Mitchell, *Seven Takeaways from the SEC DAO Report*, /DEV/LAWYER, https://writing.kemitchell.com/2017/07/25/DAO-Report-of-Investigation.html [https://perma.cc/3Y3X-N4VM] (observing that the SEC "deploys the lingo of the industry like a native speaker"); Frances Coppola, *Digital Coins and Tokens Are Just Another Kind Of Security*, FORBES (July 31, 2017), https://www.forbes.com/sites/francescoppola/2017/07/31/sec-tells-digital-coin-and -tokens-issuers-to-comply-with-securities-laws/#19faf7953bb1 [https://perma.cc/B3YA -JUK8] (arguing that with ICOs, "it is the coders, not the investors, who run this show. The SEC has decided to call them to account, and rightly so.").

IV. CONNECTING LEGAL AND BLOCKCHAIN TRUST

One way for the blockchain to achieve more robust trust is, perhaps surprisingly, through the legal system. There are several mechanisms to hybridize the blockchain's distributed, algorithmic trust structures with the human-interpreted, state-backed institutions of law. In some contexts, no legal involvement will be needed. In others, where the blockchain is purely supplemental, existing legal arrangements function normally without any special integration. In many cases, however, affirmative steps must be taken to combine the best aspects of distributed ledgers and centralized law.

A. BLOCKCHAIN AND/OR/AS LAW

Lawrence Lessig's point in saying, "code is law," was that code—as well as markets and norms—is just one coequal modality of regulation.[216] Hence the title of his book, describing code "and other laws of cyberspace." Whether it is superior or inferior depends on the context. For example, digital rights management software limits use of content more tightly than copyright law, because it ignores safety valves such as fair use and the first sale doctrine.[217] If there is to be a Lex Cryptographia, therefore, the salient challenge is to identify its strengths and weaknesses, relative to those of traditional legal mechanisms.

Both the legal system and software code can promote trust. Both can also undermine it. As distributed ledgers become more prominent, the simplistic view that they obviate the need for law will become increasingly untenable. The Silk Road takedown showed that the blockchain is not an impermeable shield against legal enforcement, and the DAO attack showed the governance limitations of purely algorithmic systems. Yet the equally simplistic view that regulators can and should direct these systems the way they manage centralized equivalents is equally misguided. Both legal actors and the technologists developing the new distributed platforms must take affirmative steps to promote trust. If governed properly, blockchain-based solutions can overcome some of the limitations of legal enforcement, and vice versa.

There are three primary ways the two systems can interact: blockchain as supplement, complement, or substitute.

1. Blockchain Supplements

Where the existing trust architecture is generally functional, the blockchain can operate as an additional layer subject to established legal rules. In such situations, the primary value proposition of the distributed ledger is the speed

216. *See* CODE VERSION 2.0, *supra* note 22, at 1.
217. LESSIG, CODE, AND OTHER LAWS OF CYBERSPACE, *supra* note 22.

and efficiency gain of a single shared data record.[218] The blockchain replaces the error-prone messaging structures between participants but does not seek to upend industry structure.[219]

For example, in the United States, there are well-developed legal rules and established practices around real estate transactions. Title insurance is used to protect buyers against defects in land titles.[220] The combination of formal rules and solid norms produces a strong environment of trust. However, there are significant inefficiencies in the system. Title insurance is still largely based on paper records, which must be exchanged among multiple parties. Goldman Sachs estimates moving to distributed ledgers could reduce title insurance premiums in the United States and generate two to four billion dollars in cost savings, thanks to improved efficiency and reduced risk.[221]

In this scenario, the existing legal obligations and centralized business arrangements bear the primary trust burden for the transaction. The blockchain steps in as a potentially superior record-keeping mechanism. Trust in the integrity of the data on the shared ledger is sufficient. The buyer's trust relationships with the seller and various intermediaries such as banks and brokers remain unchanged. Systemic concerns about the technical viability of distributed ledgers remain relevant as trust considerations.[222] The other concerns and limitations of the blockchain as a trust infrastructure are less relevant because the shared ledger is not attempting to supplant legal recourse.

Another example is Corda, a project of the R3 financial industry consortium. It uses distributed ledger technology to manage agreements between financial institutions, thus avoiding the costs of reconciliation.[223] Only identified institutions can participate in the Corda network.[224] The data structure for recording transactions is actually not a blockchain and does not use proof of work, although it employs a consensus-based distributed ledger with smart contracts.[225]

Corda networks can explicitly invite in regulators, who can operate "supervisory observer nodes" with access to real-time information about

218. *See* Schneider et al., *supra* note 15, at 4.

219. *Cf.* UBS, *supra* note 43, at 8 ("Instead of making them superfluous, the blockchain may very well make banks better at what they do.").

220. Title insurance is only necessary because the United States, unlike much of the world, has a system of "registration by title" instead of "title by registration." Valid recording of a title transfer does not guarantee indefeasible ownership. *See* Schneider et al., *supra* note 15, at 33–35.

221. *See* Schneider et al., *supra* note 15, at 4–5.

222. *See id.* at 4.

223. *See* Brown, *supra* note 58.

224. *See id.*

225. *See id.*

transactions.[226] This is an important point. If designed to facilitate regulatory oversight, rather than to exclude government as with the original Bitcoin protocols, blockchain-based systems can actually support more effective regulation. The real-time transparency of the shared ledger could allow regulators to identify and respond to problems before the consequences become dire.[227] They could even build compliance mechanisms directly into the system.[228]

With supplementary distributed ledgers, all the work of establishing trust has already been done. The blockchain is used solely to protect the integrity of data on the shared ledger. This is the least ambitious mode of applying the blockchain and the least transformative. It is likely to be most comfortable for regulators and other government actors, because it does not ask them to change their roles or rules substantially. The risks are lower, but the benefits are concomitantly more limited. The blockchain as a supplement to existing legal regimes can promote efficiency and reduce transaction costs, but is unlikely to transform industry structures or produce breakthrough innovations.

2. Blockchain Complements

A second class of applications involves situations where trust based on the legal system is breaking down or insufficient. Distributed ledgers can complement and extend the existing trust architecture. Often the problem in the current environment is that centralized arrangements cannot scale effectively enough, preventing desirable solutions. Where the blockchain powers new markets, it often does so in ways that are complementary to existing legal arrangements.

Consider the challenge of orphan works under copyright law.[229] These are works whose rights-holders cannot be located. Those who wish to use them, for example, documentary filmmakers wishing to incorporate archival footage, cannot negotiate a license even if they wanted to. Orphan works are thus in legal limbo. The risk of statutory damages for copyright infringement is a severe threat that scares away potential users of the material, even though in some cases it might actually be in the public domain. The marketplace envisioned by copyright law, in which authors can control and monetize their

226. *Id.*

227. *See* UBS, *supra* note 43, at 24 ("In a blockchain-based system, where transactions are immediate and the ledger public, regulators could have a real-time view of what is transpiring in the system at all times.").

228. *See id.* at 25.

229. *See generally* Jerry Brito & Bridget Dooling, *An Orphan Works Affirmative Defense to Copyright Infringement Actions*, 12 MICH. TELECOMM. & TECH. L. REV. 75 (2005).

output, fails to develop.

Orphan works are a good opportunity to use a shared registry to create a new market.[230] A blockchain-based registry would be available to all and would not give excessive gatekeeper power to any intermediary. It could keep track of efforts to engage in the diligent search for rights-holders required under copyright law.[231] Smart contracts could be used to ensure that those who use orphan works pay licensing fees to legitimate rights-holders who come forward (most likely vetted by an arbitration mechanism). The distributed ledger here would not take the place of standard copyright law, but it would extend it in a direction that it cannot easily go today.[232]

A more ambitious version of a similar idea is to give artists and other content creators persistent control over rights associated with their creations. Today, digital rights management systems are controlled by intermediaries and distributors, not the creators themselves. As a result, many artists have difficulty receiving sufficient compensation. Initiatives are underway to decentralize control over digital rights using distributed ledgers, giving power back to artists, including Ujo Music, PeerTracks, and the Open Music Initiative.[233]

These ventures still face the challenge of entrenched power dynamics. Even if artists have the technical capacity to control their output, they may not have the practical ability to do without the marketing and distribution power of the music industry. In all likelihood, a limited segment of artists will be able to take advantage of distributed rights platforms, but this could still be an

230. *See* Patrick Murck, *Waste Content: Rebalancing Copyright Law to Enable Markets of Abundance*, 16 ALB. L.J. SCI. & TECH. 383, 416–17 (2006) (discussing the potential new market if orphan works are liberated).

231. *See generally* Jake Goldenfein & Dan Hunter, *Blockchains*, *Orphan Works*, *and the Public Domain*, 41 COLUM. J.L. & ARTS 1, 22–25 (2017) (describing a blockchain-based system to solve the orphan works problem). The prohibition on formalities in international copyright agreements would make it difficult to establish a mandatory registry for orphan works.

232. Similarly, the blockchain could be used to create unique digital assets that allow for a digital version of copyright's longstanding first sale doctrine. *See* Patrick Murck, *The True Value of Bitcoin*, CATO UNBOUND (July 31, 2013), http://www.cato-unbound.org/2013/07/31/patrick-murck/true-value-bitcoin [https://perma.cc/Y28Q-4MD7].

233. *See* Gideon Gottfried, *How 'the Blockchain' Could Actually Change the Music Industry*, BILLBOARD (Aug. 5, 2015), http://www.billboard.com/articles/business/6655915/how-the-blockchain-could-actually-change-the-music-industry [https://perma.cc/84TX-3HGM]; Ian Allison, *Imogen Heap Shows How Smart Music Contracts Work Using Ethereum*, INT'L BUS. TIMES (Oct. 29, 2015), http://www.ibtimes.co.uk/imogen-heap-shows-how-music-smart-contracts-work-using-ethereum-1522331 [https://perma.cc/QP8L-BJRM]; Malcolm Gay, *Can Major Initiative Led by Berklee Solve Music-Rights Problems?*, BOSTON GLOBE (June 13, 2016), https://www.bostonglobe.com/arts/music/2016/06/12/berklee-lead-musical-rights-initiative/aXBXC8adJgXE4IRRt8dcKO/story.html [https://perma.cc/T6FJ-57J2].

advance over the current artist-hostile system. As with the supplemental applications, these blockchain-based solutions leave conventional law (in this case, the copyright system) in place. However, they extend it to new applications that are untenable through existing trust architectures. As a result, there may need to be mappings between the apparatus of legal enforcement and the technical framework of distributed ledgers.

3. Blockchain Substitutes

The final category of blockchain legal applications involves no backstop of traditional legal enforcement. The saga of The DAO illustrates the dangers of this path.[234] However, where legal enforcement is weak, the blockchain can in some cases function as a substitute. If there is no workable rule of law to begin with, rule of blockchain may be a significant improvement. Several billion people in the developing world, for example, lack access to bank accounts and the opportunities for easy payments and credit they bring. Bitcoin and other cryptocurrencies offer a shortcut to address this challenge of the unbanked.[235] In 2017, the United Nations World Food Program conducted a successful trial using the Ethereum blockchain to track food aid distribution to 10,000 Syrian refugees in Jordan.[236] The program provided accountability in an environment where conventional legal enforcement is difficult.

In many parts of the world, land title records are incomplete and challenging for ordinary citizens to interact with. The Peruvian economist Hernando de Soto argues that the absence of well-functioning land registration systems in the developing world is a major impediment to economic development.[237] Initiatives are underway in various parts of the world to use the blockchain as a solution, including Ghana and the country of Georgia.[238]

234. *See supra* notes 135–139 and accompanying text.

235. *See* Mark S. Miller & Marc Stigler, *The Digital Path: Smart Contracts and the Third World*, *in* MARKETS, INFORMATION, AND COMMUNICATION: AUSTRIAN PERSPECTIVES ON THE INTERNET ECONOMY 63–88 (2003), http://www.erights.org/talks/pisa/paper/index.html [https://perma.cc/NFP8-R2J4]; Susan Athey, *5 Ways Digital Currencies Will Change the World*, WORLD ECON. FORUM (Jan. 22, 2015), https://agenda.weforum.org/2015/01/5-ways-digital-currencies-will-change-the-world/[https://perma.cc/Z8AU-8RF2].

236. *See* Leigh Cuen, *UN Using Blockchain Technology to Help Refugees, Fight World Hunger*, INT'L BUS. TIMES (May 4, 2017), http://www.ibtimes.com/un-using-blockchain-technology-help-refugees-fight-world-hunger-2534759 [https://perma.cc/Q2FG-VUJ2].

237. *See* HERNANDO DE SOTO, THE MYSTERY OF CAPITAL: WHY CAPITALISM TRIUMPHS IN THE WEST AND FAILS EVERYWHERE ELSE 15–28 (2000).

238. *See* Laura Shin, *Republic of Georgia to Pilot Land Titling on Blockchain With Economist Hernando De Soto, BitFury*, FORBES (Apr. 21, 2016), http://www.forbes.com/sites/laurashin/2016/04/21/republic-of-georgia-to-pilot-land-titling-on-blockchain-with-economist-hernando-de-soto-bitfury/#5a2979f36550

The hurdle for these systems is the human actors outside the ledger. A corrupt local land office that refuses to record information accurately on a blockchain, or that disregards the information it reports, can still do so. One of the first initiatives to record land titles on a blockchain, an effort in Honduras involving the startup Factom, never got off the ground because of difficulties with the local partners.[239] For that reason, the initiatives likely to move forward first are in relatively stable countries such as Georgia, and very stable ones such as Sweden, even though the need might be greater in the developing world.

And of course, communities will use the blockchain to substitute for law when their goal is to evade legal responsibilities. Only when the point is to ensure honor among thieves in a dark marketplace such as Silk Road is the blockchain in opposition to legal enforcement. Recall the case of Uber in Buenos Aires. There, bitcoin was used to route around limits on payment processing at the behest of the city government; the transactions involved were not *per se* illegal.[240] The cryptocurrency gave Uber leverage by establishing a trusted payment option outside traditional centralized channels.[241] Such scenarios are real, but they occupy a relatively small and shrinking portion of the distributed ledger landscape.

B. MAKING LAW MORE CODE-LIKE

In any of the three scenarios just described, the relationship of blockchain-based systems and legal institutions can be smooth or rough. Blockchain developers cannot ignore the law, but neither can governments disregard the growing significance of the blockchain. One way to bridge the gap is for law to adapt. Some of that will happen naturally as regulators, legislators, and judges confront the challenges and opportunities this foundational new technology presents. More explicit steps can accelerate the process.

[https://perma.cc/ZHW3-4JVL]; Roger Aitken, *Bitland's African Blockchain Initiative Putting Land on the Ledger*, FORBES (Apr. 5, 2016), http://www.forbes.com/sites/rogeraitken/2016/04/05/bitlands-african-blockchain-initiative-putting-land-on-the-ledger/#59ee9ab11029 [http://perma.cc/99TT-4RYD].

239. *See* Pete Rizzo, *Blockchain Land Title Project 'Stalls' in Honduras*, COINDESK (Dec. 26, 2015), https://www.coindesk.com/debate-factom-land-title-honduras/ [https://perma.cc/MKJ8-ZM87].

240. *See supra* note 101.

241. The Buenos Aires government could not block the Uber riders from using the distributed Bitcoin network. However, it could probably issue an order against the Swiss firm, Xapo, that provides the debit cards which translate between Bitcoin and the local currency. *See* Valenzuela, *supra* note 101.

1. Safe Harbors and Sandboxes

A safe harbor is a regulatory provision formally limiting legal enforcement. When firms can take sufficient steps to police themselves, the safe harbor incentivizes them to do so. It also defines what specific conduct is necessary. Perhaps the best known safe harbor in the technology world is Section 230 of the Communications Act, which was adopted in 1996 as part of the Communications Decency Act (CDA).[242] It shields online intermediaries from liability for content flowing across their systems. The breadth of this safe harbor, created in the early days of the commercial Internet, is problematic. It shields intermediaries even when they ignore harmful activity, such as online harassment.[243] On the other hand, the CDA safe harbor was a significant factor in the rapid growth of online intermediaries.[244] It was particularly important to the spread of user-driven "Web 2.0" services and social media.[245]

Based on this history, Coin Center has proposed a new safe harbor for blockchain-based startups.[246] Specifically, it urges legislation stating that non-custodial services—those which do not obtain control over user funds—are exempt from rules governing money transmitters. This would acknowledge that distributed ledgers change the relationship between those who move currencies and the users who own that currency.

Prior to Bitcoin, possessing money meant having the ability to do anything with it. An online service such as PayPal, where a user parks funds, has the power (absent legal or regulatory obligations) to steal it or send it to terrorists. On a blockchain, by contrast, many actors such as miners, DApps, and wallet software providers touch the records of transactions, but without the private keys governing user accounts, they lack any such capabilities. Only the custodial exchanges which users authorize to move funds operate like traditional money transmitters. Embedding the distinction between possession and control in a legal safe harbor would remove uncertainty from the market and make the legal regime more consistent with technical realities.

---

242. 47 U.S.C. § 230 (2018).

243. *See, e.g.*, Danielle Keats Citron & Mary Anne Franks, *Criminalizing Revenge Porn*, 49 WAKE FOREST L. REV. 345, 359 (2014).

244. *See, e.g.*, Derek Khanna, *The Law that Gave Us the Modern Internet—and the Campaign to Kill It*, ATLANTIC (Sept. 12, 2013), https://www.theatlantic.com/business/archive/2013/09/the-law-that-gave-us-the-modern-Internet-and-the-campaign-to-kill-it/279588/ [https://perma.cc/HG7W-VJEB].

245. *See id.* ("It was simple and intuitive to understand for entrepreneurs and . . . has functioned as a permission slip for . . . [e]ntrepreneurs [to found] the user-generated content sites we know and love today.").

246. *See* Peter Van Valkenburgh, *Bitcoin Innovators Need Legal Safe Harbors*, COIN CENTER (Jan. 24, 2017), https://coincenter.org/entry/bitcoin-innovators-need-legal-safe-harbors [https://perma.cc/C5ES-KZGN].

Sandboxes are similar to safe harbors but limited in time or scale. A regulatory sandbox exempts certain companies or activities from regulation as a means to foster experimentation and startup activity. Unlike a safe harbor, a sandbox is not necessarily permanent, and it usually only applies to new companies. One of the concerns about the Internet safe harbors is that they were designed to help nascent firms without the resources to police content on their platforms but wound up helping titans like Google and Facebook. A sandbox can be constructed to apply to organizations at early stages of development and disappear when they mature.

In the United Kingdom, the Financial Conduct Authority (FCA), the primary financial regulator, established a Fintech Sandbox program that allows companies to experiment with new services.[247] Companies apply to operate in the sandbox, and if approved, they receive individualized waivers and supervised special authorizations to engage in pilot projects without regulatory concerns. There is nothing quite comparable in the United States at this time, although the CFTC's LabCFTC program is designed to move in a similar direction.[248]

In contrast to the "prohibit if not permitted" approach of New York's BitLicense, a sandbox model would encourage the kind of "permissionless innovation" that was critical to the development of the Internet marketplace.[249] The ethos of software developers, including those building blockchain-based systems today, is reflected in the Internet Engineering Task Force motto that decisions should be based on "rough consensus and running code."[250] Well-designed sandboxes can make it easier for startups to write that running code and give regulators visibility to understand the public policy concerns that may arise.

2. Modularizing Contracts

Private law can be made more code-like as well. Most business contracts are essentially modules that lawyers string together and customize. Some sections describe business terms and what should happen under defined circumstances. Such "operational" aspects are the kind that can often be

247. *See Financial Conduct Authority Unveils Successful Sandbox Firms on the Second Anniversary of Project Innovate*, FIN. CONDUCT AUTH. (July 11, 2016), https://www.fca.org.uk/news/press-releases/financial-conduct-authority-unveils-successful-sandbox-firms-second-anniversary [https://perma.cc/86BN-RSR7].

248. *See* Giancarlo, *supra* note 214.

249. *See generally* ADAM THIERER, PERMISSIONLESS INNOVATION: THE CONTINUING CASE FOR COMPREHENSIVE TECHNOLOGICAL FREEDOM (2016).

250. *See* Andrew L. Russell, *'Rough Consensus and Running Code' and the Internet-OSI Standards War*, *in* 28 IEEE ANNALS OF THE HIST. OF COMPUTING 48, 49 (2006).

automated in smart contracts.[251] Other parts of the contract are non-operational or legal terms, such as limitations on damages, indemnification, confidentiality, and choice of law or forum. Lawyers often re-use standard clauses, which they adapt and negotiate for the particular transaction.

To make this contract drafting process more analogous to the formalized coding that goes into a smart contract, the contractual clauses can be represented as components that are assembled into a digital document using a markup language. Templates could be created from these modules to provide baseline agreements for common scenarios. Lawyers would still have a role in customizing the templates, deciding which variations to use, and negotiating contentious terms. The skills required of lawyers would have to change, with the field becoming more like legal engineering.[252] Legal code audits could also be implemented to ensure the contracts match the parties' intent, analogous to the security audits widely used by firms engaged in software development.[253]

Several initiatives are developing exactly this sort of system. These include Open Law, a project of Ethereum development studio Consensys;[254] the startups Clause.io and Agrello;[255] the smart contracts templates group of the

251. Christopher D. Clack, et al., Smart Contract Templates: Foundations, Design Landscape and Research Directions 5 (Aug. 4, 2016) (unpublished manuscript), https://arxiv.org/pdf/1608.00771.pdf [https://perma.cc/PQW8-8GCJ] (defining operational aspect as "the parts of the contract that we wish to automate, which typically derive from consideration of precise actions to be taken by the parties and therefore are concerned with performing the contract.").

252. Or perhaps creating a new niche for legal hackers. Following the DAO attack, security expert Robert Graham suggested that, "in the past, people hired lawyers to review complicated contracts. In the future, they'll need to hire hackers. After a contract is signed, I'm now motivated to hire a very good hacker that will keep reading the code until they can find some hack to my advantage." Robert Graham, *Ethereum/TheDAO Hack Simplified*, ERRATA SEC. (June 18, 2016), http://blog.erratasec.com/2016/06/etheriumdao-hack-similfied.html#.V2wGDOYrKV5 [https://perma.cc/9HLC-HRNM].

253. There are already technical auditing firms that review smart contract code for bugs or security vulnerabilities. *See* Alyssa Hertig, *Blockchain Veterans Unveil Secure Smart Contracts Framework*, COINDESK (Sept. 15, 2016), https://www.coindesk.com/blockchain-veterans-unveil-secure-smart-contracts-framework/ [https://perma.cc/L2MB-442J]. Traditional auditing firms are also considering how they might participate in this new world. As Grainne McNamara stated at a financial services conference, "we're looking at how to audit the technology using the technology." Grainne McNamara, Blockchain Strategist, PricewaterhouseCoopers, Address at the American Banker Blockchains + Digital Currencies Conference (June 13, 2017) (transcript on file with author).

254. *See Introducing OpenLaw*, CONSENSYS (July 25, 2017), https://media.consensys.net/introducing-openlaw-7a2ea410138b [https://perma.cc/T896-2LCU].

255. *See Clause.io Sets Out Strategy With Its Smart Contract Engine*, ARTIFICIAL LAW. (July 6, 2017), https://www.artificiallawyer.com/2017/07/06/clause-io-sets-out-strategy-with-its-smart-contract-engine/ [https://perma.cc/FE9J-VZVV]; *Agrello Becomes 1st LegalTech Co. To Launch Its Own Digital Currency*, ARTIFICIAL LAW. (July 17, 2017),

R3 consortium;[256] and the CommonAccord and Legalese projects.[257] Some of these are focused more on the non-operational side, making the process of legal contract drafting more efficient. Others are concentrating more on operational templates that can be incorporated into smart contract systems. By standardizing and reviewing the elements of the smart contract ahead of time, such mechanisms should cut down on the errors that led to failures such as The DAO hack.

As the contractual mechanisms around blockchains become more standardized and modularized, the line between enforcement through law and code will blur. Something similar has already occurred in derivatives trading, where standardized master agreements and terminology under the International Swaps and Derivatives Association (ISDA) allows widespread automation of transactions even without the use of distributed ledgers.[258]

C. MAKING CODE MORE LAW-LIKE

Just as regulators and lawyers can adapt to the blockchain environment, distributed ledger systems can become more hospitable to legal enforcement. The three main pathways being explored are to integrate the terms of legal and smart contracts, to integrate traditional legal enforcement mechanisms into smart contracts, and to integrate law-like governance processes into blockchain platforms.

1. Contractual Integration

The simplest way to make blockchain-based systems more consistent with legal enforcement is literally to connect the two. Even if smart contracts can be enforced in court under basic principles of contract law, they serve a different function than the fundamentally remedial institution of contract.[259] Smart contracts are good at setting forth anticipated conditions and consequences *ex ante*, and then ensuring the consequences occur upon fulfillment of the conditions. Legal contracts are good at cleaning up the mess when, inevitably, things do not go according to plan. There is no reason, however, that the two mechanisms cannot coexist. Difficulties arise when the

https://www.artificiallawyer.com/2017/07/17/agrello-becomes-1st-legaltech-co-to-launch-its-own-digital-currency/ [https://perma.cc/578M-W5XQ].

256. *See generally* Clack, et al., *supra* note 251.

257. COMMONACCORD, http://commonaccord.org [https://perma.cc/D7LZ-BAYG] (last visited Sept. 2, 2018); LEGALESE, http://legalese.com [https://perma.cc/2TUM-7SXM] (last visited Sept. 2, 2018).

258. *See* INT'L SWAPS & DERIVATIVES ASS'N., The Future of Derivatives Processing and Market Infrastructure [hereinafter ISDA WHITE PAPER] (Sept. 2016), at 15, https://www2.isda.org/attachment/ODcwMA==/Infrastructure%20white%20paper.pdf [https://perma.cc/KE4P-BZDS].

259. *See* Werbach & Cornell, *supra* note 25, at 318.

smart and legal contracts disregard one another, as in The DAO collapse.

The alternative approach is to pair smart contracts and legal contracts explicitly. Information security expert Ian Grigg first explored this idea in 2004, before the advent of cryptocurrencies, as part of the Ricardo digital transaction platform for financial instruments.[260] Ricardo defined its contracts as having three components: legal code (the human-readable text of a contract), computer code (the executable steps of s smart contract), and parameters (the variables that influence how the computer code executes). The legal code included the cryptographic hash string of the computer code, which guaranteed that it was referencing the proper smart contract. In parallel, the smart contract included the cryptographic hash string of the legal contract text. Thus, the two were definitely linked. If there was a problem with the smart contract, one could turn to the legal contract for resolution. Grigg called this structure the Ricardian contract because it was developed for the Ricardo system.[261]

Like Szabo's original notion of smart contracts, Ricardian contracts were largely a theoretical construct prior to the blockchain, and in particular, Ethereum's successful implementation of blockchain smart contracts.[262] The approach has since been rediscovered. Several groups are building solutions using the mutual hashing of smart and legal contracts, including a subgroup of the R3 consortium led by the British bank Barclays,[263] the Monax Burrow software now part of the Hyperledger open source project,[264] and OpenLaw.[265]

With this approach, the human and smart contracts explicitly reference one another through digital signatures. In contrast to The DAO terms of service, which privileged the algorithmic contract over the human-readable explanations, this approach makes each dependent on the other. A court or other decision-maker can use the conventional contract to understand the intent of the smart contract, which handles execution of the agreement.[266]

---

260. *See generally* Ian Grigg, *The Ricardian Contract*, *in* PROCEEDINGS OF THE FIRST IEEE WORKSHOP ON ELECTRONIC CONTRACTING 25 (2004).

261. *See id.* at 25.

262. The Ricardo platform that Grigg was building never took off.

263. *See* Clack et al., *supra* note 251, at 12; Bailey Reutzel, *BNP Paribas Works With Blockchain Startup to Open Source Law*, COINDESK (May 5, 2016), http://www.coindesk.com/commonaccord-legal-smart-contracts-prove-beneficial-one-bank-veritcal/ [https://perma.cc/P23T-DS6N]; Ian Allison, *Barclays' Smart Contract Templates Stars in First Ever Public Demo of R3's Corda Platform*, INT'L. BUS. TIMES (Apr. 18, 2016), http://www.ibtimes.co.uk/barclays-smart-contract-templates-heralds-first-ever-public-demo-r3s-corda-platform-1555329 [https://perma.cc/5SFT-XLAY].

264. *See Putting the Contracts in Smart Contracts*, MONAX, https://monax.io/explainers/dual_integration [https://perma.cc/YQK4-43LS].

265. *See supra* note 254.

266. In the wake of the DAO attack, researchers have proposed technical mechanisms

Every smart contract will not require a bespoke human-negotiated contract alongside it. As with the contract system today, forms will be widespread for business-to-consumer and low-value agreements. In many cases, the costs of dispute resolution will so far exceed the potential recovery that "quick-and-dirty" reliance on the naïve actions of machines will be sufficient. Regulation of intermediaries such as registries may obviate the need to specify legal terms for every associated smart contract. As blockchain-based systems become more familiar, a combination of customer, common law, and model legislation is likely to develop to address common situations.

2. Oracles and Computational Courts

Contractual integration links the substantive terms of a legal agreement with those of a smart contract. A different approach is to take some aspects of enforcement out of the automated system of the smart contract. In other words, a smart contract can be self-executing but not fully self-enforcing, thus avoiding the ambiguities and limitations of automated code-based enforcement.

Many smart contracts will already need to interface with the outside world. For example, a call option to buy a security at a certain price can be executed algorithmically on the blockchain, with payment in bitcoin or another cryptocurrency. The blockchain, however, does not know stock prices. That information must be provided to the smart contract through an external connection, either to an automated data source or a human arbiter. Those external sources are called oracles.[267] Some oracles are just traditional data feeds designed with interfaces for smart contracts to process them in an automated way. Thomson Reuters, one of the largest business publishing firms, is making some of its data feeds available in a manner designed to function as smart contract oracles.[268] Oraclize is a startup focused entirely on

tantamount to rescission of smart contracts, without necessarily involving judicial actors. *See, e.g.*, Ittay Eyal & Emin Gun Sirer, *A Decentralized Escape Hatch for DAOs*, HACKING, DISTRIBUTED (July 11, 2016), http://hackingdistributed.com/2016/07/11/decentralized-escape-hatches-for-smart-contracts/ [https://perma.cc/6DBH-487G] (proposing an "escape hatch" mechanism in which all transactions would be buffered and subject to reversion based on a crowdsourcing mechanism); Bill Marino & Ari Juels, *Setting Standards for Altering and Undoing Smart Contracts*, *in* RULE TECHNOLOGIES. RESEARCH, TOOLS, AND APPLICATIONS: 10TH INTERNATIONAL SYMPOSIUM, RULEML 2016, STONY BROOK, NY, USA, JULY 6–9, 2016. PROCEEDINGS 151 (2016) (detailing scenarios for modifying or rescinding smart contracts).

267. *See* Stefan Thomas & Evan Schwartz, *Smart Oracles: A Simple, Powerful Approach to Smart Contracts* (July 17, 2014), https://github.com/codius/codius/wiki/Smart-Oracles:-A-Simple,-Powerful-Approach-to-Smart-Contracts [https://perma.cc/S5TV-Q3JH].

268. *See* Maria Terekhova, *Thomson Reuters Is Making a Blockchain Push*, BUS. INSIDER (June 15, 2017), http://www.businessinsider.com/thomson-reuters-is-making-a-blockchain-push

turning data feeds into oracles.[269]

As Wright and De Filippi point out, oracles could be extended to dispute resolution by courts or private actors.[270] Oracles can also be humans. Consider a simple smart contract in which each of the parties has a private key and a third key is given to an expert arbitrator. The smart contract requires two of three keys in order to execute. If the parties agree the contract has been fully performed, they each provide their key and the smart contract executes. If there is a dispute, they turn to the arbitrator. She either provides her key along with that of the party seeking to enforce the contract or refuses it and therefore prevents completion of the transaction. This system mimics a legal arbitration process.

Smart contracts could by default incorporate arbitration mechanisms or rollback provisions. They could be designed to operate only in extreme cases, with high barriers through the design of the multisignature (or "multisig") process. This would help address extraordinary cases such as The DAO attack. Or they could be used to create a regular outlet for private dispute resolution, the way so many business-to-consumer form contracts today push disputes into arbitration. Balaji Srinavasan, a noted blockchain investor and founder of the startup 21, suggests that, "over time blockchains will provide 'rule-of-law-as-a-service' as an international, programmable complement to the Delaware Chancery Court."[271]

The distributed nature of the blockchain may call for new enforcement mechanisms that are themselves distributed.[272] For example, new international arbitration networks might need to be developed that were tuned to the needs of blockchain disputes, much as the World Intellectual Property Organization created the Uniform Dispute Resolution Process (UDRP) to handle trademark disputes over Internet domain names.[273] However, because arbitration

-2017-6 [https://perma.cc/P8HK-GV8L].

269. ORACLIZE, http://oraclize.it (last visited Sept. 3, 2018) [https://perma.cc/5CP7-VV8H].

270. *See* Wright & De Filippi, *supra* note 23, at 50.

271. Balaji S. Srinivasan, *Thoughts on Tokens*, MEDIUM (May 27, 2017), https://medium.com/@balajis/thoughts-on-tokens-436109aabcbe [https://perma.cc/NK5P-KNU6].

272. Ethereum creator Vitalik Buterin has speculated about a regime of "decentralized courts" to resolve disputes. *See* Vitalik Buterin, *Decentralized Court*, REDDIT, https://www.reddit.com/r/ethereum/comments/4gigyd/decentralized_court/ [https://perma.cc/M5UY-5A39] (last visited Sept. 2, 2016); Izabella Kaminska, *Decentralised Courts and Blockchains*, FIN. TIMES (Apr. 29, 2016), http://ftalphaville.ft.com/2016/04/29/2160502/decentralised-courts-and-blockchains/ [https://perma.cc/BRV3-EBC6].

273. *See generally* Luke A. Walker, *ICANN's Uniform Domain Name Dispute Resolution Policy*, 15 BERKELEY TECH. L.J. 289 (2000).

decisions could, in some cases, be directly executed on the blockchain and would apply on a peer-to-peer basis, blockchain arbitration systems would be different than any current example.[274] Andreas Antonopoulos and Pamela Morgan proposed a decentralized arbitration and mediation network (DAMN) in 2016.[275]

Even more speculative—yet under development today in some blockchain-based projects—are computational courts, or as they are sometimes called, computational juries. Instead of arbitrators resolving disputes, these mechanisms employ the wisdom of the crowd through prediction markets.[276] The Augur Ethereum-based prediction market is developing this approach internally. One reason real-money prediction markets such as Intrade have been shut down by regulators is that they can be used in illegal or unethical ways. A prediction market for murder of one's mother-in-law, for example, would be troublesome.

Augur proposes to address such unethical markets through the same reporting process it uses to verify outcomes of predictions. Augur uses a system in which participants in the marketplace purchase a token called Rep.[277] When someone creates a contract, such as a prediction that the President will be impeached within a certain period of time, they post a bond in Rep. They win additional Rep if the prediction is correct and lose the bond if incorrect. A randomly selected group of reporters (analogous to a jury) are tasked with verifying the outcome. Those reporters must also post a bond. The reports can be challenged, and if a second randomly selected jury agrees with the challenge, the reporter providing incorrect information loses her bond. This process is designed to produce verified outcomes without having to trust a specific central authority. It is admittedly complicated, and could fail. The process, though, illustrates a promising pathway to make decentralized blockchain-

274. *See* Abramowicz, *supra* note 47, at 405.

275. *See* Michael del Castillo, *Lawyers Be DAMNed: Andreas Antonopoulos Takes Aim at Arbitration With DAO Proposal*, COINDESK (May 26, 2016), http://www.coindesk.com/damned-dao-andreas-antonopoulos-third-key/ [https://perma.cc/VW7G-E5FK]. It is based on the New York Convention, under which sixty-five countries agreed that their courts would enforce decisions of recognized arbitrators. The tradeoff of an arbitration regime is that it reintroduces intermediation to the decentralized blockchain environment. *See* James Grimmelmann & Arvind Narayanan, *The Blockchain Gang*, SLATE (Feb. 16, 2017), http://www.slate.com/articles/technology/future_tense/2016/02/bitcoin_s_blockchain_technology_won_t_change_everything.html [https://perma.cc/7RGA-YMAC] ("[A]n arbitrator who can give you back your car is also an arbitrator who can take your car away from you. He's an intermediary of precisely the sort the block chain was supposed to eliminate.").

276. *See* Rizzo, *supra* note 178.

277. *See* Tony Sakich, Jeremy Gardner & Joey Krug, *What Is Reputation?* (June 18. 2015), http://augur.strikingly.com/blog/what-is-reputation [https://perma.cc/B35A-EAMS].

based technology operate more like the established institutions of the legal system.

Any of these voluntary mechanisms could be baked into blockchain applications, or even in some cases legally mandated. The full range of incentives and governance mechanisms could be used to encourage compliance with desirable approaches. Furthermore, just as the Federal Arbitration Act directs courts to accept private arbitration decisions when fraud is not involved, legislation could create similar legal force for appropriately designed blockchain dispute resolution systems.[278]

3. On-Chain Governance

One of the biggest problems with blockchain networks as governance institutions is that it is difficult to change their foundational rules. Systems that have well-structured mechanisms for considering and implementing changes to consensus rules or other technical attributes are not fundamentally decentralized. They may operate more like industry standards bodies or open source projects, where rule changes occur through collective agreement rather than the hierarchical edicts of corporate management.

Ethereum resembles Wikipedia more than General Electric. Wikipedia is a great example of how a novel organizational approach combined with massive user participation can transform a market.[279] It not only replaced other encyclopedias, it created perhaps the biggest open information resource in history. If Ethereum achieves as much, it will be a tremendous success story. But the promise of Ethereum and other blockchain networks is greater still. To be truly transformative, these systems would have to evolve their governance using the same decentralized approach they use to enforce it.

Even though Bitcoin lacks a formal governance structure, its developers have rigged a voluntary signaling mechanism called BIP 9.[280] Under BIP 9, miners can broadcast their willingness and readiness to adopt changes. This process was used for the Segwit upgrade. Segwit is automatically activated on the Bitcoin network after a threshold of 80 percent network hashing power signaled for it.[281] While BIP 9 thus enables a crude voting mechanism for controversial Bitcoin protocol upgrades, it leaves much to be desired as on-chain governance. The thresholds for approval are arbitrary. They are set

278. *See* Federal Arbitration Act, 9 U.S.C. § 10 (2012).

279. *See generally* YOCHAI BENKLER, THE WEALTH OF NETWORKS (2006); DON TAPSCOTT & ANTHONY D. WILLIAMS, WIKINOMICS: HOW MASS COLLABORATION CHANGES EVERYTHING (2008).

280. BIP stands for Bitcoin Improvement Proposal. It is a mechanism to propose technical changes to Bitcoin for community review based on the Internet Engineering Task Force's "Request for Proposal" process.

281. This process was technically referred to as BIP 91.

centrally by those who propose the upgrades. Even more important, BIP 9 only signals; it does not enforce policies. Debates about scaling Bitcoin still require agreement among a critical mass of network participants.

There are several efforts underway to create true on-chain governance. A project called Rootstock is trying to create a smart contracts layer on top of Bitcoin, with a built-in process giving both miners and users power to make binding votes on network changes. Decred and Tezos are building entirely new blockchains with governance mechanisms baked in. These systems use various algorithms to allow network participants to vote on changes to the protocol, which are automatically implemented when adopted. Decred successfully executed a change to its algorithm for allocating these voting tokens using the governance mechanism in Spring 2017.[282] Tezos, which raised $200 million in one of the largest initial coin offerings, has generated tremendous interest for its governance approach.[283]

There are limitations to these systems. They internalize many aspects of the rules governing distributed ledger systems. However, they rely on hard-coded rules for democratic voting to carry out changes. This may be a very good way to govern; it may even be, to paraphrase Winston Churchill, the best possible among a set of bad options.[284] It is not perfect. Any governance structures that are imperfect will eventually need to be modified by someone. Moreover, humans need to define the rule changes that network participants vote on, and code the software to implement them if adopted. The on-chain governance systems make the blockchains operate more like a human-based legal or governance regime, but they still leave gaps that traditional institutions must fill.

V. CONCLUSION: STRANGE BLOCKFELLOWS

Distributed ledgers are the first foundational technology in twenty years whose potential impact matches that of the Internet. At a time when trust in centralized power structures is waning, the blockchain's "trustless trust" offers

282. *See* Christine Chiang, *Decred Launches Decentralized Voting Process for Blockchain Protocol Changes*, BRAVE NEWCOIN (June 17, 2017), https://bravenewcoin.com/news/decred-launches-decentralized-voting-process-for-blockchain-protocol-changes/ [https://perma.cc/9F8B-2F7L].

283. *See* Alice Lloyd George, *Behind the Scenes With Tezos, a New Blockchain Upstart*, TECHCRUNCH (July 12, 2017), https://techcrunch.com/2017/07/12/behind-the-scenes-with-tezos-a-new-blockchain-upstart/ [https://perma.cc/HTC6-H5D3].

284. *See* Winston S. Churchill, *The Worst Form of Government*, INT'L CHURCHILL SOC'Y (Nov. 11, 1947), https://winstonchurchill.org/resources/quotes/the-worst-form-of-government/ [https://perma.cc/XD75-Y7BB] ("No one pretends that democracy is perfect or all-wise. Indeed it has been said that democracy is the worst form of Government except for all those other forms that have been tried from time to time . . . .").

a compelling alternative. Further growth will depend partly on technical advances, partly on adoption patterns, partly on the business innovations built on top of distributed ledger platforms, and partly on resolution of the governance challenges to the blockchain's trust architecture. It is tempting to see law and regulation primarily as impediments to these processes, but that would be a mistake. Too much law could stifle the blockchain or drive it underground, yet so could too little law.

These are still early days for the blockchain. Satoshi Nakamoto's Bitcoin white paper was published less than a decade ago, and Ethereum just launched in 2015. As big as the market has grown, there is far less at stake, and therefore far less path dependence, than there will be in three, or five, or ten years. Now is the time to develop hybrids of law and code. Regulators, legislators, and courts can take the initiative to create both clarity and explicit spaces for experimentation. Blockchain developers must also take responsibility to find common ground.

Like the Internet, the blockchain is a foundational technology,[285] whose impacts could reach into every corner of the world. To move forward, though, law and distributed ledgers need each other.

285. *See* Iansiti & Lakhani, *supra* note 16 (describing foundational technologies).

FINAL REPORT OF THE BERKELEY CENTER FOR LAW & TECHNOLOGY SECTION 101 WORKSHOP: ADDRESSING PATENT ELIGIBILITY CHALLENGES

Jeffrey A. Lefstin[†], *Peter S. Menell*[††] *& David O. Taylor*[†††]

ABSTRACT

Over the past five years, the Supreme Court has embarked upon a drastic and far-reaching experiment in patent eligibility standards. Since the founding era, the nation's patent statutes have afforded patent protection to technological innovations and practical applications of scientific discoveries. However, the Supreme Court's 2012 decision in *Mayo Collaborative Services v. Prometheus Laboratories* imposed a new limitation on the scope of the patent system: a useful application of a scientific discovery is ineligible for patent protection unless the inventor also claims an "inventive" application of the discovery. The following year, the Court ruled that discoveries of the location and sequence of DNA compositions that are useful in diagnosing diseases are ineligible for patent protection in *Association for Molecular Pathology v. Myriad Genetics, Inc.* Additionally, in its 2014 *Alice Corp. v. CLS Bank International* decision, the Court ruled that software-related claims are ineligible for patent protection unless the abstract ideas or mathematical formulas disclosed are inventively applied.

These decisions sent shock waves through the research, technology, business, and patent communities. Medical diagnostics companies experienced a dramatic narrowing of eligibility for core scientific discoveries. Reactions within the information technology community have been mixed, with some applauding the tightening of patent eligibility standards on software claims and the opportunity to seek early dismissal of lawsuits, particularly those filed by non-practicing entities, and others criticizing the shift in patent eligibility. Several members of the Federal Circuit bluntly criticized the Supreme Court's shift in patent eligibility standards on jurisprudential and policy grounds. Additionally, the Patent Office has struggled to apply the Supreme Court's new and rapidly evolving standards.

As this sea change unfolded, many patent practitioners, scholars, PTO officials, and jurists hoped that the Supreme Court would provide fuller and clearer guidance on patent eligibility

---

DOI: https://doi.org/10.15779/z38MW28F2T

† Professor of Law and Associate Academic Dean, University of California Hastings College of Law.

†† Koret Professor of Law and Director, Berkeley Center for Law & Technology, University of California at Berkeley School of Law.

††† Associate Professor of Law and Co-Director of the Tsai Center for Law, Science and Innovation, SMU Dedman School of Law.

We thank Richard Fisk for administrative assistance in planning the workshop and Amit Elazari, Andrea Hall, and Reid Whitaker for research assistance.

standards. In the aftermath of the Supreme Court rejecting the invitation to reexamine its *Mayo* decision, many stakeholders have shifted their attention toward legislative reforms. This Report summarizes the presentations and discussion of a workshop that included leading industry representatives, practitioners, scholars, policymakers, and a retired jurist exploring the legal background and effects bearing on legislative action.

TABLE OF CONTENTS

I. INTRODUCTION

Over the past five years, the Supreme Court has embarked upon a drastic and far-reaching experiment in patent eligibility standards. Since the beginning of the American patent system, the nation's patent statutes have afforded patent protection to technological innovations and practical applications of scientific discoveries.[1] As the Supreme Court explained long ago, although no one can patent a natural phenomenon or "principle, *in the abstract*" (such as steam power, electricity, or "any other power in nature"), the patent system has recognized an invention in "*applying* [the processes used to extract, modify, and concentrate natural phenomena] to useful objects."[2]

Notwithstanding the relative stability of this long-standing legal principle[3] and in the absence of any legislative change, the Supreme Court engrafted an additional substantive requirement for patent eligibility of scientific discoveries in its 2012 *Mayo Collaborative Services. v. Prometheus Laboratories* decision.[4] The Court unanimously held that a useful application of a scientific discovery is ineligible for patent protection unless the inventor has claimed an additional "inventive" application of the discovery.[5] The following year, the Court ruled that the discovery of an isolated DNA sequence useful in diagnosing diseases

1. *See* Brief of Professors Jeffrey A. Lefstin & Peter S. Menell as Amici Curiae in Support of Petitioner for a Writ of Certiorari at 4–14, Sequenom, Inc. v. Ariosa Diagnostics, Inc., 136 S. Ct. 2511 (2016) (No. 15-1182), 2016 WL 1605520 [hereinafter Lefstin-Menell Sequenom Amicus Cert. Petition Brief].

2. Le Roy v. Tatham, 55 U.S. 156, 175 (1853) (emphasis added).

3. The Supreme Court's decisions in *Funk Bros. Seed Co. v. Kalo Inoculant Co.*, 333 U.S. 127 (1948) and *Parker v. Flook*, 437 U.S. 584 (1978) arguably strayed from this principle. However, *Funk Brothers* was largely ignored following the enactment of the 1952 Patent Act, and *Flook* was effectively overruled three years later in *Diamond v. Diehr*, 450 U.S. 175 (1981).

4. *See* Mayo Collaborative Servs. v. Prometheus Labs., Inc., 566 U.S. 66 (2012).

5. *See id.* at 81.

is ineligible for patent protection, regardless of whether the sequence would be novel or non-obvious over the prior art.[6] Additionally, in its 2014 *Alice Corp. v. CLS Bank International* decision,[7] the Court ruled that software-related claims are ineligible for patent protection unless the abstract ideas, algorithms, or mathematical formulas disclosed are inventively applied.[8]

These decisions have sent shock waves through the research, technology, business, and patent communities. Medical diagnostics companies have experienced a dramatic narrowing of eligibility for core scientific discoveries.[9] Reactions within the digital and high technology community have been mixed.[10] Many high technology companies that rely on software innovation—ranging from start-ups to Google—and their customers welcomed the tightening of patent eligibility standards on software claims and the opportunity to seek early dismissal of lawsuits, particularly those filed by non-practicing entities.[11] At the same time, other high technology companies that also rely on software innovation—ranging from start-ups seeking financing to IBM—have been sharply critical of the shift in the patent eligibility landscape.[12] Several members of the Federal Circuit have bluntly criticized the Supreme Court's shift in patent eligibility standards on jurisprudential and policy grounds.[13] Additionally, the Patent Office has struggled to apply the Supreme

6. *See* Ass'n for Molecular Pathology v. Myriad Genetics, 569 U.S. 576 (2013) (holding that synthetic derivatives of naturally occurring molecules may be patent-eligible under 35 U.S.C. § 101, seemingly without any requirement that the synthetic molecule represent an inventive advance over the naturally occurring species).

7. *See* Alice Corp. v. CLS Bank Int'l, 134 S. Ct. 2347 (2014).

8. *See id.* at 2359–60. The Court concluded that the representative method claim did no more than implement the abstract idea of intermediated settlement on a generic computer and that the system and media claims added nothing of substance to the underlying abstract idea.

9. *See* U.S. PATENT & TRADEMARK OFFICE, PATENT ELIGIBILITY SUBJECT MATTER: REPORT ON VIEWS AND RECOMMENDATIONS FROM THE PUBLIC 35–36 (July 2017), https://www.uspto.gov/sites/default/files/documents/101-Report_FINAL.pdf [https://perma.cc/XPX9-XW3Y] [hereinafter USPTO REPORT].

10. *See id.* at 37.

11. *See id.* at 24–27, 37.

12. *See id.* at 37–38.

13. *See* Ariosa Diagnostics Inc. v. Sequenom, Inc., 788 F.3d 1371, 1380–81 (Fed. Cir. 2015) (Linn, J., concurring) (noting that "[t]he Supreme Court's blanket dismissal of conventional post-solution steps" bars patent eligibility to *Sequenom*'s "truly meritorious" invention and that the invention at issue would have been valid under the standards reflected in *Le Roy v. Tatham*, 63 U.S. 132, 135–36 (1859) (whether the claimed invention "effectuate[d] a practical result and benefit not previously attained") (quoting Househill Coal & Iron Co. v. Neilson, 8 Eng. Rep. 616 (H.L. 1843), *reprinted in* 1 WEBSTER'S PATENT CASES 673, 683 (1844) and Le Roy, 55 U.S. at 175); Ariosa Diagnostics, Inc. v. Sequenom, Inc., 809 F.3d 1282, 1286–87 (Fed. Cir. 2015) (Lourie, J., concurring in the denial of en banc rehearing) (noting that although the claims at issue "recite innovative and practical *uses* for the [law of nature] . . . [the *Mayo* decision] unfortunately obliged [us] to divorce the additional steps from the asserted

Court's new and rapidly evolving standards.[14]

As this sea-change unfolded, many patent practitioners, scholars, PTO officials, and jurists hoped that the Supreme Court would provide fuller and clearer guidance on patent eligibility standards. After all, the Court's sudden shift in patent eligibility standards was neither squarely posed nor carefully briefed in the *Mayo* case.[15] With the exception of one amicus brief, based upon a questionable understanding of historical precedent,[16] none of the many briefs

---

natural phenomenon to arrive at a conclusion that they add nothing innovative to the process," and commenting that "it is unsound to have a rule that takes inventions of this nature out of the realm of patent-eligibility on grounds that they only claim a natural phenomenon plus conventional steps") (emphasis in original); *id.* at 1289 (Dyk, J., concurring in the denial of en banc rehearing) ("[T]here is a problem with *Mayo* insofar as it concludes that inventive concept cannot come from discovering something new in nature—*e.g.*, identification of a previously unknown natural relationship or property. In my view, *Mayo* did not fully take into account the fact that an inventive concept can come not just from creative, unconventional application of a natural law, but also from the creativity and novelty of the discovery of the law itself. This is especially true in the life sciences, where development of useful new diagnostic and therapeutic methods is driven by investigation of complex biological systems. I worry that method claims that apply newly discovered natural laws and phenomena in somewhat conventional ways are screened out by the *Mayo* test."); *id.* at 1294 (Newman, J., dissenting from the denial of en banc rehearing) (questioning *Mayo*'s breadth: "[p]recedent does not require that all discoveries of natural phenomena or their application in new ways or for new uses are ineligible for patenting").

14. The USPTO has issued numerous guidance documents during the past several years in an effort to keep up with the shifting patent eligibility jurisprudence. *See infra* app. C (USPTO Patentable Subject Matter Guidance Documents).

15. *See generally* Brief for Petitioners, Mayo Collaborative Servs. v. Prometheus Labs., Inc., 566 U.S. 66 (2012) (No. 10-1150), 2011 WL 3919717 [hereinafter Brief for Petitioners] (focusing brief on overbreadth of the Prometheus patent claims, not arguing for an inventive application test, and making no mention of the *Neilson v. Harford* decision); *see also* Brief for the United States as Amicus Curiae in Support of Neither Party at 9–11, Mayo Collaborative Servs., 566 U.S. 66 (No. 10-1150), 2011 WL 4040414 [hereinafter Brief for the United States] (asserting that claims at issue were patent-eligible and do not preempt all practical uses of the law of nature, but are likely invalid under Sections 102 (novelty) and 103 (nonobviousness)). Moreover, the Supreme Court's 2010 *Bilski v. Kappos* decision, 561 U.S. 593 (2010), took a cautious, textual approach to patent eligibility and expressly "decline[d] to impose limitations on the Patent Act that are inconsistent with the Act's text." *Id.* at 612. The breadth and analytical basis for the *Mayo* decision came as a shock to many practitioners and scholars.

16. The brief filed by Professor Joshua Sarnoff on behalf of nine law professors, Brief of Nine Law Professors as Amici Curiae in Support of Petitioners, Mayo Collaborative Servs., 566 U.S. 66 (No. 10-1150), 2011 WL 4071921 [hereinafter Sarnoff *Mayo* Amicus Brief], contended that the English Court of the Exchequer's decision in *Neilson v. Harford*, 151 Eng. Rep. 1266 (Ex. 1841), http://www.commonlii.org/uk/cases/EngR/1841/887.pdf [https://perma.cc/7RNA-UZ85], *reprinted in* 1 WEBSTER'S PATENT CASES 295 (1844), established the principle that scientific discoveries should be treated as part of the prior art and that this principle was brought into U.S. law through *O'Reilly v. Morse*, 56 U.S. 62 (1853). *See* Sarnoff *Mayo* Amicus Brief at 8–10. However, as Professor Lefstin's research demonstrates, the Court of Exchequer was not setting forth a broad principle that scientific discoveries or

submitted in *Mayo* framed the fundamental shift in patent eligibility doctrine that emerged.[17] When the Supreme Court later denied a petition for a writ of certiorari, without even requesting the views of the government through the Solicitor General,[18] in *Sequenom, Inc. v. Ariosa Diagnostics, Inc.*—a case that many Federal Circuit jurists, scholars, and practitioners regarded as an ideal vehicle for clarifying patent eligibility standards[19]—attention turned toward the legislative arena.

In the aftermath of the Supreme Court rejecting the invitation to reexamine its earlier *Mayo* decision in *Sequenom*, we began planning a roundtable discussion among leading industry representatives, practitioners, scholars, policymakers, and retired jurists to explore the patent eligibility landscape and possible legislative solutions to the problems that have emerged. Drawing on the prior experience of the Berkeley Center for Law & Technology (BCLT) in hosting roundtables on salient intellectual property issues,[20] in the fall of 2016 we began planning this event with funding from Google and Intel

laws of nature are to be treated as known or in the prior art. *See* Jeffrey A. Lefstin, *Inventive Application: A History*, 67 FLA. L. REV. 565, 580–87 (2015). Rather, the pertinent language from *Neilson v. Harford* quoted in the Sarnoff *Mayo* Amicus Brief and repeated in the *Mayo* decision addressed whether Neilson's invention—the preheating of air injected into a hot blast furnace—constituted a claim to a machine or an abstract principle. *See infra* text accompanying notes 80–88. Furthermore, as Professors Lefstin and Menell have revealed, neither the patent statutes nor the legislative history of these enactments dating back to the nation's founding contain any hint of a second, "inventive application" hurdle for patent eligibility of scientific discoveries. *See* Lefstin-Menell Sequenom Amicus Cert. Petition Brief, *supra* note 1, at 4–14.

17. Neither the Petitioners' opening brief nor the government's brief discussed the *Neilson v. Harford* decision. *See* Brief for Petitioners, *supra* note 15; Brief for the United States, *supra* note 15. The Respondent's brief noted that "the patent in *Neilson* wholly preempted the 'natural phenomenon' that 'heating the blast, in a receptacle, between the blowing apparatus and the furnace' would cause iron to smelt more rapidly in a furnace." Brief for Respondent at 39, Mayo Collaborative Servs., 566 U.S. 66 (No. 10-1150), 2011 WL 5189089. The Petitioners' reply brief argued that *Neilson v. Harford* is "irrelevant . . . because the patents . . . narrowly confined a scientific principle within a process that left other uses freely available." *See* Reply Brief for Petitioners at 21, Mayo Collaborative Servs., 566 U.S. 66 (No. 10-1150), 2011 WL 5562514 (stating only that "*Neilson* upheld a patent on a mechanical apparatus for blowing hot air into a furnace, having discovered that hot air worked better than cold"). None of these briefs addressed or explained the excerpt from *Neilson* on which the Supreme Court erroneously based the "inventive application" doctrine. *See* Lefstin-Menell Sequenom Amicus Cert. Petition Brief, *supra* note 1, at 15–20.

18. *See* Sequenom, Inc. v. Ariosa Diagnostics, Inc., 136 S. Ct. 2511 (2016).

19. *See* USPTO REPORT, *supra* note 9, at 11; *see Sequenom, Inc. v. Ariosa Diagnostics, Inc.*, SCOTUSBLOG (compiling certiorari petition party and 22 amici briefs), http://www.scotusblog.com/case-files/cases/sequenom-inc-v-ariosa-diagnostics-inc/ [https://perma.cc/9NVN-MFHP].

20. *See, e.g.*, Stuart Graham, Peter Menell, Carl Shapiro, & Tim Simcoe, *Final Report of the Berkeley Center for Law & Technology Patent Damages Workshop*, 25 TEX. INTELL. PROP. L.J. 115 (2018).

Corporation. We insisted on and received complete independence from the funding organizations.

We sought participants with significant knowledge and experience in the key industries affected by the shift in patent eligibility standards—principally the bioscience and software fields. To promote candid discussion among these participants, we established the following ground rules: (1) Participants would be free to use the information received, but neither the identity nor the affiliation of the speaker(s) could be revealed; (2) We would prepare a report describing the results of the workshop—and that report would not attribute statements or views to individuals (other than the co-convenors); and (3) The report would list the participants and be made available to the public through BCLT. Appendix A contains the Workshop Schedule. Appendix B contains the list of participants. Appendix C lists the preparatory materials that we distributed to the participants in advance of the workshop. This document constitutes the workshop report.

Part I contains a lightly edited version of the background document that we circulated to participants prior to the workshop. Part II summarizes the four workshop sessions leading up to the discussion of legislative proposals: (A) legal background; (B) effects on research and development (R&D); (C) effects on patent prosecution; and (D) effects on patent assertion, litigation, and case management. Part III summarizes the discussion of legislative proposals and sets forth a framework for seeking compromise on reform legislation.

II. BACKGROUND MEMO

A. LEGAL BACKGROUND AND WORKSHOP GOALS

Over the past several years, the Supreme Court has embarked on a dramatic experiment in patent eligibility jurisprudence. For most of American patent law history, the boundary of the patent system was drawn between abstract principles and practical applications of those principles as embodied in statutorily-defined categories of inventions. Although augmented by limitations to the technological arts and by the exclusion of mental steps and printed matter, the distinction between abstractions and practical applications remained the primary test of patent eligibility since the nation's founding era.

In *Gottschalk v. Benson* (1972),[21] *Parker v. Flook* (1978),[22] and *Diamond v. Diehr* (1981),[23] the Supreme Court charted an uncertain course as it confronted advances in information technologies. The Court's decisions vacillated among

21. Gottschalk v. Benson, 409 U.S. 63 (1972).
22. Parker v. Flook, 437 U.S. 584 (1978).
23. Diamond v. Diehr, 450 U.S. 175 (1981).

multiple rationales for the patent eligibility doctrine: a requirement of tangibility; hesitation to extend the reach of the patent system to areas unanticipated by Congress; and the exclusion of concepts that had "always existed" such as laws of nature and basic mathematical relationships. And while each case presented a different vision of 35 U.S.C. § 101—the statutory section governing patent eligibility—the Court maintained a pretense that each was consistent with its long-standing principles. Nonetheless, at the end of its path in *Diehr*, the Court reaffirmed two traditional foundations of the patent eligibility doctrine: that the boundary of eligible subject-matter lay between abstract principles and practical applications of those principles,[24] and that considerations of prior art play no role in determining eligibility under § 101.[25]

Nearly thirty years after *Diehr*, the Court reopened the interpretation of § 101 in *Bilski v. Kappos*.[26] *Bilski* acknowledged that Congress had not limited patent-eligible subject matter other than setting forth the eligible categories of inventions in § 101.[27] Nonetheless, the Court concluded that "as a matter of statutory *stare decisis* going back 150 years,"[28] its precedents demanded the exclusion of "laws of nature, physical phenomena, and abstract ideas."[29] *Bilski* declined to further explain the rationale for imposing extra-textual limitations on patent-eligible subject matter or explain how such limitations were to be applied in practice.

However, in *Mayo Collaborative Services v. Prometheus Laboratories*, the Court grounded the patent eligibility doctrine in the rationale that patents preempting access to fundamental principles would foreclose more innovation than they would promote.[30] At the same time, drawing on a markedly ahistorical reading of foundational nineteenth century cases such as *Neilson v. Harford*,[31] *O'Reilly v.*

24. *See id.* at 187 ("It is now commonplace that an *application* of a law of nature or mathematical formula to a known structure or process may well be deserving of patent protection."); *id.* at 191 ("We recognize, of course, that when a claim recites a mathematical formula (or scientific principle or phenomenon of nature), an inquiry must be made into whether the claim is seeking patent protection for that formula in the abstract.").

25. *See id.* at 188–89 ("The 'novelty' of any element or steps in a process, or even of the process itself, is of no relevance in determining whether the subject matter of a claim falls within the § 101 categories of possibly patentable subject matter.").

26. Bilski v. Kappos, 561 U.S. 593 (2010).

27. *See id.* at 601.

28. *Id.* at 602.

29. *Id.* at 601. It was not until *Gottschalk v. Benson,* 409 U.S. 63 (1972), that abstract ideas were described as a separate category of excluded subject matter. *See id.* at 71–72; the Court's earlier precedents simply distinguished between principles (including laws of nature) in the abstract and practical applications. *See* Le Roy v. Tatham, 55 U.S. 156, 175 (1852).

30. *See* Mayo Collaborative Servs. v. Prometheus Labs., Inc., 566 U.S. 66, 71 (2012).

31. 151 Eng. Rep. 1266 (1841).

Morse,[32] and in Justice Douglas's 1948 opinion in *Funk Brothers*,[33] the *Mayo* Court suggested that the test for patent eligibility under § 101 was neither practical application nor the extent to which a claim preempted an underlying principle.[34] Instead, patent eiligibility would depend on whether the claim represented an "inventive" application of that principle.[35] In *Alice Corp.*,[36] the Court extended the *Mayo* framework to computer-implemented inventions, confirming that *Mayo*'s requirement for an "inventive concept" in the claim represents the new test for patent-eligible subject matter under § 101.[37]

The *Mayo/Alice* decisions established a two-step inquiry for determining patent eligibility:

> Step 1: Does the patent claim a patent-ineligible law of nature, natural phenomena, or abstract idea?
>
> Step 2: If so, does the claim nevertheless contain an inventive concept sufficient to transform the ineligible law of nature, natural phenomena, or abstract idea into a patent-eligible application of the ineligible subject matter?

The *Alice* decision emphasized the preemption concerns (identified in *Mayo*) as central to patent eligibility and characterized step two as a search for an "inventive concept"—i.e., an element or combination of elements that is "sufficient to ensure that the patent in practice amounts to significantly more than a patent upon the [ineligible concept] itself."[38] In so doing, the *Mayo* and *Alice* decisions brought considerations of prior art and claim scope, traditionally lodged in the statutory requirements of non-obviousness[39] and enablement or written description[40] into the patent eligibility determination.

Neither *Mayo* nor *Alice* addressed the legislative history of § 101's

---

32. 56 U.S. 62 (1853); *see generally*, Lefstin-Menell Sequenom Amicus Cert. Petition Brief, *supra* note 1.

33. Funk Bros. Seed Co. v. Kalo Inoculant Co., 333 U.S. 127 (1948).

34. *See Mayo*, at 566 U.S. at 72.

35. *See id.* at 66, 72–73.

36. Alice Corp. v. CLS Bank Int'l, 134 S. Ct. 2347 (2014).

37. *See id.* at 2355, 2357. The Court's omission of any reference to "inventive concept" in *Ass'n for Molecular Pathology v. Myriad Genetics, Inc.*, 133 S. Ct. 2107 (2013), in which the claims were directed to compositions of matter, had led some observers to question whether it was a universal requirement. While *Alice* confirmed that an "inventive concept" was required under § 101, the Court's analysis in *Alice* emphasized that the claims recited only a generic application of an abstract idea, rather than focusing on inventiveness per se.

38. *See Alice*, 134 S. Ct. at 2355 (quoting *Mayo*, 566 U.S. at 73) (alterations in original).

39. *See* 35 U.S.C. § 103 (2013).

40. *See* 35 U.S.C. § 112(a) (2013).

predecessor statutes, nor did they engage with the legislative text, history, or structure of the 1952 Act.[41] Moreover, the Court's decisions have left a raft of unanswered questions. Must a claim embodying an application of a newly discovered natural law satisfy a double requirement of both discovery and invention? Are inventive data-processing algorithms ineligible abstract ideas, or potentially eligible applications? What is the relationship between the underlying preemption rationale identified in *Mayo* and the actual test for patent eligibility? If the function of § 101 is to calibrate patent scope, how does that role relate to the other patentability doctrines of the 1952 Act?

The uncertainty and confusion resulting from the Court's recent jurisprudence create significant problems for many companies and investors contemplating research and development projects, as well as for patent prosecutors, patent examiners, and patent jurists.[42] In the decade prior to the *Mayo* decision, the USPTO rarely rejected patents on subject matter grounds, and one could count on one hand the number of judicial § 101 invalidity decisions in any year. Since *Mayo*, the number of § 101 invalidity rulings has skyrocketed, with more than one hundred invalidity determinations per year during the past two years.[43] Courts now routinely confront § 101 invalidity motions at the very outset of, and throughout, many patent cases. The USPTO has issued numerous guidance documents cataloging this rapidly evolving terrain.[44]

For some, the Supreme Court's rulings provide a ready means to eliminate some "unworthy" patents at an early stage of litigation. Yet given the lack of clarity in the test the Court has framed, do these rulings represent a return to the vague and subjective "I-know-it-when-I-see-it" standards for patentability that bedeviled the patent system before the 1952 Act? At the very least, we have witnessed an inversion of relative patent eligibility standards between the United States and other developed countries, some of which now maintain significantly more generous standards of patent-eligible subject matter.[45]

41. *See* Lefstin-Menell Sequenom Amicus Cert. Petition Brief, *supra* note 1, at 26–28.

42. *See generally* David O. Taylor, *Confusing Patent Eligibility*, 84 TENN. L. REV. 157 (2016).

43. *See infra*, tbl.1

44. *See infra* app. C, USPTO Patentable Subject Matter Guidance Documents.

45. *See* Kevin Madigan & Adam Mossoff, *Turning Gold into Lead: How Patent Eligibility Doctrine Is Undermining U.S. Leadership in Innovation*, 24 GEO. MASON L. REV. 939, 941 n.10 (2017) (reporting that over 1,700 patent applications covering the same inventions that were rejected in the U.S. as ineligible were considered eligible in both China and the European Union). The database identified the abandoned U.S. patent applications in the following fields (with the number of applications in each field shown in parentheses): Drug and Therapeutics (474); Molecular Biology and Microbiology (356); Amusement Devices (245); Combinatorial Chemistry (238); Measuring and Testing (83); Databases (80); Multicellular Living Organisms (38); Structural Design (35); Control Systems (21); Business Methods (18); Surgery (17); Chemistry (15); Immunology (15); Computer Graphics (14); Food Or Edible Materials (11);

Many observers saw a chance for the Supreme Court to moderate or at least clarify *Mayo*'s effect on patent eligibility in 2015. Relying on a narrow interpretation of *Mayo*, the Court of Appeals for the Federal Circuit held in *Ariosa Diagnostics v. Sequenom* that an innovative prenatal diagnostic test was ineligible under § 101, because the inventors, having discovered a natural phenomenon, had relied upon known means for its practical application.[46] Nonetheless, despite widespread support for reviewing the decision, the Court denied the writ of certiorari without even requesting the Solicitor General's views. The Court's refusal signals that the Court is not inclined to act on the serious challenges created by its recent jurisprudence and is unlikely to further refine its § 101 jurisprudence in the foreseeable future.[47] Responsibility now lies with Congress to bring greater clarity, consistency, and logic to patent eligibility.

The workshop aimed to: (1) identify areas of consensus and disagreement on the appropriate scope of patent eligibility; (2) understand the impact of the recent decisions on R&D, use of the patent system, and use of trade secret and copyright protection; and (3) explore potential legislative approaches to patent eligibility.

While various groups have been considering potential legislative reforms, there appears to be a substantial divide across the range of technology industries. The workshop aimed to provide a forum for discussing these perspectives and hopefully to bridge the divide through candid engagement.

B. SUMMARY OF LEGISLATIVE PROPOSALS

In the aftermath of the Court's denial of a writ of certiorari in *Sequenom*, various groups have proposed legislative reforms on patent eligibility.[48] The USPTO also has held workshops and solicited comments on patent

---

Agriculture (10); User Interfaces (9); Organic Compounds (8); Data Processing (5); Artificial Intelligence (3); Education And Demonstration (3); Electrolysis (3); Vehicle Navigation (3); Communications (2); Telecommunications (2); Coatings (2); Information Security (2); Cleaning & Compositions (2); Electro-Chemistry; (2) Marine Propulsion (1); Resins And Rubbers (1); Refrigeration (1); Compositions: Ceramic (1); Video Recording (1); Mineral Oils (1); Radiation Imagery (1); Dentistry (1); Registers (1); Image Analysis (1); Chemical Disinfecting (1); Digital Communications (1); Fluid Sprinkling (1); Power Plants (1); Radiant Energy (1); Error Detection (1); Adhesives (1); Evaporators (1).

46. *See* 788 F.3d 1371, 1377 (Fed. Cir. 2015). In a case decided after certiorari was denied in *Sequenom*, the Federal Circuit has seemingly placed less emphasis on the need for novelty in the inventor's means of application. *See* Rapid Litig. Mgmt. Ltd. v. CellzDirect, Inc., 827 F.3d 1042, 1051 (Fed. Cir. 2016).

47. *See* David O. Taylor, *Amending Patent Eligibility*, 50 U.C. DAVIS L. REV. 2149, 2157–64 (2017).

48. For an overview of various potential legislative reforms, *see generally id.*

eligibility.[49]

1. Result of Human Effort

The Intellectual Property Owners Association (IPO) proposal would amend the patent statute to replace the current two-part test with a test that would find a claim eligible if it describes something that is the result of human effort.[50] This approach harkens back to P.J. Federico's commentary[51] and the legislative history of the 1952 Patent Act, which suggested "anything under the sun made by man" might be eligible for patenting.[52]

2. Physicality

Another proposal would replace the current two-step test with a test that would find a claim eligible if it describes something that takes physical or tangible form. This approach excludes claims describing purely mental steps. The IPO proposal reflects this approach to the extent it recites that a "claimed invention is ineligible . . . if the claimed invention as a whole . . . exists solely in the human mind."[53]

3. Practical Application or Embodiment

A different proposal would not wholly replace the existing two-step test, but rather modify only the second part of that test. This proposal would replace the current search for an "inventive concept" or "inventive

49. *See* USPTO REPORT, *supra* note 9 at 23.

50. *See* INTELLECTUAL PROPERTY OWNERS ASS'N, PROPOSED AMENDMENTS TO PATENT ELIGIBLE SUBJECT MATTER UNDER 35 U.S.C. § 101 (2017), http://www.ipo.org/wp-content/uploads/2017/02/20170207_IPO-101-TF-Proposed -Amendments-and-Report.pdf [https://perma.cc/JE95-UBCW]. The American Intellectual Property Law Association (AIPLA) proposal, which was released after our workshop, parallels this proposal. *See* AIPLA, AMERICAN INTELLECTUAL PROPERTY PROPOSAL AND REPORT ON PATENT ELIGIBLE SUBJECT MATTER (2017), https://www.aipla.org/resources2/reports/2017AIPLADirect/Documents/AIPLA%20Report%20on%20101%20Reform-5-19-17-Errata.pdf [https://perma.cc/BPA7-4HQ7].

51. *See* Pasquale J. Federico, *Commentary on the New Patent Act*, 35 U.S.C.A. 1 (1954 ed.), *reprinted in* 75 J. PAT. & TRADEMARK OFF. SOC'Y 161 (1993).

52. *See* S. REP. No. 82-1979, at 5 (1952), *reprinted in* 1952 U.S.C.C.A.N. 2394, 2399 (noting that "[a] person may have 'invented' a machine or a manufacture, which may include anything under the sun that is made by man, but it is not necessarily patentable under section 101 unless the conditions of [this] title are fulfilled.") That phrase first surfaced in patentable subject matter jurisprudence in *In re Bergy*, 596 F.2d 952, 961 (C.C.P.A. 1979). It was then picked up in *Diamond v. Chakrabarty*, 447 U.S. 303, 309 (1980), and *Diamond v. Diehr*, 450 U.S. 175, 182 (1981), without its full context or ellipses. *See* Brief of Professors Peter S. Menell & Michael J. Meurer as Amici Curiae in Support of Respondent at 10–22, Bilski v. Kappos, 130 S. Ct. 3218 (2009) (No. 08-964), 2009 WL 3199629 (providing comprehensive analysis of the legislative history of the 1952 Patent Act).

53. INTELLECTUAL PROPERTY OWNERS ASS'N, *supra* note 50, at 1.

application" of an abstract idea, natural law, or physical phenomenon with a search for a "practical application" of an abstract idea, natural law, or physical phenomenon, assuming the claim falls within one of the § 101 categories.[54] The Lefstin-Menell Sequenom Amicus Cert. Petition Brief contends that this approach comports with the core principles of pre-*Mayo* jurisprudence.[55] The ABA's Section of Intellectual Property Law (ABA-IPL) submitted comments to the USPTO that are consistent with a "practical application" test.[56]

4. List of Exclusions

Another proposal would replace the existing two-step test with a list of eligibility exclusions, where subject matter would be excluded when claimed "as such." This proposal is modeled on the European Patent Convention.[57] Paragraph 2 of Article 52 of the European Patent Convention states that "(a) discoveries, scientific theories and mathematical methods; (b) aesthetic creations; (c) schemes, rules and methods for performing mental acts, playing games or doing business, and programs for computers; [and] (d) presentations of information" "shall not be regarded as inventions." Paragraph 3 notes, however, that "Paragraph 2 shall exclude the patentability of the subject-matter or activities referred to therein only to the extent to which a . . . patent application or . . . patent relates to such subject-matter or activities as such."[58]

5. Technological Arts

Drawing on the constitutional clause authorizing Congress to grant patent protection ("[t]o promote the Progress of . . . useful Arts . . ."[59]), a technological arts test would ask whether the claimed invention contributes to the technological arts, solves a technological problem, or otherwise falls within the technological arts. This test has some similarities with Article 52 of the European Patent Convention, which provides that European patents are available for inventions in all technologies susceptible of industrial application while excluding certain fundamental principles claimed as such. A group of

54. For a discussion of this approach, *see* Taylor, *supra* note 47, at 2205–07.

55. *See* Lefstin-Menell Sequenom Amicus Cert. Petition Brief, *supra* note 1, at 27–28.

56. *See* Letter from Donna P. Suchy, Section Chair, Section of Intellectual Prop. Law, Am. Bar Ass'n, to The Honorable Michelle K. Lee, Under Secretary of Commerce for Intellectual Prop. & Dir. of the USPTO (Jan. 18, 2017). The ABA submitted a formal reform proposal in May 2017. *See* Letter from Donna P. Suchy, Section Chair, Section of Intellectual Prop. Law, Am. Bar Ass'n, to The Honorable Michelle K. Lee, Under Secretary of Commerce for Intellectual Prop. & Dir. of the USPTO (Mar. 28, 2017).

57. European Patent Convention art. 52, Nov. 29, 2001, 1065 U.N.T.S. 199, http://www.epo.org/law-practice/legal-texts/html/epc/2016/e/ar52.html [https://perma.cc/TU3M-VLQ3].

58. *Id.*

59. U.S. CONST. art. I, § 8, cl. 8.

patent professionals organized by Ken Sonnenfeld, Hans Sauer, and Margaret Brivanlou (the "Banbury group") has released a statement favoring a technological arts requirement.[60] For more information, see the Banbury Statement listed in Appendix C.

6. Elimination of Eligibility in Favor of Other Statutory Doctrines

Another proposal is to eliminate the doctrine of patent eligibility as a separate patentability requirement in favor of the other existing statutory patentability requirements: utility, novelty, non-obviousness, written description, enablement, and definiteness.[61]

In conjunction with at least some versions of this proposal, some have advocated for amending existing statutory doctrines outside of the eligibility requirement to address the inability of those doctrines to deal with relevant concerns. For example, *Mayo* raised concerns that claims encompassing fundamental principles may impede further research. Yet, many have called for overruling the Federal Circuit's narrow conception of the common law experimental use exception in favor of codifying a broader experimental use exception. A broader statutory experimental exception might allow, for example, experimentation on patented technology to improve upon it. Alternatively, if the limitation of patent-eligible subject matter under § 101 is a response to the concern that § 112 insufficiently limits the patentee's reach into after-arising technologies, the enablement or written description doctrines might be revised to directly address those concerns.[62] Professor Taylor has proposed modifying the utility requirement to require that claims, rather than merely specifications, identify the relevant utility.[63] Requiring claims to identify utility would address concerns that claims are not sufficiently clear, over-broad, and inappropriately prevent the use of basic tools of science and technological development.[64]

60. Statement by Kenneth H. Sonnenfeld et al, A Proposed Path Forward for Legislatively Addressing Patent Eligibility Law, from the Conference: Patenting Genes, Natural Products and Diagnostics: Current Status and Future Prospects, (Nov. 9–11, 2016), https://www.uspto.gov/sites/default/files/documents/Updated%20Banbury%20Statement.pdf [https://perma.cc/Q2QV-PZAJ].

61. *See, e.g.*, Brief for Eli Lilly and Company, Eisai Inc., Upsher-Smith Labs., Inc., Pfizer Inc., and Etiometry, Inc. as Amici Curiae in Support of Petitioner, Sequenom, Inc. v. Ariosa Diagnostics, Inc., 136 S. Ct. 2511 (2016) (No. 15-1182), 2016 WL 1298192. For a discussion of this approach, *see* Taylor, *supra* note 47, at 2207–11.

62. *See* Rebecca S. Eisenberg, *Wisdom of the Ages or Dead-Hand Control? Patentable Subject Matter for Diagnostic Methods After In re Bilski*, 3 CASE W. RES. J.L. TECH. & INTERNET 1, 59 (2012); Mark A. Lemley et al., *Life After Bilski*, 63 STAN. L. REV. 1315, 1331 (2011).

63. *See* Taylor, *supra* note 47, at 2189.

64. *See id.*

7. *No Change*

Another proposal is not to amend the patent statute, but to instead allow the courts to continue to apply the current law to develop relevant distinctions between eligible and ineligible claims. In particular, this proposal rejects both the view that current eligibility law is unduly confusing or problematic and the view that the existing statutory doctrines adequately address the problem of poor quality patents. Two groups opposing change to the patent statute are the Internet Association and the Computer & Communications Industry Association.[65]

C. GUIDING PRINCIPLES FOR ANALYSIS OF LEGISLATIVE PROPOSALS

If the workshop participants conclude that some statutory amendment would be appropriate to address problems with the current state of eligibility law, the next question is what the best approach might be for such an amendment. It might be helpful to think about potential guiding principles for analyzing and comparing proposals.[66]

1. *Scope of Eligibility*

The scope of eligibility may be thought of in general or specific terms. That is, as a general matter, many may think that broad but not unlimited eligibility is the appropriate lens. In terms of particular technologies, like software or diagnostic technologies, however, there will no doubt be differing views. Each proposal ought to be analyzed in terms of whether it strikes the correct balance in terms of the scope of eligibility and takes future, unforeseen technologies into account.

2. *Clarity*

To the extent that patent law is meant to induce investment in research and development, as with any property-type right, the governing law and the governing legal instrument ought to be relatively clear. Thus, patent eligibility ought to provide a relatively clear demarcation between eligible and ineligible claims.

3. *Constraint on Judicial Intervention*

The Supreme Court has decided eight cases in the last forty years (and four cases in the last seven years) on the issue of patent eligibility, far more than on

65. *See generally* William G. Jenks, Comments of the Internet Association and the Computer & Communications Industry Association Regarding the USPTO Patent Subject Matter Eligibility Guidelines (Part I) (Jan. 18, 2017) (unpublished comment), https://www.uspto.gov/sites/default/files/documents/comments_jenkins_jan182017.pdf [https://perma.cc/E8E9-LPX7].

66. *See* Taylor, *supra* note 47, at 2189–97.

any other patent law doctrine. This indicates that the Supreme Court has been unable to identify a workable standard despite numerous attempts to do so. Thus, one guiding principle for a statutory amendment may be constraint on judicial intervention and, in particular, constraint on the Supreme Court's opportunity to treat patent eligibility as a common law doctrine subject to repeated interpretation as a matter of legal doctrine (rather than application).

4. Flexibility

Flexibility refers to the ability of any proposal to be applied meaningfully to new, unforeseen, and even unimagined human activity. In other words, one may ask whether a proposal may be meaningfully applied to new claimed inventions or, instead, whether it is only backward-looking.

5. Technological Zoning

Thinking more broadly along "scope of eligibility" lines, Professor Menell, among others, has long advocated a *sui generis* approach for computer software.[67] Beyond administrative considerations, there is no economic basis for uniform patent duration across vastly different technologies. Prior to the emergence of software protection, patent eligibility had not been such a divisive aspect of patent protection. Furthermore, there is relatively little evidence indicating that computer software developers need robust patent protection to thrive. For many applications, computer software receives effective protection under trade secrecy law. In addition, copyright law affords software protection against piracy. There is relatively strong empirical evidence that patent protection for computer software has caused more harm than good. Much of the controversy over patent assertion entities relates to software-related patents.

Thus, another principle for guiding patent eligibility policy would be to explore putting software-related technologies into a separate regime that is tailored to the distinctive economic needs and technological attributes of computer software. This could involve a system with a much shorter duration and tailored remedies. It could also exclude pure business methods and other non-technological fields from patent eligibility. Such compromises could defuse the apparent impasse between discovery-based and information-based industries.

67. *See* Peter S. Menell, *Tailoring Legal Protection for Computer Software*, 39 STAN. L. REV. 1329, 1371 (1986).

III. WORKSHOP PROCEEDINGS

We convened the BCLT patent eligibility workshop at the University of California at Berkeley on March 17, 2017. Substantially all of the invitees were able to attend. The participants are listed in Appendix B. In order to understand the range of views about patent eligibility law and policy, we organized the day around two principal areas: (1) the legal background and the effects of the Supreme Court's shift in patent eligibility standards; and (2) the need for and design of legislative reform.

As reflected in the workshop agenda contained in Appendix A, we devoted the morning and early afternoon to a first set of issues: (A) the statutory and jurisprudential basis for patent eligibility limits and the effects of the recent Supreme Court cases (*Mayo/Myriad/Alice*) on the lower courts' handling of patent cases; (B) the effects of the shift in patent eligibility law on research and development in the most affected industries; (C) the effects of shifting patent eligibility jurisprudence on USPTO activity and patent prosecution; and (D) the effects of the changed landscape on patent assertion activity, litigation strategy, and case management. This Part summarizes these four sessions, each of which ran for approximately 90 minutes. Part III summarizes the second major discussion area: views on the need for and design of legislative reform of patent eligibility standards.

A. LEGAL FOUNDATION

The first session was intended to assess the degree of consensus regarding the legal foundation for patentable subject matter limitations and to summarize empirical data on how district courts and the Federal Circuit have applied the Supreme Court's recent patentable subject matter rulings.

1. Patentable Subject Matter Limitations: Patent Act and Jurisprudence

Professors Lefstin and Menell opened the workshop by exploring how the Supreme Court arrived at the *Mayo* decision and scrutinizing the decision's legal basis.[68] Their presentation began by noting that in the absence of any indication that Congress intended to limit the scope of the patent system beyond the categories it enumerated in § 101, the Supreme Court has based its subject matter jurisprudence on a particular view of history—in *Bilski*'s words, "a matter of statutory *stare decisis* going back 150 years."[69] In particular, *Mayo* relied on a passage from *Neilson v. Harford*,[70] a case decided by the Court of Exchequer in 1841, which had also been central to the Supreme Court's

68. The presentation largely summarized the analysis in Lefstin-Menell Sequenom Amicus Cert. Petition Brief, *supra* note 1.

69. Bilski v. Kappos, 561 U.S. 593, 602 (2010).

70. 151 Eng. Rep. 1266 (1841).

decisions in *Le Roy v. Tatham*,[71] *O'Reilly v. Morse*,[72] and *Tilghman v. Proctor*[73] The passage quoted in *Mayo* referred to the challenge raised to Neilson's patent on the hot blast iron smelting process, and *Mayo* concluded that Neilson's patent had been sustained only because his apparatus represented an inventive and unconventional means of applying Neilson's discovery that preheating the blast dramatically increased the efficiency of the smelting process. According to *Mayo*:

> The English court concluded that the claimed process did more than simply instruct users to use the principle that hot air promotes ignition better than cold air, since it explained how the principle could be implemented in an inventive way. Baron Parke wrote (for the court):
>
> > "It is very difficult to distinguish [Neilson's claim] from the specification of a patent for a principle, and this at first created in the minds of some of the court much difficulty; but after full consideration, we think that the plaintiff does not merely claim a principle, but a machine embodying a principle, and a very valuable one. We think the case must be considered as if the principle being well known, the plaintiff had first invented a mode of applying it by a mechanical apparatus to furnaces; and his invention then consists in this—by interposing a receptacle for heated air between the blowing apparatus and the furnace. In this receptacle he directs the air to be heated by the application of heat externally to the receptacle, and thus he accomplishes the object of applying the blast, which was before of cold air, in a heated state to the furnace." *Neilson v. Harford*, Webster's Patent Cases, at 371.
>
> Thus, the claimed process included not only a law of nature but also several unconventional steps (such as inserting the receptacle, applying heat to the receptacle externally, and blowing the air into the furnace) that confined the claims to a particular, useful application of the principle.[74]

The same passage had been cited by *Parker v. Flook* in support of the notion (later rejected by *Diehr)* that discoveries should be treated as part of the prior art.[75] However, in the briefing for *Mayo*, only one brief, filed by Professor

71. 55 U.S. 156 (1853).
72. 56 U.S. 62 (1853).
73. 102 U.S. 707 (1880).
74. Mayo Collaborative Servs. v. Prometheus Labs., Inc., 566 U.S. 66, 83–84 (2012).
75. *Parker v. Flook*, 437 U.S. 584, 592 (1978).

Joshua Sarnoff on behalf of nine law professors,[76] quoted and discussed the language from *Neilson*. Professor Sarnoff's brief connected the supposed "requirement for prior art treatment of new discoveries" with a strong distinction between inventions and discoveries, the latter being ultimately creations of the divine rather than the human.[77]

Professors Lefstin and Menell pointed out the close relationship between this line of analysis and the Supreme Court's reasoning in *Mayo*. The Court's opinion quoted the referenced passage from the *Neilson* case, and grounded its inventive application requirement on the same interpretation of that case raised in *Flook* and offered in Professor Sarnoff's brief.[78]

Professors Lefstin and Menell then highlighted three critical errors with the Supreme Court's *Mayo* analysis. First, the Court provided no analysis of the statutory text, which refers repeatedly to patent protection for "inventions" *or* "discoveries." Every major patent statute since the nation's founding has afforded patent protection to technological innovations *and* scientific discoveries.[79] Thus, the dual "invention *or* discovery" thread runs through the fabric of U.S. patent law. Furthermore, the very constitutional clause empowering Congress to establish patent protection expressly refers to "Discoveries."[80]

Second, the legislative history of the patent statutes has consistently endorsed patent protection for *applied scientific discoveries*, whether or not they are *inventively* applied. The legislative history of the 1836 Patent Act, perhaps the most important patent statute in the nation's history,[81] expresses

76. *See* Sarnoff *Mayo* Amicus Brief, *supra* note 16.

77. *See id.* at 8, 10 ("[D]iscoveries were not thought to be human creations that were the proper objects of exclusive property rights.").

78. *See Mayo*, 566 U.S. at 83–84.

79. *See* Patent Act of 1790, ch. 7, 1 Stat. 109–12, § 1 (authorizing granting of patents to any person who "invented or *discovered* any useful art, manufacture, engine, machine, or device . . . if they shall deem the invention or *discovery* sufficiently useful and important . . . .") (emphasis added); Patent Act of 1793, Stat. 318, § 1 (retaining the dual eligibility structure, referring to "said invention or discovery"); *id.* at § 10 (referring to the patentee as the "inventor or discoverer"). Currently, § 100 defines "invention" to mean "invention or discovery," and § 101 authorizes one who "invents or discovers" one of the enumerated categories of subject matter to apply for a patent. *See* 35 U.S.C. §§ 100(b), 101 (2013).

80. *See* U.S. CONST. art. I, § 8, cl. 8 (authorizing Congress "To promote the Progress of Science and useful Arts, by securing for limited Times to Authors and Inventors the exclusive Right to their respective Writings and *Discoveries*" (emphasis added)).

81. The 1836 Patent Act established the Patent Office. From 1790 to 1793, Congress authorized any two of the "Patent Board," comprised of the Secretary of State, the Secretary for the Department of War, and the Attorney General to grant patents. That system proved unworkable, and the 1793 Act shifted to a patent registration system with validity decisions left to courts enforcing patents. The lack of an examination system led to the proliferation of "unrestrained and promiscuous grants of patent privileges," JOHN RUGGLES, SELECT

Congress's fervent hope that patent protection would encourage *scientific discovery*:

> Whoever imagines that, because so many inventions and so many improvements in machinery have been made, there remains little else to be discovered, has but a feeble conception of the infinitude and vastness of mechanical powers, or of the unlimited reach of science. Much as has been discovered, infinitely more remains unrevealed. The ingenuity of man is exploring a region without limits, and delving in a mine whose treasures are exhaustless. "Neither are all the mysteries of nature unfolded, nor the mind tired in the pursuit of them."
>
> The first conceptions of ingenuity, like the first suggestions of science, are theories which require something of experiment and practical exemplification to perfect.[82]

The timing of this pronouncement coincides with the *Neilson v. Harford* (1841), *LeRoy v. Tatham* (1853), and *O'Reilly v. Morse* (1854) era, indicating that jurists from this critical formative era would have seen applications of scientific discoveries to be comfortably within the scope of patentable subject matter.

Professors Lefstin and Menell showed that the dual eligibility framing—inventions or discoveries—continued through to the present statute.[83] In particular, the legislative history of the 1930 Plant Patent Act explicitly stated Congress's view that the patent statutes embrace the act of discovery. In that Act, Congress sought to provide patents for the work of the plant breeder, who might do nothing more than discover a naturally occurring bud mutant on a cultivated plant, and then propagate that mutant by conventional techniques. The proposed scheme raised questions whether the patent system could embrace discoveries with such minimal human intervention in their application. Congress was emphatic that the patent laws could, and in fact did,

---

COMMITTEE REPORT ON THE STATE AND CONDITION OF THE PATENT OFFICE, S. DOC. NO. 24-338, at 4 (1836), eroding faith in the patent system and ultimately leading to the Act of 1836 which instituted examination in a newly constituted Patent Office. *See* S. REP. ACCOMPANYING S. BILL NO. 239, 24th Cong. (Apr. 28, 1836).

82. S. REP. ACCOMPANYING S. BILL NO. 239, 24th Cong. (Apr. 28, 1836).

83. *See* Patent Act of 1870, ch. 230, 16 Stat. 198 (Jul. 8, 1870) (referring to "invention or discovery" and "inventor or discoverer" throughout the statute. *See* REVISED STATUTES OF THE UNITED STATES, 946–53 (2d ed. 1878) (reproducing Rev. Stat. §§ 4884, 4886, 4887, 4888, 4890, 4891, 4892, 4893, 4895, 4896, 4897, 4899, 4902, 4908, 4916, 4917, 4920, 4922, 4923, 4924, 4926, 4927)); Plant Patent Act of 1930, 46 Stat. 703 (amending Rev. Stat. § 4886); Patent Act of 1952 § 100(a) (restates the traditional definition of "invention" as "invention or discovery"), § 100(b) (defining "process" to include "a new use of a known process, machine, manufacture, composition of matter, or material"), § 101 ("Whoever invents or discovers . . . .").

extend to such discoveries:

> Present patent laws apply to "any person who has invented or discovered any new and useful art, machine, manufacture, or composition of matter, or any new and useful improvement thereof . . . ." *It will be noted that the laws apply both to the acts of inventing and discovery* and this alternative application has been true of the patent laws from their beginning. See, for instance, the Patent Act of 1790 (1 Stat. 109).[84]

Notably, Congress implemented patents for plants by adding them as a new category of inventions or discoveries protectable under the basic patentability statute, R.S. § 4886, indicating that Congress saw no distinction between plant and utility patents in the nature of the inventive act. Congress specifically rejected a proposal by the Patent Office that would have had the statute distinguish between the quantum of invention or discovery required for plant patents versus utility patents.[85]

Third, Professor Lefstin explained that neither the Court of Exchequer in *Neilson*, nor the U.S. Supreme Court in *O'Reilly*, had required *inventive* application of scientific discoveries.[86] The statement emphasized in the Sarnoff brief and quoted in the *Flook* and *Mayo* decisions—"[w]e think the case must be considered as if the principle [of preheating air prior to injection into a hot-blast smelter] being well known"—was a declaration that Neilson's patent claimed a machine rather than an abstract scientific principle. While American precedent of the era (such as *O'Reilly*) understood the Exchequer's holding clearly, *Flook* and *Mayo* took that passage out of its proper context and misinterpreted it drastically.

Professor Lefstin explained that Neilson's specification had disclosed next to nothing about his heating apparatus, yet claimed that his patent covered every hot-blast smelter no matter what means of heating were employed. Beyond a challenge on enablement grounds, Neilson's refusal to be limited to a particular heating apparatus laid his patent open to the challenge that he had claimed an abstract scientific principle, rather than a patentable machine.[87]

The Exchequer recognized that the defendant's challenge was exactly the same raised by the defendant in a case it had decided seven years earlier, *Minter*

84. H.R. REP. NO. 71-1129, at 7 (1930); S. REP. NO. 71-315, at 6 (1930) (quoting Rev. Stat. § 4886) (emphasis added).

85. *See A Bill to Provide for Plant Patents: Hearing on H.R. 11372 Before the H. Comm. on Patents*, 71st Cong. 7 (1930). The Office's proposal would have had the statute define "invented" and "discovered" specifically for plant patents. That rejected language stated: "finding a thing already existing and reproducing the same as well as in the sense of creating."

86. *See generally* Lefstin, *supra* note 16 (explicating the history of the *Neilson* litigation).

87. Processes were not recognized as patentable at the time.

v. Wells[88]—except that Neilson's case involved a newly discovered principle, rather than one well-known.

Minter's patent had claimed a reclining chair embodying the principle of self-adjusting leverage.[89] Like Neilson, Minter had declared that his claim was not limited to any precise shape or form of chair. The defendants therefore attacked the patent on the ground that Minter had merely claimed a well-known principle of mechanics in the abstract.[90] The Exchequer rejected the challenge, holding that Minter's claim was not to the well-known principle, but to the application of that principle in the construction of a chair.[91] Thus, Minter's claim was not to a well-known principle, but rather it applied a well-known principle to a chair to produce a patent-eligible *machine*. The critical passage in *Neilson* refers to this doctrine—relating to what constitutes a *machine*. *Neilson* holds that the same doctrine governing applications of well-known principles should govern applications of newly discovered principles. It does not declare that scientific discoveries are to be treated as well-known or prior art for purposes of patent eligibility.[92]

Reinforcing this point, the English courts have never interpreted *Neilson v. Harford* to require inventive application of scientific discoveries.[93] Conventional application of newly discovered scientific principles is all that English law has ever required.[94]

The *Mayo* decision compounded its misinterpretation of early English law to require *inventive* application of newly discovered laws of nature by asserting that Neilson had inventively applied the pre-heating principle. The *Mayo* opinion states that "the claimed process included not only a law of nature but also several unconventional steps (such as inserting the receptacle, applying heat to the receptacle externally, and blowing the air into the furnace) that

88. 149 Eng. Rep. 1180 (Ex. 1834), http://www.commonlii.org/uk/cases/EngR/1834/222.pdf [https://perma.cc/7WCV-RMNB], *reprinted in* 1 CARPMAEL'S PATENT CASES 622 (1834).

89. *Id.* at 622.

90. *Id.* at 644.

91. *Id.* at 646.

92. This conclusion is also apparent from the sentence preceding the passage on which the Supreme Court derives the inventive application doctrine. That sentence reads: "[A]fter full consideration, we think that the plaintiff does not merely claim a principle, but a machine embodying a principle, and a very valuable one." *Neilson v. Harford*, 151 Eng. Rep. 1266, 1273 (Ex. 1841), http://www.commonlii.org/uk/cases/EngR/1841/887.pdf [https://perma.cc/7RNA-UZ85], *reprinted in* 1 WEBSTER'S PATENT CASES 295, 371 (1844). The Exchequer was assessing whether a broad claim to all manner of pre-heating air, like the broad claim in *Minter v. Wells* to a wide range of chair shapes, was to an abstract principle or a machine.

93. *See* Lefstin, *supra* note 16, at 591–93.

94. *See* Genentech, Inc.'s Patent, (1989) RPC 147, 213–17; Kirin-Amgen Inc. v. Hoechst Marion Roussel Ltd., (2004) UKHL 46.

confined the claims to a particular, useful application of the principle."[95] But Neilson's patent was sustained precisely because he employed well-understood, routine, and conventional means in the application of a new scientific discovery.[96] In rejecting the defendant's argument that Neilson had not disclosed enough about the heating means to enable practice of the invention, the Exchequer relied on the fact that Neilson's means of preheating were routine and well-known in the art. As Baron Parke's opinion acknowledged and accepted, the patentee argued that:

> [t]he mode of heating air was perfectly well known; it was no discovery of Mr. Neilson's, everybody knew it. Air had been heated, and there had been different shaped vessels employed for heating the air; for heating the air economically, and for heating it to a higher or lesser degree of temperature; all that was perfectly well known.[97]

Given the lack of historical foundation for an inventive application requirement, Professors Lefstin and Menell noted that it was particularly surprising that the Supreme Court, which has increasingly emphasized textualist modes of interpretation, would overlook the unbroken chain of references to patent protection extending to both "inventions" and "discoveries." Moreover, by intermingling nonobviousness (§ 103) and enablement or written description (§ 112) considerations into the subject matter inquiry, the *Mayo/Alice* decisions short-circuited the factual inquiries and structure mandated by the 1952 Act. Professors Lefstin and Menell surmised that the Court's failure to engage these critical issues likely resulted from a lack of adequate briefing. The questions presented did not signal to the litigants or amicus community that the Court might venture into such a radical reconsideration of patentable subject matter limitations.

Professors Lefstin and Menell concluded their review of the *Mayo/Myriad/Alice* decisions by highlighting the decisions' impacts on several

---

95. Mayo Collaborative Servs. v. Prometheus Labs., Inc., 566 U.S. 66, 84 (2012).

96. As the Supreme Court recognized in *O'Reilly v. Morse*, Neilson's patent had been attacked for inadequate disclosure, what modern practitioners refer to as enablement, as well as for subject matter grounds. *See O'Reilly v. Morse*, 56 U.S. 62, 115 (1853). ("[T]he defendant among other defences [sic] insisted—that the machinery for heating the air and throwing it hot into the furnace *was not sufficiently described* in the specification, and the patent void on that account—and also, that a patent for throwing hot air into the furnace, instead of cold, and thereby increasing the intensity of the heat, was a patent for a principle, and that a principle was not patentable.") (emphasis added).

97. *Neilson*, 1 WEBSTER'S PATENT CASES at 344. That the Exchequer acknowledged and accepted this fact is shown by the judges' repetition of this point. *See id.* at 337 (Alderson, B.) (stating that Neilson's heating means were "perfectly well known"). *Neilson* even became the authority for the proposition that practical applications of discoveries were patentable without any invention in the means of application. *See* Lefstin, *supra* note 16, at 592, 606–08.

key technology industries. For the bioscience industries, the *Mayo/Myriad* decisions exclude from patent protection path-breaking discoveries unless they are inventively applied. This in effect requires scientists working in diagnostics and other discovery-based fields to make two breakthroughs in order to obtain patent protection: (1) they must "discover" a law of nature or natural phenomenon; and (2) they must "inventively" apply that discovery. Conventional application of even a Nobel Prize-worthy discovery no longer suffices to obtain a patent. The rule is nominally clear, but excludes subject matter that has been patentable since the creation of the patent system: conventional applications of scientific discoveries.

By contrast, for the software industries there is tremendous uncertainty regarding what constitutes an inventive application of abstract ideas and algorithms. While pure business methods that do not improve the functioning of a computer are no longer patent-eligible, there remains substantial subjectivity surrounding the patent eligibility of computer-implemented processes in general.

2. § 101 Invalidity Rates—Courts

Robert Sachs presented data on changes in § 101 invalidity rates in the courts.[98] In the decade preceding the *Mayo* decision (in March 2012), there were only a handful of district court decisions that found patents invalid under § 101.[99] Table 1, however, summarizes a significant increase in district court

98. The data was current as of February 28, 2017.

99. *See* Climax Molybdenum Co. v. Molychem, LLC, No. 02-cv-00311, 2007 WL 3256698 (D. Colo. Nov. 1, 2007); Perfect Web Techs., Inc. v. Infousa, Inc., 89 U.S.P.Q.2d 2001 (S.D. Fla. 2008), *aff'd on other ground*, 587 F.3d 1324 (Fed. Cir. 2009); CyberSource Corp. v. Retail Decisions, Inc., 620 F. Supp. 2d 1068 (N.D. Cal. 2009), *aff'd*, 654 F.3d 1366 (Fed. Cir. 2011); DealerTrack, Inc. v. Huber, 657 F. Supp. 2d 1152 (C.D. Cal. 2009), *aff'd in part, vacated in part, rev'd in part*, 674 F.3d 1315 (Fed. Cir. 2012); Fort Props., Inc. v. Am. Master Lease LLC, 609 F. Supp. 2d 1052 (C.D. Cal. 2009), *aff'd*, 671 F.3d 1317 (Fed. Cir. 2012); Bancorp Servs., L.L.C. v. Sun Life Assurance Co. of Can., 771 F. Supp. 2d 1054 (E.D. Mo. 2011), *aff'd*, 687 F.3d 1266 (Fed. Cir. 2012); Glory Licensing LLC v. Toys "R" Us, Inc., 2011 WL 1870591 (D.N.J. May 16, 2011); VS Techs., LLC v. Twitter, Inc., 2012 WL 1481508 (E.D. Va. Apr. 27, 2012); CLS Bank Int'l v. Alice Corp. Pty. Ltd., 768 F. Supp. 2d 221 (D.D.C. 2011), *aff'd*, 717 F.3d 1269 (Fed. Cir. 2013) (en banc), *aff'd* 134 S. Ct. 2347 (2014); Ass'n for Molecular Pathology v. USPTO, 702 F. Supp. 2d 181 (S.D.N.Y. 2010), *aff'd in part, rev'd in part*, 689 F.3d 1303 (Fed. Cir. 2012), *aff'd in part, rev'd in part*, Ass'n for Molecular Pathology v. Myriad Genetics, Inc., 569 U.S. 576 (2013); King Pharms., Inc. v. Eon Labs, Inc., 593 F. Supp. 2d 501 (E.D.N.Y. 2009) (ruling four claims ineligible), *aff'd on other grounds, vacated in part*, 616 F.3d 1267 (Fed. Cir. 2010) (reversing § 101 invalidity determination). In addition, the Federal Circuit struggled with several patentable subject matter disputes appealed from USPTO § 101 rejections. The Federal Circuit also upheld a few PTO patent rejections on eligibility grounds. *See In re* Comiskey, 554 F.3d 967 (Fed. Cir. 2009); *In re* Bilski, 545 F.3d 943 (Fed. Cir. 2008), *aff'd on different reasoning*, Bilski v. Kappos, 561 U.S. 593 (2010); *In re* Nuijten, 500 F.3d 1346 (Fed. Cir. 2007).

§ 101 invalidity decisions both in the 32 months preceding the Supreme Court's *Alice* decision (in June 2014) and in the 32 months following.

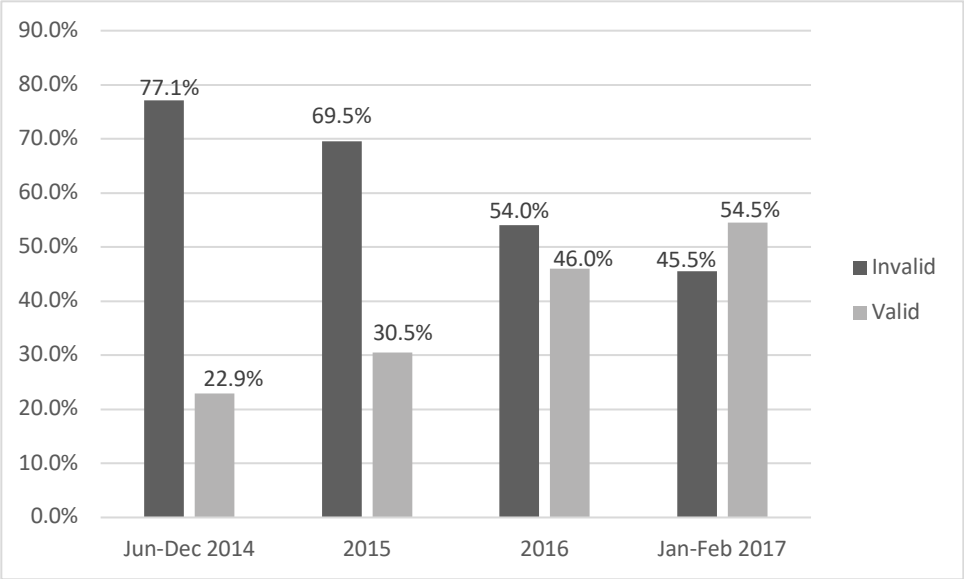
Table 1.
All District Court Decisions on § 101 Related Motions

	After *Mayo* but Before *Alice* (24 months, June 2012 to June 2014)				After *Alice* (32 months, June 2014 to February 2017)				
	Invalid	Not invalid	*Total*	Percent Invalid	*Invalid*	Not invalid	*Total*	Percent Invalid	% Change Post-Alice
Decisions	16	21	37	**43.2%**	222	137	359	**61.8%**	**+19%**
Patents	26	55	81	**32.1%**	324	454	778	**41.6%**	**+10%**

We see a dramatic rise in the number of district court § 101 invalidity decisions following the *Mayo* decision, with no more than three in any year prior to 2012 to an average of 8 per year in the two years following the *Mayo* decision. That number increases 10-fold after the *Alice* decision.

Furthermore, the rate at which patents were found invalid increased significantly as well. Figure 1 shows the district court outcomes on § 101 invalidity determinations over time.

Fig. 1
Section 101 Outcomes in District Courts



The number of decisions rose sharply from 35 in the second half of 2014 to 141 in 2015, and to 161 in 2016. As shown, the percentage of invalidity determinations fell from a high of 77.1% in 2014 to less than 50% for the first two months of 2017.

Table 2 shows the § 101 invalidity decisions by court and litigation stage.

Table 2
Section 101 Decisions by Court and Litigation Stage
June 2014 to February 2017

Tribunal	§ 101 Invalidity Decisions	**% Invalid**	Total § 101 Decisions
District Court	**222**	**62%**	**359**
Motion for attorney fees	1	100%	1
Motion for Judgment on the Pleadings (JOP)	63	68%	92
Motion to Dismiss (MTD)	94	60%	157
Motion for Summary Judgment (MSJ)	62	64%	97
Post-Trial Motion (PTM)	2	17%	12
Federal Circuit	**70**	**91%**	**77**
Appeal-PTAB-Covered Business Method Review (CBM)	7	100%	7
Appeal-JOP	14	88%	16
Appeal-MSJ	24	92%	26
Appeal-MTD	20	95%	21
Appeal-Prelim Inj. (PI)	1	100%	1
Appeal-PTAB	4	100%	4
Appeal-PTM	0	0%	2
Grand Total	292	67%	436

District courts have resolved the majority of § 101 controversies early in case management—on the pleadings, motion to dismiss, and summary judgment stages. The Federal Circuit has affirmed a high percentage of invalidity determinations.

Table 3 summarizes the Federal Circuit's review of § 101 invalidity decisions.

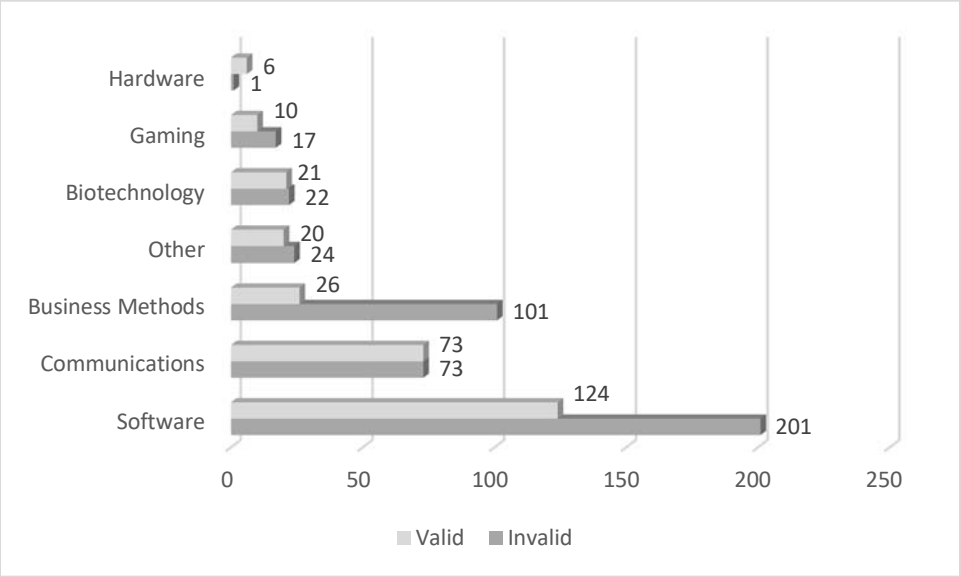
Table 3
Federal Circuit Review of § 101 Determinations
June 2014 to February 2017

	Invalid			**Not Invalid**		**Total**
	Affirmed	Affirmed *Per Curiam*	Reversed	Affirmed	Reversed	
Appeal-CBM	2	1	-	-	-	**3**
Appeal-JOP	2	12	-	-	2	**16**
Appeal-MSJ	10	13	1	-	2	**26**
Appeal-MTD	10	10	-	-	1	**21**
Appeal-PI	1	-	-	-	-	**1**
Appeal-PTAB	1	7	-	-	-	**8**
Appeal-PTM	-	-	-	2	-	**2**
Total	**26**	**43**	**1**	**2**	**5**	**77**

The Federal Circuit has affirmed substantially all district court invalidity determinations. Nearly two-thirds of affirmances have been with opinion. By contrast, the Federal Circuit reversed five of the seven district court findings of no invalidity.

Figure 2 shows the distribution of invalidated patents across technology fields.

Fig. 2
Patents Challenged under § 101 by Technology Field
June 2014 to February 2017



3. Discussion

None of the workshop participants questioned the core points in the legal presentation. One scholar noted that Professor Sean O'Connor's research suggests that the term "discoveries" in the U.S. Constitution reflected a heightened level of inventiveness.[100] While acknowledging Professor O'Connor's research, Professor Menell noted that the 1790 Patent Act and all subsequent Patent Acts refer to the patentability of "inventions or discoveries." Professor Lefstin noted that the legislative history of the Plant Patent Act of 1930 and the 1952 Act make clear that Congress has supported broad coverage of both inventions and discoveries, bearing in mind that patentable "discoveries" have always been practical applications embodied in one of the statutory classes of subject matter, not discoveries in the abstract. And there was broad consensus among the participants that the basis for the

100. *See* Sean M. O'Connor, *The Overlooked French Influence on the Intellectual Property Clause*, 82 U. CHI. L. REV. 733, 739 (2015) (suggesting that the French *Encyclopédie* defines "discoveries" as "the most important inventions, rather than the uncovering of existing facts").

Supreme Court's "inventive application" requirement was flawed and that patent law had long afforded protection for applied discoveries.

One participant commented on the undesirable effects of the Supreme Court's recent patentable subject matter jurisprudence on district judges. That participant noted that docket pressures already motivate judges to reduce their trial burdens and that the Supreme Court's "inventive application" jurisprudence, which can be wielded at early stages of litigation, invites cursory analysis of patentable subject matter. Based on the clear text of the Patent Act and jurisprudence, that participant expressed the view that § 101 should be liberally and broadly construed, and that §§ 103 and 112 provide the appropriate tools for curtailing dubious and overbroad patents.

The discussion turned to participants' views about what was driving the Supreme Court's renewed interest in and approach to patentable subject matter limitations. Several participants viewed the Supreme Court's recent foray into patent eligibility as a misdirected effort to address other problems in the patent system, notably broad, vague, and inadequately-supported claims. Others noted perceptions that the non-obviousness standard remains uncertain and too low with regard to software-related patents. The proliferation of "low quality" patents in conjunction with the emergence of patent assertion entities has raised the salience of the patent system, and perhaps the Supreme Court saw § 101 as a tool for reining in these problems.

One participant focused on jurisprudential philosophy, noting that the Supreme Court views patentable subject matter limitations as a common law enterprise.

Other participants emphasized broader moral concerns that might animate the Court's jurisprudence, such as public perceptions about bioscience companies claiming "ownership" of people's genetic information. One participant noted that the Court's patentable subject matter cases may reflect discomfort with intellectual property protection for fundamental tools or knowledge building blocks, such as laws of nature and mental steps. Others noted the intuition that patents are for technology, not business strategies. The Court's recent focus on diagnostics, software, and business methods reflects these considerations.

B. EFFECTS ON RESEARCH AND DEVELOPMENT

The second session focused on the effects of the shift in patentable subject matter eligibility on research and development activity. One scholar opened the session by framing key questions. An industry practitioner then discussed the relationship between patent protection for diagnostics and advances in personalized medicine. We then opened the discussion and concluded with perspectives from software industry representatives.

1. Framing

The patent system aims to promote innovation by providing time-limited exclusive rights in exchange for disclosure of useful inventions and discoveries. Without patents, we would expect many inventors to rely on trade secrets to appropriate return on their research and development investments.

The efficacy of the patent system is often difficult to measure. Some innovation occurs without the need for exclusive rights and some inventors are able to gain patent protection without providing critical information. Due to the risks of being liable for willful infringement, engineers and scientists in some fields, such as software, steer clear of reading patents. Patents in other fields, such as pharmaceuticals, provide critical security needed for the large capital expenditures and risk of research and development.

The shift in patentable subject matter eligibility suggests several questions for understanding the effects on research and development activities:

a) Are research institutions and companies shifting their research agendas?

b) Are research institutions and companies relying more significantly on trade secrecy and reducing public disclosure of scientific discoveries, technological inventions, and technical knowledge?

c) Is there greater opportunity for follow-on innovators without patents on fundamental building blocks?

2. Diagnostics, Personalized Medicine, and Biosciences

An industry practitioner then discussed the relationship between patent protection for diagnostics and personalized (or precision) medicine. According to this representative, precision medicine uses a patient's individual clinical characteristics to tailor medical intervention. Examples include detecting the patient's genotype with increased drug response, measuring drug metabolites in the patient's blood, and observing the patient's clinical response to a drug as means of modifying and optimizing drug dosage.

Molecular diagnostics play a central role in driving precision medicine research and development. It provides the clues for determining disease predisposition, diagnosing disease, assessing disease prognosis, predicting drug response, and targeting prescriptions and diagnostics. Precision medicine depends critically upon balanced regulation, robust reimbursement, and intellectual property rights.

The representative asserted that while few scholars question the need for strong patents in drug research, there is less understanding of the role of patents in medical diagnostics. Such research is more akin to conventional drug development than software or electronics in terms of its investment patterns

and research life cycles.

Notwithstanding that there have been no significant substantive changes to patent eligibility and validity standards in the patent statute, patent protection for diagnostics has significantly eroded over the past decade due to judicial decisions. While these shifts have had negative impacts on all of life science research and development, they have been particularly severe for the diagnostics sector. Reagents and many processes are seen as ineligible for patent protection. Diagnostic kits can also be more difficult to patent under the murky standards relating to "abstract ideas."

Furthermore, trade secret protection for diagnostics research can be difficult to maintain. Diagnostics companies must publish most details of their tests in peer-reviewed journals to be eligible for reimbursement. Other forms of intellectual property—trademark protection for branding and copyright for instructions—do not provide effective protection to support appropriability, i.e., the ability to derive a return on research and development investment, for diagnostics research.

Ultimately, research and development incentives for medical diagnostics depends critically on the balance among regulation, reimbursement, and patent rights. There is currently no regulatory framework balancing innovator and follow-on generic entrants as there is in the prescription drug sector (Hatch-Waxman legislation). A robust regulatory framework, such as FDA regulation of laboratory-developed diagnostic tests, would increase quality and safety of medical diagnostics but would add to the validation and investment burdens on diagnostics companies to bring their tests to market. Furthermore, the reimbursement rules governing diagnostics play a critical and uncertain role for evaluating diagnostics investments. Patent protection can be an important factor in negotiating reimbursement with health care payers. The shift in patent eligibility for diagnostics threatens research and development investment in medical diagnostics.

Other participants elaborated on the adverse effects of the *Mayo* and *Myriad* decisions on the bioscience industries more generally. One participant noted that venture capitalists and other investors pay significant attention to whether the fruits of research and development expenditures can be internalized by their creators. Ultimately, most investors are indifferent between investing in bioscience, software, or commodities—whichever offers the higher return will attract more capital. The difficulty of protecting advances in scientific discoveries has, in that person's view, tilted investment away from areas that are more difficult to protect and toward research where trade secrets are more viable.

Participants also discussed how the loss of patent protection for isolated and purified natural products further limits the range of bioscience advances

where investors cannot expect rewards from their investments. An attorney with a strong bioscience background provided several concrete examples of important scientific research that was experiencing funding difficulties as a result of the shift in patent eligibility standards: cytotoxins derived from sea organisms (purified natural products) that could be used in treating tissue sarcoma; genes relating to particular genetic mutations; and snake toxins used for treating multiple sclerosis. That participant also noted that bio-analytical data, which can in theory be protected by trade secrecy, is often very difficult to commercialize without disclosure.

One participant drew attention to the Supreme Court's definition of "law of nature" in *Mayo* as a cause of the incoherence across multiple technological fields. That participant noted that the relationship between biomarkers and diseases may be naturally occurring, but they are not "laws of nature." It would be better, in that participant's view, to characterize such relationships as contingent outcomes of evolution. From that perspective, they are no different in kind from other natural relationships that are discovered in chemistry, metallurgy, and semiconductors and could be extrapolated to software and information technologies.

3. Software and Information Technologies

Attorneys working in the software field provided a more mixed view of the shift in patent eligibility jurisprudence. While not defending the Supreme Court's recent decisions on interpretive or jurisprudential grounds, several in-house counsels in the information technology sector noted that the *Alice* decision has not materially affected their companies' research and development levels, project choice, or start-up acquisition decisions. One participant noted that some boards of directors pay attention to whether potential acquisition targets have patents, but such patents are not typically determinative in the acquisition decision.

While recognizing that software technology should be patentable, several technology industry participants commended the *Alice* decision for weeding out numerous bad patents, reducing litigation risks and costs, and providing a means for resolving litigation over weak patents earlier in the process.

One participant noted that software patents continue to be filed, although patents for analytics are more difficult to pursue. Some of these technologies, however, can be protected by trade secrecy, especially as more and more of the software industry shifts to cloud-computing, software as a service, and enterprise computing business models. This participant noted that algorithmic technologies are being replaced by neural networks and machine learning, which are also vulnerable under *Alice*, but can be protected by trade secrets. Another participant noted that software development is more collaborative and open today. Many platforms rely on open source software, with

competition occurring through implementations and cloud-based services.

An attorney working at a company that has a large research division commented that distinctions across scientific and technological fields are often artificial. Many of the most important breakthroughs happen when researchers cross-germinate methods and findings to open up fertile new research fields. This is increasingly happening in the digital age in fields such as analytics, diagnostics, drug development, bioinformatics, and medical imaging. Although it is sometimes difficult to link patents to products, patents nonetheless are critical to the investment process. This participant noted that concerns about basic building blocks being monopolized and royalty stacking can be exaggerated. Research companies license and cross-license technological advances. Patents often promote openness and sharing, whereas trade secrecy can stand in the way. A bigger impediment to research and development is the commodification of technology, which reduces profit margins. Many research enterprises are looking for areas where breakthroughs can produce significant returns on investment.

C. EFFECTS ON PATENT PROSECUTION

The third session explored the effects of the Supreme Court's recent patentable subject matter decisions on patent prosecution. A representative from the USPTO began by highlighting the agency's difficulty handling the changes to the law of patent eligibility. We then heard a presentation by Robert Sachs on patent prosecution invalidity rates at the USPTO. Participants then engaged in a general discussion about patent prosecution relating to patent eligibility, followed by more particular discussion of § 101 prosecution in the life sciences and information technology sectors.

1. The USPTO's Experience

The session began with remarks from Robert Bahr, the USPTO's Deputy Commissioner for Patent Examination Policy, who described the USPTO's efforts to keep up with the rapidly evolving patentable subject matter jurisprudence. He noted that patentable subject matter emerged as a major area of uncertainty in 2009 surrounding the *Bilski* patent. He then summarized the workload challenges and the efforts to update guidance documents.

Since the Supreme Court decided *Bilski* in 2010, the USPTO has struggled to provide guidance to its patent examiners regarding the law governing eligibility. The Supreme Court did not articulate any eligibility test in *Bilski*, and the Court limited its decision to the particular facts of that case.

When the Supreme Court later introduced the "inventive concept" test in *Mayo*, it was not immediately clear if this test applied beyond claims related to laws of nature. Moreover, *Myriad* seemed to indicate that a more traditional eligibility test—one asking whether a claim described something different than

what exists in nature—applied even after *Mayo*. In *Alice*, the Court finally made clear that the "inventive concept" test applied broadly to all of the judicial exceptions (laws of nature, natural phenomena, and abstract ideas), but the Court did not clarify whether the more traditional eligibility test applied in *Myriad* has any continuing applicability. As a result, *Alice* represented a significant shift in the framework to be applied by patent examiners, but still did not clearly eliminate other approaches to the question of eligibility. Moreover, the "inventive concept" test itself does not provide significant direction to resolve eligibility disputes.

In the face of these Supreme Court decisions—all along the way and even after *Alice*—the USPTO has issued a series of guidance documents for examiners. The preparation of these guidance documents has been increasingly challenging given both the changes in the governing law and the lack of clarity associated with application of the "inventive concept" test. Indeed, despite the issuance of numerous guidance documents examiners have expressed concerns with how they should apply the Supreme Court's "inventive concept" test. The guidance documents provide the examiners with a framework for determining eligibility. The documents, for example, include flow charts to guide the examiners in terms of the process. But the documents do not provide answers in terms of how the test applies in particular cases. They emphasize particular examples based on judicial opinions.

2. § 101 Invalidity Rates—Prosecution

Robert Sachs presented data on § 101 invalidity rates at the USPTO.[101] Table 4 presents the percentage of patents that the USPTO has rejected under § 101 in the period preceding the *Alice* decision and intervals following other developments: following the issuance of the 2014 Preliminary Guidance Document; [102] following the issuance of the 2014 Interim Guidance Document;[103] following the issuance of the July 2015 Guidance Update;[104] following the Federal Circuit's *Enfish* decision (overturning a district court

101. The data was current as of February 28, 2017.

102. *See* Memorandum from Andrew H. Hirshfeld, Deputy Comm'r for Patent Examination Policy, USPTO, on Preliminary Examination Instructions for Determining Subject Matter Eligibility in view of *Alice Corp. v. CLS Bank, et al.* (June 25, 2014), https://www.uspto.gov/sites/default/files/patents/announce/alice_pec_25jun2014.pdf [https://perma.cc/3KBG-9L6D].

103. *See* 2014 Interim Guidance on Patent Subject Matter Eligibility, 79 Fed. Reg. 74618 (Dec. 16, 2014) (to be codified at 37 C.F.R. pt. 1), https://www.uspto.gov/sites/default/files/documents/training%20-%202014%20interim%20guidance.pdf [https://perma.cc/W4PP-WVV6].

104. *See* USPTO, JULY 2015 UPDATE: SUBJECT MATTER ELIGIBILITY 1 https://www.uspto.gov/sites/default/files/documents/ieg-july-2015-update.pdf [https://perma.cc/CYS7-ZZ6P].

§ 101 invalidation decision);[105] and following the Federal Circuit's 2016 *McRO* decision (overturning a district court § 101 invalidation decision).[106]

105. *See* Memorandum from Robert W. Bahr, Deputy Comm'r for Patent Examination Policy, USPTO, on Recent Subject Matter Eligibility Decisions (*Enfish, LLC v. Microsoft Corp.* and *TLI Commc'ns. LLC v. A.V. Automotive*, LLC) 2 (May 19, 2016), https://www.uspto.gov/sites/default/files/documents/ieg-may-2016_enfish_memo.pdf [https://perma.cc/C8LM-KBCN].

106. *See* Memorandum from Robert W. Bahr, Deputy Comm'r for Patent Examination Policy, USPTO, on Recent Subject Matter Eligibility Decisions (Nov. 2, 2016), https://www.uspto.gov/sites/default/files/documents/McRo-Bascom-Memo.pdf [https://perma.cc/C8LM-KBCN].

Table 4
USPTO § 101 Invalidation Rates by Technology Center
June 2012 to February 2017

Tech Center	Tech Subtype	Before *Alice* (%)	Prelim Guidance 2014 (%)	Interim Guidance 2014 (%)	July 2015 Update (%)	*Enfish* May 2016 (%)	*McRO* Nov. 2016 (%)
1600	*Agriculture*	24.0	24.2	24.5	21.6	22.1	21.2
	Biotech	16.9	22.2	21.6	18.4	16.0	15.5
	Healthcare	3.2	4.6	4.7	3.1	2.8	3.3
1700	*Chemistry*	2.0	2.1	2.1	4.5	1.1	1.1
2100	*Computers*	21.5	22.0	20.9	17.3	15.7	17.3
2400	*Communications*	13.2	13.3	17.3	21.8	17.3	16.4
	Computers	19.7	19.4	23.6	25.5	19.7	21.0
2600	*Communications*	12.4	12.5	14.8	14.2	13.9	12.5
	Computers	10.2	9.9	10.3	9.5	9.1	8.1
2800	*Electrical Systems*	3.1	4.3	4.8	4.3	5.1	5.3
3600	*Civil Engineering*	3.0	4.1	4.2	3.9	3.1	3.2
	Manufacturing	1.8	1.9	2.0	1.9	1.7	1.5
	Transportation	12.4	15.6	13.4	13.9	14.3	13.8
3600 Business Methods	*Ecommerce*	43.3	83.0	92.5	90.7	92.1	90.9
3700	*Civil Engineering*	2.5	3.8	4.4	3.0	2.7	2.4
	Gaming & Education	19.7	39.8	50.0	43.3	38.1	35.6
	Healthcare	6.2	8.6	10.7	10.0	9.2	9.5
	Manufacturing	1.3	1.5	1.3	0.7	0.5	0.4

The most dramatic effects have been in business methods and gaming/education, although the § 101 invalidity rates in biotechnology and agriculture have also been high.

3. General Discussion

Even with the USPTO's various guidance documents, several participants noted that the Supreme Court's eligibility test is difficult to apply consistently, and there is great variance from examiner to examiner in how the test applies. One characterization of the effect on patent prosecution is the view that patent examiners and administrative patent judges in many instances could easily write official actions or opinions related to the same claims coming out either way—either finding eligibility or finding no eligibility. Examiners are sensitive to signals from management, so whether there is a signal to lean against issuance or lean toward issuance makes a difference in how examiners decide close cases. The impact of this sensitivity to management's signals has particular impact on patent eligibility given the subjectivity of the "inventive concept" test. One participant noted that some patent examiners appear to have a new attitude that they simply will not find eligibility, at least "not on [their] watch." In terms of the Patent Trial and Appeal Board, likewise, one participant expressed the view that if a patent applicant or owner takes a patent eligibility case to that tribunal, it is "not likely to end well." And while the Federal Circuit in the past served as a "savior" in terms of reversing the USPTO in appropriate circumstances, it has recently been less inclined to rescue deserving claims.

One participant noted that examiners were more likely to uphold claims if they analyzed validity under §§ 102, 103, and 112 prior to analyzing eligibility under § 101. Thus, the confusing nature of the "inventive concept" test might be undermining careful analysis and understanding of patent applications.

4. Bioscience

Several participants who specialize in prosecuting life sciences applications noted that it is now very difficult to obtain patents in particular inventive fields, such as purified products, methods of treatment using purified molecules, purified enzymes for industrial processes, enzyme variants, and personalized medicine diagnostics—fields where advances had been patentable for decades, or even centuries. Patent examiners seem less likely to allow claims focusing on the structures of these molecules, and more likely to allow claims focusing on the functions of these molecules. Examples of related types of claims not being allowed include purified strains, purified enzymes for industrial applications, and even enzyme variants. It is particularly problematic that the market seeks purified substances to eliminate, for example, contamination, but the patent law requires changes or even marked differences to be present. This is an example of the law diverging from market and technology demands. Moreover, it is not clear under the law how substantial changes to natural substances must be to warrant patentability.

As a result, companies are not pursuing such claims, are abandoning applications, and are not filing continuations. Such companies believe that patent protection for these inventions and discoveries are critically important, and they are biding their time in the hope that the law of patent eligibility will shift back to broader eligibility.

There has been a dramatic decrease in the ability to patent personalized medicine claims. One participant noted a perverse situation reflecting the apparent view that diagnostic inventions are not eligible as a category: a claim otherwise eligible appears now to be ineligible if it includes a method of diagnosing a disease or other problem or characteristic. As a result, more specific, narrower, and more useful claims have been denied patent eligibility, again merely because they include a step of diagnosis. It is also notable that the standard for patent eligibility for diagnostics has moved in the opposite direction of the underlying technology. Just as inventors have made significant advancements improving the ability to provide targeted medical information to patients, the Supreme Court has eliminated the eligibility of these inventions for patents. The Supreme Court has created a test for eligibility that stands in the way of the creation of new personalized medical inventions.

The effect on companies operating in the life sciences area has been dramatic. In the past, these companies invested very large sums of money (perhaps more than $2.5 billion) on research and development and, simultaneously, filed patent applications to protect their investments. These patent applications, when issued as patents, complied with the standards of patent eligibility as those standards existed at the time the patents issued. Now, sometimes 10 to 15 years later, the Supreme Court has changed those standards and there is no recourse available. There is no opportunity to amend the claims of the patents to comply with the new eligibility test.

5. Information Technology

Participants agreed that the *Bilski* and *Alice* decisions have substantially eliminated patent eligibility for pure business methods claims—claims that do not improve the functioning of computers. The viability of software claims is hazier. Several practitioners noted that art units addressing encryption and optical networks are not predictable.

One participant noted "almost no luck" in overcoming eligibility rejections with pre-*Alice* patent applications. The only available strategy is to file a Request for Continuing Examination and try to get a different examiner. Notably, the data indicates that patent applications filed after *Alice* show no significant improvement in terms of ability to overcome eligibility rejections. Moreover, the data shows that sometimes the only rejection preventing a patent application from issuing as a patent is a rejection based on § 101. One participant relayed how difficult it is to explain to a client that a patent

application has no prior art rejections under §§ 102 or 103, and yet the patent examiner has finally rejected the application as claiming something that is conventional or routine.

Patent prosecutors noted that a key determinant of whether a software claim will issue is how the patent is classified. If the patent is categorized within the ecommerce area, there is little chance that its claims will be found eligible. Thus, applicants focus a lot of their strategic effort in drafting their patents so that they will be assigned to a technology center with a higher eligibility proclivity. Prosecutors noted that most pre-*Alice* software-related filings are lost and not worth pursuing.

A. EFFECTS ON PATENT ASSERTION/LITIGATION/CASE MANAGEMENT

The fourth session focused on the effects of the shift in patent eligibility jurisprudence on patent litigation activity and judicial case management.

1. Framing

An experienced patent litigator launched the session by summarizing the key shifts in patent assertion strategy. This participant noted that patent owners today are far less likely to assert dubious patents. The cases being filed in the post-*Alice* era more frequently relate to patents on networking technologies and other machine-related claims as opposed to business methods. Nonetheless, there remains a substantial gray area due to the vagueness of § 101 jurisprudence.

As a result of this uncertainty, plaintiffs are likely to assert more patents and more claims. Prior to the *Mayo* decision, a typical filing would assert no more than four to six patents because of limitation of trial time and jury's cognitive capacity. Following *Mayo*, plaintiffs are more likely to assert ten or more patents as a hedge against the risks of patents being invalidated during early case management on ineligibility grounds. This has raised the complexity and potentially the cost of patent cases.

The other major effect of the shift in patent-eligibility standards has been to front-load patent case management in the software and bioscience fields. Defendants invariably seek early dismissal of claims under § 101. This puts the judge in the difficult position of applying the vague "inventive application" framework to patent claims that have already survived scrutiny under §§ 102, 103, and 112 at the Patent Office. Nonetheless, many district courts have been receptive to these motions, resulting in cursory assessment of patent eligibility—often before claim construction. These district judges may be deciding what is well-understood, routine, and conventional in technical fields without a well-developed record, although for some patents they are able to find these admissions in the patent specification.

2. Discussion

While acknowledging that the *Mayo*/*Alice* standards lack coherence—often boiling down to a subjective "I know it when I see it" standard—several participants commented that the *Alice* decision has allowed defendants to get particularly weak patent cases dismissed early in the litigation process, resulting in substantial savings and effectively eliminating many dubious patents from the system. These participants see the jurisprudence becoming somewhat more predictable. In their view the decisions effectively exclude pure business methods and emphasize technical solutions to technical problems.

Several bioscience industry participants noted that companies have been reluctant to bring test cases, especially after the Supreme Court declined review in the *Sequenom* case. They have lost faith in the Supreme Court and no longer see the Federal Circuit as having the courage to percolate eligibility standards.

IV. LEGISLATIVE PROPOSALS

The final workshop session focused on whether legislation is needed to address the shift in patentable subject matter jurisprudence, as well as reactions to various proposals. The session began with a brief summary of the pending proposals and the various evaluative criteria set forth in Section I.C. We then went around the table to afford all participants an opportunity to express their perspectives and react to views of others.

A. SUMMARY OF DISCUSSION

Building upon the prior presentations and discussions, the participants engaged in a wide-ranging discussion of the current status of the law governing patent eligibility, as well as the potential avenues for reform, including recent legislative proposals. Several themes developed. On the one hand, a consensus emerged that the current state of the law is indefensible as a matter of legal principle and is causing particular difficulties for bioscience fields. Participants largely agreed that the Supreme Court did not appear poised to make further significant pronouncements about the scope of patentable subject matter in the foreseeable future. As a result, participants largely agreed that legislation would be necessary to address the problems that have emerged for bioscience researchers. On the other hand, there was disagreement on the need for legislative reform of patentable subject matter relating to computer software. Moreover, there was a lack of agreement on the best solution to current problems, and none of the current proposals listed in Section I.B. garnered consensus. This Section summarizes the areas of consensus and disagreement, with particular attention to the bioscience and software fields. We then summarize the participants' views regarding the existing legislative proposals and other potential approaches.

1. The Need for a Legislative Solution

The discussion repeatedly returned to the need for legislation to address the problems plaguing patent eligibility. A consensus emerged that key aspects of the Supreme Court's *Mayo*, *Alice*, and *Myriad* decisions were indefensible as a matter of statutory interpretation or fidelity to prior case law. Significantly, this consensus spanned the range of industry representatives and legal scholars. No one, for example, disputed Professors Lefstin and Menell's critique of the Supreme Court's *Mayo*/*Alice* two-part test focusing on the search for an "inventive" rather than merely a "practical" application of a natural law or physical phenomenon.

More generally, there was consensus that a test requiring a search for an "inventive" application of a natural law or physical phenomenon does not provide adequate objective guidance to patent examiners, jurists, practitioners, or the inventive community. As one participant explained, the current state of affairs is "awful" because investors look for patents, which are critical to their investment decisions. And yet under the current law, patent lawyers cannot provide clear or reliable guidance about eligibility.

The manifestation of these concerns differs markedly across fields. Patent prosecutors and examiners do not know what to do when confronted with a question of software eligibility. In the words of one participant, prosecutors in particular are "pulling their hair out." By contrast, bioscience research representatives and many legal scholars worry that the Supreme Court's standards relating to breakthrough scientific advances are far too clear and clearly wrong. They believe that the Supreme Court has eliminated patent protection for important useful research discoveries that are conventionally applied. They emphasized that the major research challenge is often in scientific discovery, not application. Once scientists discover scientific laws, they can use routine, conventional, and well-understood techniques to make such discoveries useful for improving public health, safety, and welfare.

Many participants viewed patent eligibility doctrine as incoherent. It lacks the clarity needed for a property-based incentive regime to function effectively. The lack of clarity has led the USPTO to restrict patent eligibility even beyond what some participants believe the case law requires.

Although software companies that are defendants welcome the opportunity to challenge vague and uninventive claims on eligibility grounds, several participants noted that the lack of coherence presents problems. As one participant noted, the "sky was falling" after the Federal Circuit's *State Street Bank* decision,[107] when the Federal Circuit opened the patent-eligibility

107. *See* State St. Bank & Tr. Co. v. Signature Fin. Grp., Inc., 149 F.3d 1368 (Fed. Cir. 1998).

door to all software and business methods claims. While the Supreme Court has brought an end to that problem, "the sky is falling again now" because the Supreme Court has gone too far in the opposite direction in *Mayo* and *Alice*.

Many, but not all, participants agreed that legislation would be appropriate to solve problems caused by the current state of the law. The challenge is in finding a balanced compromise—which might be characterized as a separating equilibrium in which bioscience researchers can once again pursue patent protection for applications of new scientific discoveries, without unleashing a wave of assertions of dubious software and business method patents. Some others, particularly those from software companies that are frequently sued by non-practicing entities, however, expressed a preference for letting the current regime play out in the lower courts, even while recognizing the problems with the current state of the law.

Many participants highlighted the need for a clear legislative solution over the existing common law scheme. One participant expressed concern that the United States is not leading the world with respect to patent eligibility; that "things have gotten pretty bad" with respect to reaching the right result in cases, particularly in the field of biotechnology; and, in response to the argument that "we should just let the courts figure this out because it is too hard," one participant retorted that "we did, and [the courts] screwed it up really badly." Many participants bemoaned the prospects of Supreme Court correction.

As several participants noted, the Supreme Court has now heard several cases in this area since 2010 and has been unable to identify a coherent test that comports with the legislative framework. Moreover, while the Supreme Court's *Flook* decision diverged from the traditional approach for patent eligibility, the Court effectively overruled *Flook* in its decisions in *Chakrabarty* and *Diehr* within a few years. The current Supreme Court, by contrast, does not appear to be interested in revisiting the *Mayo* test (which resurrected aspects of *Flook*), as evidenced by the denial of certiorari in *Sequenom*, where the Court did not even ask for the Solicitor General's view of the case despite over twenty amicus briefs from a wide range of industries and scholars advocating review. In the end, many participants, particularly those in bioscience fields but also some in software fields, expressed an urgent need for a legislative solution. Some participants thought case law development on whether a software claim recited a technical effect could lead to a more predictable and useful body of law.

2. Field-Specific Concerns

Many participants directed their comments to challenges facing the bioscience and software fields. In this Section, we summarize their comments and identify particular areas of consensus and disagreement within these fields.

We also identify support for particular proposals from participants with expertise in these fields.

a) Bioscience

Participants from the bioscience industries as well as several academics strongly advocated for legislative reform of patent eligibility. As they explained, the case law is not developing in the biotechnology area because of fear that the courts will expand the ineligibility zone. Stakeholders are fearful of bringing test cases. One participant expressed the concern that the Supreme Court can take the next case (as it did in *Mayo*) and eliminate all of the intervening case law development. According to another participant, every § 101 case "makes your heart stop" because of the ability of courts to invalidate bioscience patents after so much money is invested in research and development predicated on the patentability of the underlying technology. Furthermore, according to several participants, the USPTO has shown little appetite for exercising its patent law expertise to confront new challenges. The agency has been largely reactive, or has adopted rigid interpretations of cases such as *Myriad*, interpretations that arguably restrict eligibility even beyond what the Supreme Court requires.

Several participants expressed that the case for legislative reform is particularly salient in particular areas of bioscience research such as medical diagnostics. There was broad agreement among bioscience industry representatives that the Supreme Court's eligibility framework fundamentally misapprehends the research challenges in the medical diagnostic field and that a legislative solution is the only effective way to restore confidence in patent protection for applied scientific advances in this area. The USPTO's interpretation of *Myriad* was another area of significant concern, because of the loss of investment and development necessary to bring treatments based on natural products to the public. One participant suggested that legislators should focus on how best to provide incentives for optimal investment in research and development. According to this participant, Congress needs to confront the challenges of curing cancer. This participant advocated erring on the side of patent eligibility so as to "provide a strong incentive for invention."

In terms of specific proposals, some participants agreed that newly discovered laws of nature should not be considered to be prior art, and that practical applications of discoveries should be eligible for patenting. Other participants noted concerns about the effects of overbroad protection on cumulative innovation—efforts by follow-on inventors and concerns about licensing impediments and costs. Several participants expressed willingness to expand 35 U.S.C. § 287 to protect doctors and/or to expand the experimental use exception to protect individuals and companies who improve patented technology from being subject to patent infringement liability. Others favored

expanding patent law's experimental use exception to infringement liability so as to balance the interest in providing an incentive for the original discovery and the interest in encouraging follow-on inventors who desire to improve upon practical applications of the discovery.

Several participants indicated a willingness, through legislative reform if necessary, to treat the biotechnology industry differently than the software industry. For example, if patenting of broad generic solutions is unacceptable to the software industry or if it is not possible to identify an elegant, omnibus solution, these participants were open to legislative reforms targeting bioscience fields. One participant suggested looking outside of patent law for a solution that would fund the biotechnology and life sciences industries, such as medical reimbursements for diagnostics.

b) Software

Participants broadly agreed that the current eligibility regime fails to provide predictability, although some in the software field expressed the view that case law is improving predictability. Many commented that patent eligibility jurisprudence is too blunt a tool to invalidate many software-related claims, while noting many of these claims would likely fail §§ 102, 103, and/or 112. Some participants noted that the current regime calls into question some software-related claims that should be eligible, although unlike in the bioscience area where participants generally favored patent eligibility for conventional applications of scientific discoveries, it was more difficult to articulate particular software areas that are being erroneously, categorically excluded. In short, the current software eligibility regime causes inefficient redundancy, a cloud of suspicion on all software-related patents, and incorrect outcomes with respect to some software-related claims.

Some software industry representatives favored the current regime on the purely instrumental ground that it provides a shortcut to invalidating many dubious software patents and can save litigation resources. Others favored a more open-ended framework that affords protection for applications of discoveries, including algorithms. One participant expressed concern that this latter approach is similar to the "useful, concrete and tangible result" test most commonly associated with the Federal Circuit's decision in *State Street Bank*.[108] Several participants, moreover, expressed the view that pure business methods should not be patent eligible, even if they are implemented on computers, because of low development cost, deleterious effects on free market competition, and the absence of any need to provide an incentive to ensure their development. One participant defended the eligibility of pure business methods on the ground that all processes meeting the §§ 102, 103, and 112

108. *Id.* at 1373–75.

requirements should be patentable.

Several participants expressed support for a technological arts test as a way of excluding eligibility for business methods (even if they use computers in non-technologically inventive ways), while preserving eligibility for software claims that improve the functioning of computers and computing technology. One participant noted, however, that it is unclear how the technological arts test applies to new technologies. That participant noted that European patent examiners initially considered artificial intelligence to be ineligible. Another participant suggested that the difficulty of determining eligibility of software relates to the broad statutory term "process," and so a legislative solution might focus on narrowing that particular statutory category.

Other participants emphasized that software patents are plagued by overbroad scope resulting in significant part from functional claiming. They advocated addressing these concerns through applying § 112(b) and (f) in a rigorous way, including early in litigation. Others similarly suggested that the primary concern is lack of enablement or written description under § 112(a), and similarly encouraged applying these doctrines earlier in litigation.

Some, but not all, participants involved with software nevertheless indicated a desire for a wait-and-see approach to allow the case law to develop with respect to software-related claims. Others similarly expressed concern about the political feasibility of amending patent eligibility at a time when many software companies are concerned about abusive patent assertion. Several participants suggested that any legislative reform to patent eligibility that eliminates this early dispute resolution mechanism would need to be paired with other reforms that help reach similarly efficient results. We address this interest in more detail below. We note, however, that several other participants responded that we should not impair innovation in the pursuant of judicial efficiency.

3. Evaluation of Existing Legislative Proposals and New Proposals

In the previous Section, we summarized comments on the impact of particular proposals on the bioscience and software industries. In this Section, we summarize more general comments as well as comments directed to particular proposals but not limited in scope to either bioscience or software industry concerns. We also summarize new proposals identified in the workshop.

Most participants agreed that eligibility should be a "coarse filter" or "minimal hurdle." Furthermore, several participants expressed the desire to prevent deconstruction of patent claims, which involves ignoring claim elements.

Many participants expressed support or concern with particular proposals.

One participant, for example, favored the IPO proposal as a constructive starting point, but also thought that a test focusing on whether the claimed invention is in the technological arts might find broader support. Another participant favored a test that focused on whether claims are specific and patentable under §§ 102, 103, and 112. Another participant suggested adopting a technological arts test, but at the same time making it clear that technology includes practical applications of discoveries. Such a technological arts test might be neutral facially, but have differential impact in different industries (in particular biotechnology versus software). Yet another participant suggested that a technological arts test, without some definition, is ambiguous and might be seen as consistent with what courts are doing now. This participant suggested that technological arts be defined as human-directed efforts to harness natural laws and physical phenomena to achieve practical end results. This definition, it was posed, would exclude purely mental processes.

What this discussion highlighted is that none of the proposals, at least in their current form, provides an effective test for distinguishing between the bioscience and software fields. Some participants advocated developing a test that expressly distinguishes between bioscience and software eligibility. Several participants saw merit in a test that restored the practical application of a discovery standard in conjunction with expressly limiting patent eligibility to the technological arts. Some questioned whether "technological" could be clearly delineated. Other participants, however, expressed a desire for a trans-technology approach. They noted the convergence of bioscience and software fields through, for example, advances in bioinformatics.

Some participants expressed reluctance to depart from the current standards because of the litigation cost savings and speed advantage of being able to challenge patent validity early in litigation through a motion pursuant to Federal Rule of Civil Procedure 12(b)(6). Several participants, however, recommended that courts allow early 12(b)(6) motions on more appropriate patent law doctrines that have extensive historical pedigrees that have produced objective guidelines, including the written description and enablement requirements. In this regard, several participants expressed a desire to preserve the ability early in litigation to eliminate poor quality patent assertions made by patent assertion entities (which occurs primarily in the software industry), while recognizing that the current test unfortunately undermines research and development incentives and investment in bioscience.

Rather than have Congress fashion legislation adopting a new test for patent eligibility, some participants suggested Congress give the USPTO the authority to do so. One participant, for example, noted the inherent difficulty in predicting technological advances and the patent system's purpose in bringing the unknown into the known. For this participant, these

considerations suggested it might be better to defer to the USPTO rather than courts given the USPTO's expertise and ability to coordinate and update standards. Another participant noted the tension between maintaining flexibility to allow for accurate results (particularly in different industries) and constraining judicial intervention. This participant questioned whether courts should be making these distinctions at all, or instead whether the USPTO should make eligibility determinations without having courts revisit the question. This participant suggested that Congress should give the USPTO rulemaking authority to decide what is and what is not eligible.

B. TOWARDS A COMPROMISE PROPOSAL: THE NEED FOR CONSENSUS-BUILDING

The workshop revealed broad agreement that the Supreme Court's patent eligibility jurisprudence has diverged from the Patent Act's text and legislative history as well as long-standing jurisprudential standards. The participants also agreed that the Supreme Court's stated rationale and formulation lacks a sound foundation and misapprehends the *Neilson v. Harford* decision on which it grounds the inventive application standard. Furthermore, the workshop revealed a consensus that it is unlikely that the Supreme Court will reconsider the patent eligibility issue in the foreseeable future. Conferees also doubted that the Federal Circuit will confront the core concerns surrounding patent eligibility. Thus, legislative reform will be necessary to effect significant change in patent-eligibility standards.

While nearly all of the conferees recognized that this state of the law poses serious concerns for bioscience research and development, there existed substantial reluctance on the part of some software industry representatives about pursuing legislative reform that could increase patent assertion activity and raise defense risks and costs in the software field. Some participants also thought that the courts should be given time to develop an appropriate screen for the eligibility of software patents and saw some progress in the developing case law.

This suggests to the workshop convenors and authors of this report (Jeffrey Lefstin, Peter Menell, and David Taylor) that the most fruitful approach to reform legislation would restore the traditional patent-eligibility standard at least for bioscience advances—that is, establishing that conventional application of scientific discoveries are eligible for patent protection—while addressing concerns about cumulative creativity and abusive patent assertion. Such additional provisions could include the following: (1) an expanded experimental use exception at least for doctors and medical researchers; (2) exclusion of non-technological subject matter, notably pure business methods (a technological arts test); (3) a mechanism to encourage courts to consider 12(b)(6) motions directed to § 112 issues (as

opposed to § 101 issues) early in patent case management; (4) fee-shifting aimed at discouraging nuisance value patent lawsuits; (5) higher thresholds for enhanced damages in the software field; and/or (6) shorter duration for algorithm-based inventions—i.e., where the point of non-obviousness is a computer-implemented algorithm. We also note that compromise legislation might also address distinctive issues relating to affected industries that lie outside of the patent field, such as reimbursement policies relating to medical diagnostics.

We recognize, however, that there are differing views regarding each of these compromise elements. We therefore call for consensus-building among the interested constituencies. In this regard, we recognize that the IPO, AIPLA, and ABA-IPL proposals were approved by the governing boards of those organizations, which include representatives of various constituencies, including parties having significant interests in the bioscience and software industries. There was no consensus among our participants, however, that any of these proposals should be the exclusive focus of a legislative effort going forward. In short, there was a consensus that more discussion is necessary. In this regard, in particular, we recommend a future workshop aimed at developing a compromise package.

APPENDIX A: PATENTABLE SUBJECT MATTER WORKSHOP AGENDA

9:00 am	Breakfast
9:30 am	Introduction
10:00 am	Legal Background
11:15 am	Break
11:30 am	Effects on R&D
12:15 pm	Lunch Buffet
12:45 pm	Working Lunch: Effects on Prosecution
1:45 pm	Effects on Patent Assertion/Litigation/Case Management
2:30 pm	Break
2:45 pm	Legislative Proposals
3:30 pm	Discussion of Proposals
5:00 pm	Next Steps
5:30 pm	Reception
6:15 pm	Dinner

APPENDIX B: PARTICIPANT LIST

Academics	**Affiliation**
Menell, Peter (convenor)	UC-Berkeley
Lefstin, Jeff (convenor)	UC-Hastings
Taylor, David (convenor)	SMU
Collins, Kevin	Wash U (St. Louis)
Cotter, Thomas	Minnesota
Eisenberg, Rebecca	Michigan
Holbrook, Timothy	Emory
Lemley, Mark	Stanford
Morris, Emily	Univ. of Maine
Narechania, Tejas	UC-Berkeley
Rai, Arti	Duke
Samuelson, Pamela	UC-Berkeley
Practitioners	
Hubbard, Marc	Hubbard Johnston
Kappos, David	Cravath, Swaine & Moore
Powers, Matthew	Tensegrity Law Group
Noonan, Kevin	McDonnell Boehnen Hulbert & Berghoff
Fu, Diana	Van Pelt, James & Yi
Sachs, Robert	Fenwick & West
Sonnenfeld, Ken	King & Spalding
Industry/In-House	
Sauer, Hans	Deputy GC (IP), BIO
Armitage, Robert	former Senior VP and General Counsel of Eli Lilly & Co.
Jackson, Benjamin	Myriad
Pleasure, Irene	Genentech
Michel, Suzanne	Google
Meehan, Michael	Uber
Jones, David	Microsoft
Underweiser, Marian	IBM
Skabrat, Steven	Intel
Rao, Dana	Adobe
Sarboraria, Matthew	Oracle

Simon, David	Salesforce
Government/Other	
Whyte, Ronald M.	U.S. District Judge, N.D. Cal. (retired)
Simpson, Jamie	Staff, Senator Christopher Coons (D. Del.)
Givens, Alexandra Reeve	Executive Director, Institute for Technology Law & Policy, Georgetown University Law Center, former Chief Counsel for IP and Antitrust on the Senate Judiciary Committee, working for senior Democrat Senator Patrick Leahy (D-Vt)
Bahr, Robert	Deputy Commissioner for Patent Examination Policy, USPTO
Kelley, Nathan	Deputy General Counsel for Intellectual Property Law and Solicitor, USPTO
Munck, Suzanne	Deputy Director and Chief Counsel for Intellectual Property, Office of Policy Planning, Federal Trade Commission

APPENDIX C: PREPATORY MATERIALS

Brief of Professors Jeffrey A. Lefstin & Peter S. Menell as Amici Curiae in Support of Petition for a Writ of Certiorari, Sequenom, Inc. v. Ariosa Diagnostics, Inc., pp. 4-14, No. 15-1182 (Apr. 29, 2016), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2767904 [https://perma.cc/ZZB9-Q4JA].

David O. Taylor, *Amending Patent Eligibility*, 50 U.C. DAVIS L. REV. 2151 (2017).

Legislative Proposals

- A Proposed Path Forward for Legislatively Addressing Patent Eligibility Law: Patenting Genes, Natural Products and Diagnostics: Current Status and Future Prospects, Conference Held at The Banbury Center, Cold Spring Harbor Laboratory (Nov. 9-11, 2016) (Banbury Statement) (available at https://www.uspto.gov/sites/default/files/documents/Updated%20Banbury%20Statement.pdf) [https://perma.cc/YX8T-3BF3].
- Intellectual Property Owners Association (IPO), Proposed Amendments To Patent Eligible Subject Matter Under 35 U.S.C. § 101 (Feb. 7, 2017).
- European Patent Convention, Art. 52, Patentable Inventions.
- ABA-IPL, Comments Related to Patent Subject Matter Eligibility (submitted to USPTO) (Jan. 18, 2017).
- Google Inc., Comments Related to Patent Subject Matter Eligibility (submitted to USPTO) (Jan. 18, 2017).
- Internet Association and Computer & Communications Industry Association (CCIA), Comments Related to Patent Subject Matter Eligibility (submitted to USPTO) (Jan. 18, 2017).
- Robert A. Armitage, Presentation Slides for USPTO Roundtable 2—Patent Eligibility Contours, Can We Find a Rational, Principled, Expansive, and Politically Palatable Approach to Statutorily Defining Patent Eligibility? (Dec. 5, 2016).
- Ryan Davis, Kappos Calls for Abolition of § 101 of Patent Act, Law 360 (Mar. 2, 2017), https://www.law360.com/articles/783604/print?section=ip [https://perma.cc/UAQ4-YL4N].

USPTO Patentable Subject Matter Guidance Documents

- 2014 Interim Guidance on Patent Subject Matter Eligibility, 79 Fed. Reg. 74618 (Dec. 16, 2014).
- July 2015 Update: Subject Matter Eligibility.
- Formulating a Subject Matter Eligibility Rejection and Evaluating the Applicant's Response to a Subject Matter Eligibility Rejection (May 4, 2016).
- Recent Subject Matter Eligibility Decisions (*Enfish, LLC v. Microsoft Corp.*, and *TLI Communications LLC v. A. V Automotive, LLC*) (May 19, 2016).
- Recent Subject Matter Eligibility Rulings (*Rapid Litigation Management v. CellzDirect* and *Sequenom v. Ariosa*) (Jul. 14, 2016).
- Recent Subject Matter Eligibility Decisions (Nov. 2, 2016).
- December 2016: Interim Eligibility Guidance Quick Reference Sheet.
- Training materials on subject matter eligibility (Mar. 3, 2017).